Large Filing Separator Sheet

Case Number: 08-709-EL-AIR
08-710-EL-ATA
08-711-EL-AAM

Date Filed: 7/25/2008

Section: 4

Number of Pages: 200

Description of Document: Application
Volume 4, 5 & 6
Schedule S-4.2
Part 1 of 3

IT 5005 – Communications and Operations Management

5005.7.3.1 eBusiness Customer Accounts

Customer accounts used for external eBusiness applications must have an access account management methodology. "IT 5006.2 User Access Management" defines the preferred account management controls, however, the following less stringent controls may be used for external eBusiness customer applications, i.e. online bill payment. In all cases, the highest level of security requirements within the environment will dictate the acceptable security controls.

a) Account Management - An External Customer Application account that has remained inactive for a period of 220 days must be removed from service.

b) Privileges - External Customer Applications accounts must only be authorized to access customer information specific to that customer and must not be authorized to access other information with a security classification higher than "Public". For more information, see "IT 5002 Asset Management".

c) Account Lockout - ID lockout must occur after ten consecutive unsuccessful login attempts. The lockout period must be at least 30 minutes. When the customer is informed of the lockout, enticement information must not be given to reveal the lockout period. Any account lockout must be reported to the Information Custodian.

d) Password Management - Password distribution controls must be implemented that will ensure that only the authorized individual knows their password. The following conditions apply:

- End Users must be instructed on the acceptable use of passwords as determined by the Application Owner.
- Passwords must not be transmitted in clear text such as e-mail or http.
- Customers may change their passwords via the extranet applications that provide the following controls:
  - A minimum of two password hints must be provided prior to resetting the password.
  - Password hints must not contain the password.

e) Password Use – The following conditions apply to the use of passwords:

- Syntax – External customer application ID's must have passwords that are a minimum of eight characters in length and contain a mixture of letters and numbers.
- Aging - Password aging is not required for External Customer Application passwords.
- Re-use - Re-use is permissible for External Customer Applications ID passwords.
- Confidentiality - eBusiness customer passwords are not to be shared with or used by the Duke Energy workforce. This does not apply to members of the workforce who subscribe to a Duke provided eBusiness application.

IT 5005 – Communications and Operations Management

5005.8 Monitoring

Information systems must be monitored for unauthorized processing activity or activity that indicates an information asset is at risk. The level and type of monitoring must be commensurate with the asset value and the associated risk of compromise.

5005.8.1 Monitoring Process

Monitoring processes must address event identification, response management and audit logging. Monitoring processes must include:

a) Event Identification – Monitoring of key activities to indicate an information asset is at risk as well as source identification.

b) Response Management – A process for generating and responding to event alarms that consists of:

- Prioritizing the potential impact of monitored events.
- Process to ensure timely discovery of events.
- Response requirements to include event reporting, i.e. CIRT notification, see "IT 5008 Information Security Incident Management".
- Process for archiving security events.

c) Audit Logging – Monitored events must be saved to a log. The log information must be protected against loss, tampering, and unauthorized access.

- The frequency of log review or archiving must be established to prevent the loss of data due to 'rollover' or 'lock log files when full' configurations.
- Log file retention periods must be established to meet operational and legal requirements and must be complaint with company records retention policies.
- Logs containing security events involved in an investigation must be archived and retained for at least one year.
- Archival of log files must include recovery procedures to ensure the data can be retrieved. Procedures must include guidance on maintaining data confidentiality and integrity and also must provide for changes in technology that may affect data availability.
- Only appropriate members of the Legal Department, Audit Services, Corporate IT Strategy and Compliance, or individuals specifically authorized by these departments may access logs.

Note: Individuals or groups authorized by Corporate IT Strategy and Compliance must have the ability to obtain, at a minimum, read-only access to all information assets.

5005.8.1.1 System Log Monitoring

System Administrators must establish a process for monitoring information system logs to detect suspicious security activity as defined above. System Administrators must ensure that logs are activated and that appropriate monitoring software is enabled. At a minimum, the following events must be monitored:

a) Session activity to include:

- Account identification
- Log-in success
- Log-in failure
- Log-in date/time
- Log-out date/time

b) System start-ups and shutdowns

c) Relevant security events, such as:

- Users switching user ID's or system identity during an on-line session
- Password guessing activities
- User privilege escalation attempts and or successes
- Modifications to system security configurations
- Privileged access activity
- Changes to system logs or logging configurations

5.8.1.2 IDS Monitoring

A centralized intrusion detection program must be implemented to provide the ability to detect and identify suspicious network traffic and server, or host, activities. This program must be centrally managed, must meet the requirements defined above for a monitoring process, and must include the following elements:

a) Only authorized individuals will have access to the sensors, the policies, or the logs.

b) Only authorized and approved policies are allowed.

c) An IDS policy management process that defines the requirements for the development, test, approval, and authorization of policies.

d) Ensure network sensors are placed to ensure all network traffic that traverses the corporate network perimeter is monitored. At a minimum, network sensors must be placed as defined below:

Connection Type	Network Configuration	IDS Monitoring points
Category I	• Perimeters • DMZs • Dial-in services, FTP, VPN, Telnet	• Between the Internet and the outer most firewall. • Between the DMZ and the Internal network. • Between the Internal network and the inside firewall.
	• Single access points for out bound only traffic	• Network Sensors on internal side of screening device.
Category II	• Inter-Business Unit Point of Entry	• All traffic between Business Units and Corporate Networks where the Business Unit traffic is identifiable. • All traffic between Business Partners and Corporate Networks.

f) Ensure that host-based sensors are installed on servers that provide a service or function which if compromised can result in negative impact to Duke Energy. At a minimum, host-based sensors must be placed as follows:

Connection Type	Server Function/Type	At Risk Services
Category I	External Servers	• External facing servers accessible via the internet. • Servers that reside in the DMZ or other external networks. (i.e. Web Presentation or Application Servers) • Servers providing remote access services such as FTP.
Category II	Business Critical	• Business Units are responsible for deciding whether to implement Host Based IDS. • Business units will coordinate with EITS to implement the Host Based IDS which should be placed on servers that support business critical applications based on: o Availability o Attack Likelihood o Security Classification

IT 5006 – Access Control

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date: 05/01/2006
Revision Date:
Revision No:

Statement of Purpose

This standard establishes the requirements for logical controls associated with access accounts and access points. Logical access must be authorized, managed and removed or retired when no longer needed.

IT 5006.1 Security Business Requirement for Access Control

Access to Duke Energy information assets will only be allowed in support of business needs. Access controls must be used to prevent accidental or malicious modification, destruction, or disclosure, and for user identification.

IT 5006.1.1 Access Control

Access accounts must be used to control individual and system access to Duke Energy information assets and to control the privilege levels. Access accounts must uniquely identify a single person or system. The access account and password combination, or other authentication mechanism, will be used to validate the identity of the account owner and to manage access privileges. Every access account must be assigned to an individual owner who is exclusively responsible for the activity associated with that account.

IT 5006.2 User Access Management

User Access Management provides for the life cycle management of access accounts. The life cycle of an access account consists of the following: registration (creation of the account), the privileges assigned to the account, password management, review of access rights, and account termination. For more information, see "IT 5006-01 User Accounts".

IT 5006.2.1 User Registration

User Registration, or the creation of an access account, requires a validated business need and information access authorization. A single individual is not allowed to request and then also authorize or enable an access account. This process requires two individuals: one to request, and the other to approve and authorize or enable an account. Business needs must be validated by management. The access must be authorized by the Information Owner. Access accounts must be requested through an approved enrollment process. See "IT 5006-01 User Accounts" for details. Following are the different types of access accounts:

a) General Account - General accounts are commonly referred to as a user account and are used for task-oriented or functional access to an information asset.

b) Privileged Account - Privileged accounts are typically associated with operational or support functions.

c) Special Account - Special accounts are used to address specific needs or situations. Typically, Special accounts are process, shared or emergency use accounts. For additional information, see "IT 5006-01 User Accounts".

d) Customer Account - Customer accounts are used for external eBusiness applications. The application owner is responsible for developing and maintaining a "User Access Management" methodology as defined in this standard. For additional information, see "IT 5005.7 Electronic Commerce Services".

IT 5006.2.2 Privilege Management

Privilege Management is the allocation and use of privileges or access rights. Privileges must be assigned to an access account based on the lowest level of access necessary. A single individual is not allowed to request and then also authorize or modify access account privileges. This process requires two individuals: one to request, and the other to approve and authorize or modify an account. Business needs must be validated by management. The Information Owner must authorize the access. Modification to access account privileges must be requested through the Duke Energy enrollment process, see "IT 5006-01 User Accounts" for details. It is the responsibility of the account owner to adhere to the controls associated with the highest privilege level assigned to an account. The following conditions apply:

a) General Access - General Access provides limited access for performing a specific task or action. It is assigned to an access account that is used to interact with an application at a functional level and is unable to effect a change to the operations of the system or application.

b) Privileged Access - Privileged access is typically used for an operational or support function, and is assigned to accounts required to effect a change to the privileges of an access account or to the configuration or operations of an infrastructure asset or an application. Privileged access must be documented to identify the individual, or system(s), assigned to the account and the applications or systems they support.

IT 5006.2.3 Access Account Management

Accounts must be disabled when no longer needed or if unauthorized use is suspected. For additional information, see "IT 5003.3 Termination or Change of Employment". The following conditions warrant account deactivation:

a) Account Inactivity - Accounts that have remained inactive for sixty days must be inactivated. The account must remain inactive until manually reset by the appropriate IT support group.

b) Account Lockout - Accounts must be locked out of the resource in which they are attempting to gain access upon ten consecutive authentication failures. The account must remain locked until manually reset by the appropriate IT support group.

IT 5006.2.4 Password Management

Password controls must be implemented to ensure that only authorized individuals know an account password. The following conditions apply:

a) Duke Energy credentials must not be used to access Non-Duke Energy systems, i.e. Duke Energy issued username and passwords are not to be used for banking, Yahoo, or other non-work related access.

b) The identity of the receiving individual must be verified before issuing a password.

c) Initial passwords must be temporary and be changed upon first use.

d) Passwords must remain confidential and be changed immediately if compromised.

e) Passwords must be encrypted or protected when in transit and storage, using approved methods and technologies, as determined by Corporate IT Strategy and Compliance.

f) Passwords being provided to external parties must be sent securely. If encryption is used, the password to open the file must be communicated separately from the file containing the password information.

IT 5006.2.4.1 Password Use

The following password controls must be used for all accounts unless otherwise specified:

a) General Account Syntax - passwords must be complex and have a minimum of eight characters.

b) Privileged Account Syntax- passwords must be complex and have a minimum of nine characters.

c) Initial Passwords - passwords must be changed after initial use, must conform to this standard and must not be easily associated with the company or the user, i.e., social security number, user-account, employee number, employee address, numerical equivalent of name, etc.

d) Aging - Users must be forced to change passwords at least every sixty days.

e) Reuse - Users must not use cyclical or patterned passwords. For example, when changing passwords, users must not add a number at the end of the password in sequence.

f) Systems must use password history controls to maintain a password history of users and disallow the user from reusing one of the passwords in their password history file.

g) The history file must contain, at a minimum, the last 10 passwords of users, stored in hashed or encrypted form.

Note: Complex Passwords have at least three of the following four characteristics:

1. Uppercase letters (A-Z)
2. Lowercase letters (a-z)
3. Numbers (0-9)
4. Special characters, i.e. "!, @, #, $, %, ^, &, *, and +"

Note: For MVS/Mainframe, only the following symbols are allowed: "@, #, and $"

IT 5006.2.5 Vendor Default Accounts

Vendor default accounts, when not required, must be removed or deactivated at the time of equipment or system installation or conversion. When default accounts are required, the following conditions apply:

a) The account must be renamed.

b) The passwords must be changed to meet the password requirement defined in "IT 5006.2.4 Password Management".

c) Only authorized personnel may have access to the default account password.

d) The default account is not to be used by individuals.

IT 5006.2.6 Review of User Access Rights

Information Owners and IT Asset Managers are responsible for maintaining access control lists for the information assets in their areas and must conduct annual reviews of access rights to ensure authorizations are current and valid.

IT 5006.3 User Responsibilities

Users of Duke Energy information systems must be made aware of and accept certain responsibilities for the security of Duke Energy information assets.

IT 5006.3.1 Unattended User Equipment

Unattended equipment must be secured to prevent unauthorized individuals from using another user's credentials or equipment. The following conditions apply:

a) User Action

Users must do the following when leaving workstations unattended:

- Enable Windows security lock (Press: CTRL + ALT + DELETE), or log off.
- Physically secure the workstation.
- Common area workstations must be logged off at the end of each user session.

b) Equipment Configuration

The following conditions apply to equipment configuration:

- Workstations and servers, not located in a processing facility, must be configured with a password protected screen saver.
- The screen saver must require the entry of a password after ten minutes of inactivity.
- Workstations and servers that cannot utilize screen savers must automatically log users off after 10 minutes of inactivity.
- Workstations and servers must be configured to ensure that patches, antivirus, and other updates can be maintained at current levels.

IT 5006.4 Network Access Control

To protect Duke Energy information assets, approved authentication techniques, isolated networks, and restricted user access controls must be implemented.

IT 5006 – Access Control

IT 5006.4.1 Use of Network

The use of Duke Energy's networks requires a valid business need and authorization, and must be restricted to only those assets necessary to meet the business need.

IT 5006.4.2 User Authentication for External Connections

External connections must be authenticated at the perimeter prior to accessing Duke Energy networks, using at least two of the three authentication factors below:

1. Something known; Password or PIN number.
2. In possession of: Smartcard or key fob.
3. Physical attribute: fingerprint or retina pattern.

IT 5006.4.3 Equipment Identification in Networks

Information assets accessible by external parties must not reveal unnecessary information about the operating systems, applications, access controls, or IP addresses. For example, an Internet user connecting to a server must not be able to identify the IP address, operating system used or its version number.

Equipment names must not contain enticement information, i.e., don't have "tax" in the host name of a server containing tax information.

IT 5006.4.4 Network Isolation

Networks must be physically or logically isolated to protect Duke Energy's assets from internal and external threats. Corporate IT Strategy and Compliance must conduct a risk assessment on all networks before they can be connected to the Duke common network. Networks that are not configured and maintained exclusively for Duke Energy are considered external or third party networks and must be isolated from Duke Energy networks. Computers must not be connected to more than one isolated network simultaneously. The following conditions apply:

a) Internal Network Isolation - Network owners are responsible for maintaining their network risk profile and notifying Corporate IT Strategy and Compliance prior to making changes that could impact the common network. Corporate IT Strategy and Compliance may require internal networks that present a higher risk profile than the common network, as measured against the IT 5000 Series, to be physically or logically isolated. For more information, see "IT 5006.5.1 Screening or Filtering Devices".

b) Perimeter Networks – Perimeter networks must only be used for business activities and must use a screened subnet architecture approved by Corporate IT Strategy and Compliance. Perimeter devices must be physically secured, with access limited to groups supporting the devices. Logical access to network devices must be limited to approved individuals.

c) External Network Isolation - Corporate IT Strategy and Compliance must review proposed connections to external sources prior to implementation. Screening or filtering devices must be maintained between Duke Energy networks and connections with external sources.

d) Third Party Networks - Information assets owned and administered by external entities over public, i.e., Internet or private networks that are located on a Duke Energy Network must reside in a perimeter subnet and must be isolated from Duke Energy assets.

e) Trust Relationships – must not be established between Duke Energy information assets and those owned or managed, in whole or in part, by a third party. Trust relationships are prohibited between internal information assets and assets located on a perimeter network.

IT 5006.5 Network Connection Control

Connections between isolated networks must be configured and managed to ensure the integrity of the risk profile of the common network.

IT 5006.5.1 Screening or Filtering Devices

Screening routers or firewalls must be used to isolate networks and must be configured and maintained by individuals or groups authorized by Corporate IT Strategy and Compliance. Screening routers or firewalls must be configured as follows:

a) Block all but authorized protocols and services.

b) Block unauthorized communications.

c) Block external connections that appear to be coming from internal addresses.

d) Configure perimeter devices to prohibit the exposure of internal network addresses or topology.

IT 5006.5.2 Remote Access Software

Remote access software, i.e., Microsoft Terminal Server, NetOps, XWindows, and PC Anywhere v8 or greater, to company networks must utilize an authentication mechanism. This authentication mechanism must be approved by Corporate IT Strategy and Compliance.

IT 5006.5.3 Outbound Connections

Outbound connections are connections that begin inside a Duke Energy network and terminate in or beyond Duke Energy's perimeter network.

IT 5006.5.3.1 Internet Connections

Internet connections are those points where connectivity exists between a Duke Energy network and the Internet. The following conditions apply to internet connections:

a) Connection points must terminate in the perimeter network.

b) Outbound VPN connections to Non-Duke Energy entities are not allowed from inside a Duke Energy network.

c) In cases where business needs require internet access from the internal network using Non-Duke Energy equipment, an isolated connection point can be requested. At a minimum, the following conditions apply to isolated internet connections:

- The connection must isolate and prevent access to Duke Energy Information assets, other than those required to complete the connection.
- Isolated connections must be implemented by individuals or groups authorized by IT Strategy and Compliance.
- The Duke Energy Sponsor must ensure that there is no simultaneous connectivity between the Duke Energy internal network and the isolated connection by wireless or network cabling mechanisms.

IT 5006.5.4 Inbound Connections

An Inbound connection is a connection that begins outside of the Duke Energy network and terminates inside of the perimeter network. The following conditions apply to inbound connections:

IT 5006.5.4.1 Internet Connections

Internet connections are intended to provide public access to Duke Energy information such as the Duke Energy web pages. See "IT 5006-02 Electronic Commerce Services" for additional information.

IT 5006.5.4.2 Inbound VPN

VPN connections must terminate in a subnet on the perimeter network configured for handling VPN traffic.

a) Employee - Employee VPN connectivity to the Duke Energy network:

- Is only allowed using Duke Energy owned equipment with an approved VPN client and software firewall.
- Must be authorized through the Duke Energy Enrollment Process. Use the "Employee Remote Access Request" form located in the Electronic Forms Repository to initiate the enrollment process.

b) Site-to-Site - VPN gateway-to-gateway connections may be used between Duke Energy offices. These connections must be configured by individuals or groups authorized by IT Strategy and Compliance.

IT 5006.5.4.3 Dial-In

Dial-in access to company information assets must be restricted to a centrally administered infrastructure that must terminate in the perimeter network is be configured for handling and monitoring dial-in traffic. The following conditions apply:

a) Employee - Employee dial-in connectivity to Duke Energy networks is only allowed through the controls established in Remote Access Services. Employee dial-in access must be authorized through the Duke Energy enrollment process. Direct modem connections that allow approved employee access to an individual information asset for maintenance must only be active during the maintenance session. When the session is complete, the line or modem must be disabled. For additional information, see "IT 5500, Network Connections".

b) System Support - Dial-in access to networking devices with directly connected modems in remote locations must be restricted to personnel who support such devices directly. These devices must be secured in the following manner:

- A modem password must be enabled.
- A password or authentication mechanism must be enabled to log in to the router and read, write, change, or delete information.
- A password or authentication mechanism must be enabled to change router configuration parameters and traffic filters.

IT 5006.6 Network Routing Control

Network routing controls must be implemented to ensure information assets are not compromised. At a minimum, the following conditions apply:

- Only approved protocols and services needed for legitimate and authorized business purposes are allowed
- Network addresses and address schemes must be hidden from external sources
- Network traffic must be restricted to support approved business and must be monitored.
- Anonymous connections to information systems are not allowed.

IT 5006.7 Operating System Access Control

Computer operating systems must be configured to restrict access to authorized users, must restrict access rights based on user privileges. System security event logs must be maintained and monitored, see "IT 5005.8 Monitoring".

IT 5006.7.1 Secure Logon Procedures

The identification of a Duke Energy network, location, information system, application, or host-specific information must not appear until after a successful log in.

IT 5006.7.2 User Identification and Authentication

An account used for operating system access must uniquely identify the account owner and meet the requirements for privileged access.

IT 5006.8 Mobile Computing and Teleworking

Computing resources used outside of the physical and logical perimeters of Duke Energy are at much higher risk than those used internally. Systems connecting to Duke Energy's networks from external locations must enforce access security controls in order to mitigate the risks associated with remote access.

IT 5006.8.1 Mobile Computing and Communications

Confidential information contained on portable devices must be secured. Users must be aware of their environment and be cognitive of sensitive information while working in a public area. They must take precautions

to avoid the viewing of sensitive information by unauthorized individuals, and must refrain from working with non-public information in a public area.

A Duke Energy approved personal firewall must be enabled while Duke Energy owned equipment is connected to a Non-Duke Energy network, or a network outside of a Duke Energy facility. See section "IT 5006.4 Network Access Control" for additional information.

IT 5007 – Information Systems Acquisition, Development, and Maintenance

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date: 05/01/2006
Revision Date:
Revision No:

Statement of Purpose

This standard establishes the information security requirements for system acquisition, development and maintenance. This standard applies to both in-house and purchased Duke Energy information systems.

IT 5007.1 Security Requirements of Information Systems

Information Security must be an integral component of the purchase, design, development, and implementation process for any new information system or existing systems undergoing a major upgrade. When creating the business case security requirements must be documented and modified as needed throughout the System Development Life Cycle (SDLC).

IT 5007.1.1 Security Requirements Analysis and Specification

Information System Owners must conduct a risk assessment to establish the scope and magnitude of risks associated with any new information system or existing system undergoing a major upgrade. A security representative (Corporate IT Strategy and Compliance, BUISF or ISC) must be consulted to evaluate the system security architecture, review the risk assessment, and consult on the security design. The Information System Owner must develop steps required to eliminate, mitigate, or accept any identified security risks and obtain the appropriate approval signatures prior to system implementation

IT 5007.1.1.1 Secure Application Development

Applications must adhere to the requirements defined in the Enterprise Wide Technology Architecture (EWTA) and be coded in a network-aware manner to secure the access and transmission of information. "IT 5007-01 Application Development Security" defines the minimum requirements for secure application development.

IT 5007.1.1.2 Externally Facing Applications

Applications with externally facing components or services (those that generate or receive network traffic from or to Non-Duke Energy networks), must reside in a DMZ, and must adhere to the requirements defined in sections "5007.1.1.1 Secure Application Development", and "5005.7 Electronic Commerce Services". Examples include the Internet, Application Service Providers (ASP's), etc. The following conditions apply:

a) Communications through a DMZ must be secured to ensure information confidentiality and integrity.

b) Applications must not reveal operational or infrastructure information to the end user.

IT 5007 – Information Systems Acquisition, Development, and Maintenance

IT 5007.2 Correct Processing in Applications

Controls must be designed into applications to protect information assets from mistakes, errors, and unauthorized activities. For additional information, see "IT 5007-01 IT Application Development Security".

IT 5007.2.1 Authentication and Authorization

Applications must incorporate approved controls that provide for secure authentication and valid authorization. Controls include:

a) Authentication performed at the outermost user interface (i.e., presentation layer) and prior to the execution of business logic.

b) Maintaining password confidentiality.

c) Role-based authorization.

IT 5007.2.2 Input Data Validation

Input controls must be incorporated that can validate data, prevent undesirable results, and warn of unauthorized activity.

IT 5007.3 Cryptographic Controls

Cryptographic controls are used to protect the confidentiality and integrity of information and systems. The use of strong key management techniques enhances the security of cryptographic controls.

IT 5007.3.1 Use of Cryptographic Controls

Information with a security classification of confidential must not be transmitted over public networks unless protected by encryption. For information about the proper handling of e-mail communications, see "IT 5002 Asset Management: Acceptable Use of Assets-Mail". Corporate IT Strategy and Compliance must approve encryption methods employed by Duke Energy. Encryption levels must be established at a minimum of 128 bits.

IT 5007.4 Security of System Files

Unauthorized access to system files and application source code must be prevented. System files and software must be thoroughly tested from the development and quality assurance stages into the production environment. Production information used in test or development environments must have the same level of control applied as in production.

IT 5007.4.1 Access Control to Program Source Code

Deploying the source code and software development kit (SDK) to the client is prohibited, i.e., do not include Java source code in JAR files—only deploy the executable files and libraries. Deploying source code to servers is permissible, i.e., ASP files for web servers.

IT 5007 – Information Systems Acquisition, Development, and Maintenance

IT 5007.5 Security in Development and Support Processes

The development, test, and support environments must be strictly controlled and application managers must be responsible for the security of these environments and the review of proposed system changes.

IT 5007.5.1 Change Control Procedures

The Business Unit must ensure changes to information systems are managed through an enterprise or BUISF approved change management process. For change control requirements see "IT 5005.1.2 Change Management".

IT 5007.5.2 Purchased Software

Purchased software, commercial off the shelf or proprietary, must comply with the requirements of the IT 5000 Series. Purchasing agreements or contracts must define security requirements and compliance expectations. For more information, see "IT 5005.2 Third Party Service Delivery Management".

IT 5007.6 Technical Vulnerability Management

Technical Vulnerability Management processes must be implemented to ensure adequate controls are in place to protect against published threat mechanisms. The following conditions apply:

IT 5007.6.1 Control of Technical Vulnerabilities

The Information Sponsor is responsible for ensuring that information systems have a process for controlling technical vulnerabilities. Information systems not covered by an Enterprise Infrastructure Vulnerability Management process must be covered by a locally developed and managed process, in either case, the processes must contain the following components:

a) A current inventory of information systems in accordance with "IT 5002 Asset Management".

b) Subscriptions to vulnerability alert services for vulnerability notification and general risk assessment.

c) A methodology for assessing and ranking the risk to Duke Energy based on applicability and severity. For additional information, see "IT 5007-02 Vulnerability Alert Ranking".

d) Remediation processes must include:

- notification of key personnel
- actions required to remediate
- remediation timeline
- remediation tracking

e) History of vulnerability alerts to include remediation strategy and results. Retention period must be compliant with Records Management Policy.

IT 5007.6.2 Enterprise Infrastructure Vulnerability Management

An enterprise infrastructure vulnerability management process must be centrally managed to ensure a consistent approach to vulnerabilities. Remediation actions are the responsibly of the personnel who support the information asset. Corporate IT Security Operations must assign target remediation dates for alerts assigned high or critical

rankings. The management of personnel supporting the information systems must assign target remediation dates for alerts assigned medium and low rankings.

IT 5007.6.2.1 Corporate IT Security Operations Responsibilities

a) Maintain subscriptions to security vulnerability alert services for key infrastructure elements including but not limited to:

- UNIX (i.e. Linux, AIX, Solaris)
- Windows (i.e. 2000, 2003, XP)
- Web services (i.e. IIS, Websphere)
- Network Devices (i.e. routers, firewalls)
- Databases (i.e. Oracle, SQL Server)

b) Conduct a Duke Energy specific vulnerability risk assessment, assign an impact ranking, and develop a remediation strategy.

c) Notify information system administrators about pertinent vulnerability alerts, impact ranking, and remediation strategy.

d) Track remediation progress on key vulnerabilities.

e) Maintain history.

IT 5007.6.2.2 Support Personnel Responsibilities

a) When notified of vulnerability, support personnel must assess their operating environments to determine if there is an impact, and if there is, must comply with remediation strategy as defined by Security Operations.

b) IT personnel supporting applications and systems are responsible for monitoring vendor sites for security alerts and updates for those applications and operating systems they support. Alerts not previously distributed by Corporate IT Security Operations must be evaluated for applicability and ranked by severity, using the guidelines in "IT 5007-02 Vulnerability Alert Rankings". Corporate IT Security Operations must be notified via the CIRT mail-in database of any alerts ranked either High or Critical, including justification for the ranking.

c) Report implementation progress to Corporate IT Security Operations.

IT 5008 – Information Security Incident Management

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date: 05/01/2006
Revision Date:
Revision No:

Statement of Purpose

This standard establishes the requirements for reporting, responding to, investigating, and prosecuting information security incidents or events.

IT 5008.1 Reporting Information Security Events and Weaknesses

The workforce must be made aware of their responsibilities to report information security weaknesses, incidents, and suspicious activities. Proper channels and procedures must be defined to ensure quick recognition and resolution of security issues.

IT 5008.1.1 Reporting Information Security Events

Suspicious information security activity must be reported to the Computer Incident Response Team (CIRT). Users are to contact the Help Desk at 704-382-7762 (704-382 SPOC) and open a Remedy ticket to the 4ITINTRUSION group whenever an information security event is suspected.

IT 5008.1.2 Reporting Information Security Weaknesses

When a security weakness is suspected or discovered, Users are to contact one of the following:

a) Manager
b) IT Support
c) Business Unit CIRT Coordinators (See IT Security Page on Portal for contact information)
d) Help Desk at 704-382-7762 (704-382 SPOC)

IT 5008.2 Management of Information Security Incidents and Improvements

An enterprise "Computer Incident Response Team" (CIRT) must be maintained to facilitate a coordinated response to security events. The CIRT Team has the authority to investigate all security events or suspicious activity that may impact an information asset.

IT 5008.2.1 Responsibilities and Procedures

Corporate IT Security Operations is responsible for the management and maintenance of the CIRT process and associated procedures. The CIRT team must be centrally managed and consist of personnel from the Business Units for local support.

IT 5008 – Information Security Incident Management

The CIRT procedure must identify an individual to serve as the CIRT Head responsible for coordinating enterprise security incident investigations and post-incident reporting. Local CIRT Leaders or Coordinators must be assigned within the Business Units to manage localized incidents and to coordinate enterprise incidents. In addition subject matter experts (SME's) must be available to provide technical expertise and remedial actions. The CIRT Team must be positioned to respond 24 hours a day. For detailed procedures, see "IT 5008-01 Computer Incident Response".

The CIRT procedure must define methodologies for:

a) Formal incident reporting
b) Response and escalation
c) Restoration
d) Post-incident analysis and reporting
e) Lessons learned and process improvement

IT 5009 – Business Continuity Management

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date: 05/01/2006
Revision Date:
Revision No:

Statement of Purpose

The purpose of this standard is to establish that departmental Business Continuity Plan's (BCP's) must address Information Security.

See also: Enterprise Policies/Risk Management/Business Continuity Crisis Management Policy.

IT 5009.1 Information Security Aspects

In the event of major system failures, significant business interruptions, or catastrophic events information security controls may not be effective or may be circumvented. Restoration of security controls must be an integral component in the design and implementation of Disaster Recovery or Business Continuity plans.

IT 5009.2 Responsibilities of Business Units

Business Unit BCP's must address the following:

a) Role definition and responsibilities of security personnel.

b) Contingencies for continued operations in the event that a CIRT event makes information resources unavailable.

c) Risk assessment

d) Planning framework

e) Testing, maintaining, and re-assessing continuity plans.

f) The structure processes, and accountabilities needed to mitigate the impact of workforce stoppage.

IT 5010 – Compliance

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date: 05/01/2006
Revision Date:
Revision No:

Statement of Purpose

This standard establishes the design, monitoring, and enforcement requirements for information security compliance as it relates to federal, state, local, and regulatory laws and company information security policies.

5010.1 Compliance with Legal Requirements

The Duke Energy workforce must adhere to the requirements specified by federal, state, local, and regulatory laws, and company policies.

5010.1.1 Applicable Legislation

The Information Sponsor must ensure that the information and information systems within their area of responsibility are compliant with the following and for establishing compliance processes when enterprise compliance processes are not applicable.

a) Laws - federal, state, and local laws are dependant on the location and type of business. The Information Sponsor is responsible for establishing a knowledge center of applicable laws that impact their information systems

b) Regulatory - Corporate IT Strategy and Compliance must maintain a list of applicable federal and industry related information security regulations. The Information Sponsor is responsible for ensuring there are standards and procedures for meeting and maintaining compliance to these requirements.

c) IT 5000 Series – Corporate IT Strategy and Compliance is responsible for maintaining the IT 5000 Series documents and for communicating requirements, maintaining and executing an enterprise compliance program, and facilitating the enforcement processes.

d) Information System Contracts – contracts for information system services or products must be reviewed to ensure that security concerns have been addressed. For more information, see "IT 5005.2.1.1 Application Service Providers".

IT 5010 – Compliance

IT 5010.1.2 Intellectual Property Rights (IPR)

For specific information about Intellectual Property and Brand Management, see the "Code of Business Ethics".

IT 5010.1.3 Information Protection and Privacy of Personal Information

See Enterprise Policies \ Law Department \ Personal Information Privacy Policy for details.

IT 5010.1.4 Prevention of Misuse of Information Processing Facilities

The use of Duke Energy information or information assets is only allowed for authorized activities. Duke Energy must have, at a minimum, read-only access to any information on a workstation or server and reserves the right to monitor, restrict, prevent, or revoke the use of its information or information assets. The unauthorized access, use, or modification of information or an information asset is subject to criminal penalties and civil liability.

IT 5010.1.4.1 Employee Monitoring

Requests to investigate suspected inappropriate employee activity must be coordinated through HR, Legal, and/or Corporate Compliance. To support requests to perform investigations, the investigative teams must be able to obtain read access to information on workstations and/or servers. Security operations must coordinate with the IT Security representative for the Business Unit to obtain the necessary access on an ongoing or as-needed basis.

IT 5010.1.4.2 Employee Notification

Servers and workstations must be configured in a way that ensures Users acknowledge their permitted access and the potential for monitoring. During the initial configuration a login banner is required that includes the following:

a) Only authorized users may use the information system.

b) By continuing to use the information system, the user agrees they are an authorized user.

c) Use of the information system constitutes consent to monitoring.

IT 5010.2 Compliance with Policies and Standards and Technical Compliance

The Information Sponsor has the accountability for ensuring information systems within their area of responsibility are compliant with the federal, state, local, and regulatory laws and company policies. Enforcement or lack of enforcement, by Corporate IT Strategy and Compliance or other governing body, is not an indication of acceptance of a non-compliance practice.

IT 5010.2.1 Compliance with Policies and Standards

The IT Compliance Program must address the roles, responsibilities, and processes for assessing, documenting, and measuring compliance. The program must define how to measure compliance and how to track, note, and solve gaps. All members of the workforce are required to support the compliance program by allocating the necessary resources to participate as requested.

Information Sponsors are responsible for ensuring non-compliant issues are resolved.

IT 5010 – Compliance

IT 5010.2.2 Security Standards Exception

An IT Security Standards Exception Request form must be processed for exceptions to IT 5000 Standards and Procedures. This form is located in the Electronic Forms Repository. For specific process details, see "IT 5010-01 Standards Exception Procedure".

The Duke Energy Policy Exception and Risk Acceptance procedure defines the authorization process for requesting exceptions to an IT Security Policy.

IT 5010.2.3 Technical Compliance Checking

Corporate IT Strategy and Compliance must conduct technical reviews of Duke Energy's security portfolio. Deficiencies are to be reported to the appropriate Managers. Managers to submit remediation plans as determined by the compliance program. The results of the technical review and the remediation steps are not to be shared with anyone one that does not have a need-to-know status.

a) Network Penetration Testing/Assessment - Corporate IT Strategy and Compliance must conduct an annual penetration test to assess the vulnerability of the company's network perimeter devices.

b) Server Scans/Vulnerability Testing/Assessment - Corporate IT Strategy and Compliance must conduct an annual server scan/vulnerability test on each server to assess the server's ongoing security patch readiness and security configuration.

IT 5010.3 Information Systems Audit Considerations

Auditing information systems must be effective and thorough but minimally impact systems operations. Controls must be in place to ensure that only authorized resources use system audit tools and that they use them properly.

Glossary of Terms

A

Access Account – an identifier (ID) and password, or other authentication mechanism, combination.

Access Control – mechanisms to protect information from accidental or malicious modification, destruction, or disclosure. Some typical access controls are permissions such as:

No Access – overrides other access privilege

List – view the contents of a folder

Read – view a file

Add – copy a new file to a folder

Change – modify the contents or overwrite a file

Full Control – change plus modify permissions or auditing on a file or folder

Access Control List (ACL) – a list of users with access to information and their rights to manipulate it, i.e., list, read, add, change, etc.

Application Software – a computer program, or set of programs, designed to carry out a specialized task(s).

Attack – the act of trying to bypass security controls on a system or a method of breaking the integrity of encrypted information. An attack may be active, resulting in the alteration of information; or passive, resulting in the release of information.

Authentication – verifying the identity, and establishing the eligibility of a workstation, originator, or individual to access specific information. It is providing assurance regarding the identity of a subject or object, for example, ensuring that a particular user is who he or she claims to be.

Authorization – the privilege granted to an individual to access information based on the individual's clearance and need-to-know; the granting to a user, program, or process, the right of access.

B

Backup – copying information to a second media as a precaution against information loss in case the first media fails.

Backup Media – the material used to store backup information, i.e., CD-ROM, Magnetic Tape, Floppy Disk, etc.

Broadband – a high speed transmission method that uses DSL (Digital Subscriber Line) or cable modem to provide Internet connectivity.

Business Unit Information Security Function (BUISF) – in a Business Unit, an individual who or group that provides Business Unit coordination with Corporate IT Strategy and Compliance on issues concerning functional implementation of the IT 5000 Series documents.

Business Partner – an individual or company who is involved with Duke Energy for the purpose of achieving a business objective.

C

Chief Information Officer (CIO) – senior strategic-level management position that oversees all information technology systems and personnel.

Classification (Information Protection) – a determination that information requires a specific degree of protection against unauthorized disclosure combined with a designation that signifies such a determination has been made.

Glossary of Terms

Commercial off the Shelf (COTS) – Commercially manufactured Information systems or software; this includes both plug and play and customizable products.

Common Network – Networks or subnets configured and maintained by Duke Energy where all devices are maintained using a common set of security practices.

Complex Passwords – passwords that have at least three of the following four characteristics:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters, i.e. "!, @, #, $, %, ^, &, *, and +"

Note: For MVS/Mainframe, only the following symbols are allowed: "@, #, and $"

Computer Incident Response Team (CIRT) – a selected group of people whose purpose is to promptly respond to an information security incident so that it can be quickly contained, investigated, and recovered from. This term is also used to describe the procedures and processes used by this team.

Controlled Environment – an area where special processing (such as fingerprinting, background checks, etc.) is required to gain authorization for access. Controlled environments have additional physical security features protecting them.

Custodian - Subject Matter Expert (SME) in a particular area.

D

Data – textual or numeric, human-readable information.

Degaussing – the action or process of destroying information so it cannot be recreated, propagated, or reused.

Digital Certificate – an electronic document that links a user or computer with a public and private key pair that can be used for encryption, authentication, non-repudiation, etc

Digital Signature – information that is encrypted with an entity private key, and appended to a message that identifies and authenticates the sender and the integrity of the information.

Direct Modem Connection – a modem connected directly to a server or workstation therefore bypassing the centrally administered modem banks.

DMZ (Demilitarized Zone) – a subnet that provides a means of securely hosting computing services accessible to external entities, utilizing screening devices, firewalls, and other security controls.

E

Encryption – the process of transforming information to an unintelligible form for secure transmission.

Enterprise – the total collection of all businesses or endeavors operating under the ownership or control of Duke Energy.

Extranet – an Internet technology used to connect two or more computers together. See also: Intranet.

External Networks –Networks or subnets that are not configured and maintained by Duke Energy.

F

File Transfer Protocol (FTP) – a means to exchange files across a network.

Glossary of Terms

Firewall – a specialized computer or software designed to protect networks by filtering and blocking access.

H

Hypertext Transfer Protocol (HTTP) – the native protocol of the Web, used to transfer hypertext documents on the Internet.

I

ID (or login account) – in general, an information asset logon identifier or account. Specific kinds include:

Information – data that is electronically processed, stored, or transmitted.

Information Attributes – the value, sensitivity, legal, regulatory, or retention requirements, and risk of loss or compromise, etc. that the company places on information.

Information Asset – Information or Information technology that provides value to Duke Energy.

Information Owner – a Duke Energy employee in a management position, responsible for securing designated information for the purposes of protecting confidentiality, integrity, and availability.

Information Sponsor – a Duke Energy vice president or Business Unit manager responsible for maintaining the confidentiality, integrity, and availability of company information within their Business Unit.

Information System – an Information Asset or combination of Information Assets designed to address a business requirement.

Information Technology – Any equipment or subsystem of equipment or electronic medium, that is used to store, process, transmit, or present information. Computers, electronic storage, software, or data communication networks are considered information technologies.

Information Technology Manager - A Duke Energy employee in a management position responsible for the functional operation of a specific information technology. The Information Technology Manager may or may not have fiscal responsibilities for the asset.

Instant Messaging – a computer conference using the keyboard, or voice (a keyboard chat) between two or more people.

Internet – an insecure, worldwide public collection of networks that use TCP/IP protocol suite for communication.

Internal Network – a general term that defines networks that are supported and maintained by Duke Energy which are isolated from Non-Duke networks.

Intranet – a network within an organization for secure communications between employees, or other intranets outside of the organization. It is a private, TCP/IP-based network that uses Internet technology, but is not accessible to the public.

L

Labeling – a visible sign designating the classification of the information.

Logically Isolated System – a computerized system that is physically connected however, traffic between networks must pass through screening or filtering equipment that restricts the flow of information across the boundary of the isolated systems.

M

Major upgrades – significant enhancements or modifications to an information system in terms of scope, impact and costs that require Business Units to use discretion when determining which upgrades are major and which are not. IT Security should be consulted if there is any doubt.

Glossary of Terms

Malicious Code – hardware, software, or firmware that is intentionally included in a system for the purpose of causing loss or harm.

Manager – Organizational position with job responsibilities that require a level of experience and accountability that identifies them as Subject Matter Experts (SME's) in a particular area and; may include administrative or operational management of people.

Monitoring Software – Software that monitors an information system and records activities or alarms.

Multifactor Authentication – the use of two or more factors to authenticate that someone is who they claim to be. The three factors are: something known, i.e., passwords, PIN; something in possession of, i.e., tokens, smartcards; or a physical attribute of the person (biometric), i.e., fingerprints, retinal scan.

N

Need-to-know – a principle that allows for the compartmentalization of information in order to restrict access. An individual is provided with the information that is necessary to complete a given task and nothing more.

Network - two or more information assets configured to share resources.

Network connection – an access point to an information asset.

O

Operating System – the principal system software that manages the hardware, program files, and other system resources and provides a systematic and consistent means for controlling the computer.

Owner – an individual who has the responsibility for controlling the production, development, maintenance, use, and security of an information asset.

P

Packet – a unit of information sent across a network.

Peer to Peer – file sharing network that permits direct access to multiple user resources.

Perimeter Asset – Information Asset or System that contributes to the transportation of information between internal and external sources. These consist of applications, servers, workstations, and network infrastructure devices such as firewalls, routers, dial-in servers, intrusion detection devices, and VPN gateways.

Perimeter Network – screened subnet architecture approved by Corporate IT Security. Utilizes physically secured devices, with access limited to groups supporting the devices. Logical access is limited to approved individuals only.

Processing Facilities – data centers, server or telecommunication rooms, or closets containing wiring or communications equipment.

Physically Isolated System – a computerized system that is not physically connected to the Duke Energy computer network, the Internet, or another third party network. Physical connection includes computer networks, modems, or an interface to a telephone system. The use of broadcast wireless technology (radio, infrared, or any means of electromagnetic frequency) precludes a system from meeting this definition.

Policy – high-level statement of enterprise beliefs, goals, or courses of action adopted in support of principles and objectives. Policies provide a statement of position or intent in a specific subject area.

Portable Device – an information asset that is used for mobile computing. The device is typically small and easily transportable, i.e., PDA, laptop computers, pocket computers, smart phones, and storage media.

Procedure – the specific actions required to be compliant with the IT Security Standards. They are documented, step-by-step instructions for a particular area and may exist at any level of the organization.

Glossary of Terms

R

Records – *information on a particular subject collected and preserved.*

Recovery – the process of restoring information from backup.

Remote Control Software – software that facilitates the remote control or remote access to another computer system.

Risk – the likelihood that vulnerability may be exploited or that a threat may become harmful. The probability that an undesirable event may occur that results in financial or other loss, or otherwise creates a problem.

Router – a device that interconnects networks.

S

Screening Router – a router that is configured to implement part of the firewall security by permitting or denying traffic at a network level.

Security Event – an anomaly or indicator of a potential security problem.

Security Incident – a security event or events that have been evaluated and require action.

Security Weakness – a deficiency that could be exploited.

Senior Management – management at the vice president level and above.

Separation of Duties – a control that prevents an individual from having total control of information entry and validation, which would enable that person to enter or conceal an error that is intended to defraud the company.

Server – typically a more powerful computer than a PC that is dedicated to providing services such as file and print sharing, etc.

Server/Telecommunications Room – a room containing several servers and/or telecommunications equipment. The room is not manned and environmental and fire suppression controls may or may not be in place.

Simple Network Management Protocol (SNMP) – a standard network management protocol enabling communication and control with SNMP agents within networked devices.

Software – instructions that tell a computer what to do. Unless otherwise stated, Software comprises the entire set of programs, procedures, and routines (Operating System, application software, and middleware) associated with the operation of an information system.

Sponsor – an individual who is responsible for the activities or work efforts provided by a vendor, contractor, or consultant; or, an individual responsible for the implementation or management of a specific business need. Generally, a Sponsor is a Duke Energy employee.

Standard – mandatory rules or regulations that define the minimally acceptable practices for achieving the objectives of the IT Security Policy.

T

Telnet – standard internet protocol for accessing remote systems.

Third Party – someone other than the principal parties who are involved in a transaction.

Threat – a circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of information, denial of service, or any combination thereof.

Trust Relationships – relationship between two systems or domains where an authenticated user on one system is automatically authenticated to the other.

Glossary of Terms

Two-factor Authentication – authentication that uses at least two of the three Multifactor Authentication mechanisms.

U

User ID – assigned to a specific individual who is accountable for its use; sometimes referred to as a LAN ID in a Windows domain.

V

Virus – a computer program that replicates by attaching copies to existing programs. Computer programs that can infect, replicate, and spread among computer systems. A virus requires human involvement to propagate.

Virtual Private Network (VPN) – a network used for highly confidential information transmission. It is an encrypted IP connection between two sites over the Internet.

Vulnerability – a weakness in computer information systems that could be exploited by gaining unauthorized access to information, disrupting critical processing, or violating a system security policy.

W

Workforce Identification Process (WIP) – establishes the Human Resources Management System as the Enterprise system of record for establishing and maintaining employee identity.

Workforce – company employees, joint ventures, partnerships, subsidiaries, contractors, vendors, and agents.

Workstation – a computer with a primary purpose to provide access to networks and applications directly to the end-user.

Exhibit IT-5

SCADA Cyber Security Policy and Standards

IT 6000 SERIES

PROVISIONAL EDITION

March 31, 2006

IT 6000 – SCADA Cyber Security Policy

IT 6000 Series – SCADA Cyber Security Standards

This governance document is comprised of the IT 6000 Cyber Security Policy and supporting Standards and Procedures. This document is associated with Duke Energy Information Technology Security Policy and Standards, (the "IT 5000 Series"). This document incorporates integrated information security practices established as a result of the merger of Duke Energy and Cinergy..

The format of this document is based on and aligns with NERC CIP Cyber Security Standards[1]--however it contains two additional scope-defining sections not found in the NERC format:

1. Enterprise - the "Enterprise" section denotes associated requirements that are applicable to any and all SCADA systems, irregardless of additional Business Unit or more specific regulatory requirements. This section specifies the minimum security controls that the entire company will meet to protect its SCADA systems. Enterprise requirements are denoted in bold and designated by an "**R9.9.9**" format (as established by NERC CIP format). Requirements that address material beyond the scope of the NERC format, but still applicable to Duke Energy are designated by a "**DR**" prefix. Enterprise requirements for "Critical Infrastructure" systems are shaded, and are not required for "Operational" systems.
2. Business Unit - the "Business Unit" section describes any additional security controls that may apply to a particular subset of SCADA systems. These additional controls are mandated by the Business Unit for any number of reasons, but primarily to reflect any regulatory requirements on a specific operational part of the Company, but not the Company as a whole. For example, NERC may regulate electric process systems but not gas distribution systems.

(Note: There is no section "6001", as would be logically assumed based on the first section (6000) and the next section (6002). Section 6001, as "6001" is currently used by NERC for a non-cyber-based standard and therefore was excluded from this document.)

[1] http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

IT 6000 – SCADA Cyber Security Policy

Table of Contents

Statement of Purpose **5**
Policy Expectation **5**
6000.1 Supervisory Control and Data Acquisition (SCADA) **5**
6000.2 General SCADA Requirements **6**
6000.3 Examples of a SCADA System **6**
6000.3.2 Functions of SCADA systems include: **7**
6000.4 Roles and Responsibilities **7**
Statement of Purpose **10**
6002.1 SCADA System Protection Classifications **10**
6002.2 Enterprise Requirements **11**
6002.3 Business Unit Requirements **12**
6002.3.1 Business Units Regulated by NERC 12
6002.3.2 Business Units Regulated by NRC 13
Statement of Purpose **14**
6003.1 Enterprise Requirements **14**
6003.2 Business Unit Requirements **17**
6003.2.1 Business Units Regulated by NERC 17
6003.2.2 Business Units Regulated by NRC 18
Statement of Purpose **19**
6004.1 Corporate Requirements **19**
6004.2 Business Unit Requirements **22**
6004.2.1 Business Units Regulated by NERC 22
6004.2.2 Business Units Regulated by NRC 23
Statement of Purpose **24**
6005.1 Corporate Requirements **24**
6005.2 Business Unit Requirements **31**
6005.2.1 Business Units Regulated by NERC 31
6004.2.2 Business Units Regulated by NRC 33
Statement of Purpose **34**
6006.1 Enterprise Requirements **34**
6006.2 Business Unit Requirements **37**
60062.1 Business Units Regulated by NERC 37
6004.2.2 Business Units Regulated by NRC 38
Statement of Purpose **40**
6007.1 Corporate Requirements **40**
6007.2 Business Unit Requirements **47**

IT 6000 – SCADA Cyber Security Policy

6007.2.1 Business Units Regulated by NERC 47
6004.2.2 Business Units Regulated by NRC 49
Statement of Purpose **50**
6008.1 Corporate Requirements **50**
6008.2 Business Unit Requirements **51**
6008.2.1 Business Units Regulated by NERC 51
6008.2.2 Business Units Regulated by NRC 51
Statement of Purpose **53**
6009.1 Corporate Requirements **53**
6009.2 Business Unit Requirements **54**
6009.2.1 Business Units Regulated by NERC 54
Access Controls **55**

IT 6000 – SCADA Cyber Security Policy

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval: Information Technology Management Team (ITMT)

Approval Date:
Revision Date:
Revision No:

Statement of Purpose

The purpose of this policy is to establish guidelines for the protection of information, applications, and systems used, operated, or maintained by Duke Energy that are subject or related to Supervisory Control and Data Acquisition (SCADA), Process Control, or other operational processes that include real-time or similar systems involved in the operation, control, or monitoring of physical assets. These systems will generically be referred to as "SCADA" or "SCADA Systems", and include all of the systems described in this document.

Policy Expectation

This policy applies to the entire Duke Energy workforce, including but not limited to, employees, joint ventures, partnerships, subsidiaries, contractors, vendors, agents and third parties involved in the maintenance or operation of SCADA assets. It is the responsibility of every Duke Energy subsidiary and Business Unit to manage security risks locally and to maintain the security of Enterprise SCADA systems.

This policy applies to all current operational systems and must be applied as part of system requirements to newly purchased or developed systems. All systems must comply to either these policies or with the Information Security Governance Standards, "IT 5000 Series" policy series.

6000.1 Supervisory Control and Data Acquisition (SCADA)

SCADA (Supervisory Control and Data Acquisition) systems are computer systems used to manage industrial production, transmission or distribution processes. SCADA systems are used, for example, to supervise a reactor functioning in a nuclear power plant, to monitor electricity distribution through a high voltage transmission grid, and to control natural gas flow through a pipeline.

IT 6000 – SCADA Cyber Security Policy

6000.2 General SCADA Requirements

General SCADA requirements are defined as follows:

a) The protection of SCADA systems is the responsibility of all Company employees, joint ventures, partnerships, and subsidiaries, as well as contractors, vendors, agents, and third parties.

b) Unless otherwise stated in a Duke Energy privacy statement (or policy) or, unless otherwise prohibited by local law, the Company reserves the right to access, view, copy, change, delete and disclose any information monitored and/or stored by any SCADA system.

c) To the extent required by law, personally identifiable information held by the Company, such as Social Security Numbers, will be kept confidential in accordance with "Personal Information Privacy Policy – DE 7000".

d) Access to SCADA systems will be determined by business need.

e) Access to SCADA data will be determined on a "need-to-know" basis.

f) SCADA systems are valuable Company assets and their accessibility, integrity and availability must be protected in accordance with "IT 6103 SCADA System and Information Classification".

g) All systems must be classified commensurate with their value and in accordance with "IT 6002.1 SCADA System Protection Classification".

h) The integrity, availability, and security of all Company SCADA systems must be maintained through the application of appropriate security, monitoring, quality and access controls, legal and retention requirements, and recovery processes.

i) The CIO has the final authority on all enterprise SCADA cyber security policy and standards.

j) Legislative, regulatory requirements or other legal obligations will supersede any SCADA cyber security policy, and subsequent standards, and procedures, except in cases where Company policy, standards, or procedures require a higher level of security.

k) Personnel accountable for SCADA system protective controls outlined in Company policy, standards, or procedures may be subject to disciplinary actions up to and including termination of employment or contract (Corrective Action - HR 1060) if they are deemed to be non-compliant.

6000.3 Examples of a SCADA System

SCADA systems include, but are not limited to:

a) Plant Control Systems, i.e., Distributed Control Systems (DCS)

b) Energy Management Systems

c) Environmental Monitoring Systems

d) Metering and Physical Status Reporting Systems

IT 6000 – SCADA Cyber Security Policy

6000.3.1 Typical components of SCADA systems:

a) Network (routers, cabling, switches, firewalls, or other telecommunication infrastructure)
b) Servers/SCADA host computers
c) Historical and Real Time Databases
d) HMIs (dedicated and general-purpose)
e) Measurement workstations
f) Data Consolidators or Concentrators
g) Data Gathering and Device Control Equipment, i.e., Field Equipment, I/O, RTUs, PLCs.
h) IP Addressable remote devices
i) Calibration, Testing and Diagnostic Equipment
j) Standalone controllers

6000.3.2 Functions of SCADA systems include:

a) Monitoring or polling
b) Metering/measurement
c) Controlling equipment
d) Human machine interface (HMI))
e) Alarming and/or event notification
f) Event logging, history

6000.4 Roles and Responsibilities

a) Chief Information Officer - The CIO (or designated body) has been assigned the responsibility for the approval of SCADA Cyber Security standards. This office may delegate this responsibility to the Information Technology Management Team (ITMT, or NewCo equivalent).

b) SCADA Cyber Security Council (SCSC) - The SCADA Cyber Security Council is composed of representatives from multiple Business Units with operational interests in SCADA Cyber security. This council will be responsible for:

1. The collaborative maintenance of the Enterprise (or "Corporate") SCADA Cyber Security standards, including review of the SCADA security strategies and architecture,
2. Endorsement of enhanced and additional SCADA security standards,
3. Support of SCADA security initiatives, and
4. Support of SCADA security awareness.

The SCSC will endorse the standards for final approval. The individual representing a Business Unit on the SCSC must also belong to the Business Unit SCADA Cyber Security Function.

c) Business Units - Each Business Unit of Duke Energy will be responsible for compliance with SCADA Cyber Security policy, standards, and procedures. Business Units will designate local resources for accountability where required.

d) Business Unit SCADA Cyber Security Function - Each Business Unit will define a BUSCSF. The Business Unit SCADA Security Function is defined as follows:

1. The primary approval body for Business Unit specific SCADA Cyber Security standards, procedures and processes, which includes the "Business Unit" section of the Enterprise SCADA Cyber Standards.
2. Responsible for providing communications, awareness, and compliance with SCADA Cyber Security standards in the Business Unit.
3. Responsible for identifying requirements and defining Business Unit SCADA Cyber Security standards and procedures.
4. Responsible for reviewing exceptions to SCADA Cyber security standards generated from the Business Unit.
5. Responsible for reviewing SCADA system architecture as it pertains to cyber security.

e) SCADA System Owner (May be technical and/or business)

A SCADA System Owner is a manager or designee(s) responsible for specific SCADA Systems cyber security. A SCADA System Owner has responsibility for securing the designated SCADA System asset(s) for the purposes of protecting accessibility, integrity, and availability. The SCADA System Owner is responsible for:

1. Ensuring their use and access to the SCADA system complies with enterprise and Business Unit SCADA Cyber Security Standards and procedures, and all governmental and regulatory laws and requirements.
2. Data Ownership for the data produced by the SCADA system.
3. Identifying all SCADA assets and components that are under the System Owner's responsibility.
4. Ensuring a change control process for SCADA security is implemented.
5. Reviewing and understanding current Duke Energy enterprise SCADA standards, government regulations and industry standards relating to SCADA System security.
6. Ensuring that security standards and information protection practices employed comply with government and regulatory laws and requirements, and Company policies and standards.
7. Classify, periodically review, and protect the SCADA assets in accordance with "IT 6002.1 SCADA System Protection Classification".
8. Review, document, and control access requests in accordance with "IT 6002.1 SCADA System Protection Classification".

9. Controlling and monitoring physical and cyber access to the SCADA system. This includes ensuring appropriate security controls and processes are in place.
10. Delegating, as necessary, SCADA Development and Support Personnel to assist with ownership responsibilities.
11. Determining SCADA System back-up and recovery requirements.
12. Reporting breeches of security as soon as possible to the appropriate CIRT (see "IT 5008 Computer Incident Response") and any Business Unit specific procedures.

f) SCADA Development or Support Personnel

The SCADA Development or Support Personnel develops or installs, and configures the SCADA application and infrastructure software and hardware. From a cyber security point of view, this role includes the following responsibilities:

1. Ensure SCADA software and infrastructure meets or exceeds the Cyber Security Policy, standards and procedures.
2. Ensure SCADA software and infrastructure meets or exceeds regulatory requirements (including abiding by any local laws having jurisdiction on the system)
3. Ensure that changes to production systems are made only by authorized individuals or groups following the approved change process.
4. Never allow an unauthorized individual access to the SCADA system.

g) SCADA System User

The SCADA System User interfaces with the production SCADA system, i.e., control room operator or dispatcher. This role includes these responsibilities:

1. Using or accessing SCADA systems for authorized purposes and via approved methods only.
2. Ensuring unauthorized individuals do not interact with the SCADA system.

h) Audit Services

Audit Services will review business activities to confirm compliance as part of their normal corporate role and report the results to the ITMT and the responsible Business Unit management.

i) Corporate IT Strategy and Compliance

Corporate IT Strategy and Compliance is responsible for oversight and administration of the Duke Energy Information Security Program.

IT 6002 - Assets

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

This purpose of this standard is to define criteria for the identification and protection of SCADA Systems and to establish the requirements for SCADA system classification. Specifically, this standard addresses the criticality and vulnerability of SCADA assets, and the risks to which they are exposed. All SCADA systems must be classified so they are protected at a level commensurate with their value. This includes raw data, infrastructure, and applications. Additional Business Unit SCADA classifications must be approved by Corporate IT Strategy and Compliance. These classifications can supplement, but not supersede, the enterprise standard.

6002.1 SCADA System Protection Classifications

SCADA systems must be classified based on the system's value to Duke Energy, sensitivity, regulatory requirements, and risk of loss or compromise. Components of a SCADA system can have different classifications, for example, a control room may be classified as "Critical Infrastructure" whereas, a remote field device may be classified as "low risk" if appropriate isolation between the system and the "low risk" device is provided. For all SCADA system classifications, confidentiality or sensitivity of the SCADA system to failure should be a consideration when applying cyber security controls. The following conditions apply:

a) Critical Infrastructure - The system should be classified as "Critical Infrastructure" if the incapacitation or destruction of the SCADA system would have a debilitating impact on national security, national economic security, public health or safety, or any combination of these matters, (Examples: nuclear safety SCADA systems, significant gas and petroleum transportation pipeline SCADA systems, sour gas processing or transportation SCADA systems, and electric grid systems.) Any system designated at this level would encompass the attributes of systems at all other levels. Any system controlling physical access and/or physical monitoring of any facility containing SCADA systems meeting this definition is also designated as "Critical Infrastructure". (For example, physical security systems for nuclear plants, large energy storage facilities, dams are "critical infrastructure".) Any system designated by NERC definition as a "Critical Cyber Asset" must be in this classification.

IT 6002 - Assets

b) Operational - Other SCADA systems critical to the operation and profitability of the company Examples of critical systems might include: steam or hydro generation plants, gas processing plants, gas transmission compressor stations.

6002.2 Enterprise Requirements

All SCADA System Owners must comply with the following requirements:

R1. The SCADA System Owner shall identify and document a risk-based assessment methodology to use to classify all SCADA systems.

R1.1. The SCADA System Owner or Business Unit SCADA Security Function shall maintain documentation describing their risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following:

R1.2.1. Control centers, control rooms, computer rooms, or control complexes (and backup/redundant control centers and complexes) performing the functions of the SCADA system.

R1.2.2. Outlying facilities that support the reliable operation of the SCADA system, i.e., substations, redundant start-up power sources, etc.

R1.2.3. Energy supplies or raw-material sources must be factored, such as generation plants or inbound/outbound pipelines that support the reliable operation of the SCADA system.

R1.2.4. Systems and facilities critical to system restoration, including resources used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic safety sub-systems or system reliability sub-systems, for example, pressure relief valves or load-shedding assets.

R1.2.6. This requirement is not applicable.

R1.2.7. Any additional assets that support the reliable operation of the SCADA system that the System Owner deems appropriate to include in their assessment.

R2. SCADA System Inventory - The SCADA System Owner or Business Unit SCADA Security Function shall develop a list of their SCADA system(s). The SCADA System Owner or Business Unit SCADA Security Function shall review this list at least annually, and update it as necessary. This inventory list shall include at a minimum: Name of System, location(s), purpose, and key contact people.

SCADA System Owners must maintain and periodically review asset (component) inventories of each SCADA system, including the identification and classification of critical assets of the system. The level of detail and period of review should be determined by the criticality of the overall system.

R3. SCADA System Classification - Using the inventory (of systems and assets) developed pursuant to Requirement R2, the SCADA System Owner or Business Unit SCADA Security Function shall assess each system's classification, through a risk-based assessment methodology required in R1. After significant changes to a system the risk-base assessment for classification shall be repeated. The SCADA System Owner or Business Unit SCADA Security Function shall review this list at least annually, and update it as necessary.

IT 6002 - Assets

R3.1. This requirement is not applicable

R3.2. This requirement is not applicable

R3.3. This requirement is not applicable

R4. Annual Approval -A senior manager or delegate(s) shall approve annually the inventory list of SCADA Systems classified as "Critical Infrastructure". Based on Requirements R1, R2, and R3 the SCADA System Owner or Business Unit SCADA Security Function may determine that it has no "Critical Infrastructure" SCADA Systems. The SCADA System Owner or Business Unit SCADA Security Function shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of "Critical Infrastructure" SCADA Systems, even if such lists are null.

DR5. SCADA System Proprietary Devices Exclusion:

PLCs, RTUs, and other field equipment that run a proprietary operating system (as opposed to generic operating systems, that includes Windows, VMS, or any common flavor of Unix (including Linux)), and that do not use IP-based networking are excluded on any corporate SCADA Cyber Security Standards and requirements except those related to physical security, unless otherwise specified.

6002.3 Business Unit Requirements

6002.3.1 Business Units Regulated by NERC

CIP-002 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6002.2 and are noted with "See Enterprise Requirements".

R1. Critical Asset Identification Method - The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

IT 6002 - Assets

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification - the Responsible Entity must develop a list of Critical Assets specific to their area, which must be determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification - using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a Control Center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval - A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets, even if such lists are null.

6002.3.2 Business Units Regulated by NRC

See NSD-804

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6003 – Compliance, Monitoring, and Response

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

The purpose of this standard is to define the minimum controls required to protect Duke Energy SCADA assets. This standard applies to members of the workforce associated with SCADA assets, including, but not limited to, employees, joint ventures, partnerships, and subsidiaries, contractors, vendors, agents and third parties. This standard identifies those persons responsible for establishing compliance measures in their areas of responsibility in advance of enterprise compliance rules which are administered by Corporate IT Strategy and Compliance.

6003.1 Enterprise Requirements

R1. Cyber Security Policy - Corporate IT Strategy and Compliance and the SCSC shall document and implement a SCADA cyber security policy that represents management's commitment and ability to secure its SCADA systems. Corporate IT Strategy and Compliance and the SCSC shall, at minimum, ensure the following:

R1.1. The SCADA cyber security policy addresses the minimum industry best practices, including provision for energy sector specific situations.

R1.2. The SCADA cyber security policy is readily available to all personnel who have access to, or are responsible for, SCADA systems. Company communications that contain non-restricted information on SCADA cyber security training, policy updates, or alerts must be posted on the Corporate IT Strategy and Compliance Website or other public displays to ensure that all users have access to the information.

R1.3. Annual review and approval of the SCADA cyber security policy by Corporate IT Strategy and Compliance and the SCSC must be performed.

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6003 – Compliance, Monitoring, and Response

R2. Leadership/Compliance - Corporate IT Strategy and Compliance has overall responsibility for leading and managing a Standards Compliance Program to ensure enterprise implementation and adherence to the Cyber Security standards.

R2.1. This requirement is not applicable.

R2.2. This requirement is not applicable.

R2.3. The Business Unit SCADA Cyber Security Function and Corporate IT Strategy and Compliance must authorize and document any exception from the requirements of the cyber security policy.

DR2.4. All Business Unit SCADA Cyber Security Function or SCADA System Owners are responsible to respond to requests for information from the compliance program.

DR2.5. It is the responsibility of Corporate IT Strategy and Compliance to execute this compliance program on an ongoing basis and at least annually.

DR2.5.1. This process must create metrics that measure success against meeting the SCADA cyber security standards, gather and validate data from SCADA asset owners, and provide reports to executive management on the results.

DR2.6. Business Unit SCADA Cyber Security Functions or SCADA System Owners are responsible for resolving all identified issues around non-compliance for their responsible systems.

R3. Exceptions - A Standards Exception Request form must be submitted for all exceptions to SCADA Cyber Security Standards and Procedures. For more information, see "IT 5010-01 Standards Exception Procedure", which describes the process for submitting an exception to the IT Security Standards. This procedure must also be followed for SCADA Cyber Security Standards exceptions. Exceptions must be filed for all systems incapable of meeting requirements. Exception forms must be routed to the Business Unit SCADA Cyber Security Function prior to the final review by Corporate IT Strategy and Compliance. When formally executed, the following requirements document the exception process:

R3.1. Once initial reporting or identification of a non-compliance issue occurs, the SCADA System Owner must identify a course of action (exception or remediation) within 30 days. The SCADA System Owner must file the exception form or file a remediation plan within 30 additional days.

R3.2. Documented exceptions to the SCADA cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6003 – Compliance, Monitoring, and Response

R4. Information Protection - SCADA System Owners shall Identify, classify, and protect information processed by and associated with SCADA systems. For SCADA systems classified as "Critical Infrastructure", the additional requirements apply:

R4.1. The information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in SCADA Cyber Security Standard 6002, network topology or similar diagrams, floor plans of computing centers that contain such systems, equipment layouts, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The information should be classified according to IT 5002.5.2 "Security Classifications" (Public, Internal, and Confidential).

R4.3. The Business Unit SCADA Cyber Security Function shall, at least annually, assess adherence to its information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. The level of detail of this assessment is defined by the Business Unit SCADA Cyber Security Function.

R5. Controlling Access to Protected Information - The SCADA System Owner or Business Unit SCADA Cyber Security Function shall document and implement a program for managing access to SCADA system protected information.

The requirements define below are for SCADA systems classified as "Critical Infrastructure".

R5.1. The SCADA System Owner or Business Unit SCADA Cyber Security Function shall maintain a list of designated personnel who are responsible for authorizing electronic or physical access to SCADA system protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to SCADA protected information shall be verified at least annually.

R5.2. The SCADA System Owner or Business Unit SCADA Cyber Security Function shall review at least annually the access privileges SCADA system protected information to confirm that access privileges are correct and correspond with the operational needs and appropriate personnel roles and responsibilities.

R5.3. The SCADA System Owner or Business Unit SCADA Cyber Security Function shall assess and document at least annually the processes for controlling access privileges to protected SCADA system information.

DR5.4. All SCADA roles must be aware of the regulatory and governmental requirements regarding the release of SCADA information to government agencies, i.e., Department of Homeland Security 6 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Interim Rule",

regulations stemming from the Freedom of Information Act (FOIA)). Contact the Legal Department in your area for information and guidance for SCADA information release.

R6. Change Control and Configuration Management - The SCADA System Owner or Business Unit SCADA Cyber Security Function shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing SCADA system hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

As such, any software or hardware changes with potential impact to SCADA system cyber security must be managed through a Business Unit SCADA Cyber Security Function approved change management process.

The change process must convey at a minimum:

1. Reason for the change
2. Appropriate authorization
3. Appropriate change notification (communication of the change)
4. Change back-out plan

It is the responsibility of the SCADA System Owner to maintain the change management process history per the Business Unit document retention policy.

6003.2 Business Unit Requirements

6003.2.1 Business Units Regulated by NERC

CIP-003 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6003.2 and are noted with "See Enterprise Requirements".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

R1.2. See Enterprise Requirement

R1.3. See Enterprise Requirement

R2. See Enterprise Requirement

IT 6003 – Compliance, Monitoring, and Response

R2.1. The *senior manager* shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. The senior manager or delegate(s) must authorize and document any exception from the requirements of the cyber security policy.

R3. See Enterprise Requirement

R3.1. See Enterprise Requirement

R3.2. See Enterprise Requirement

R3.3. See Enterprise Requirement

R4. See Enterprise Requirement

R4.1. See Enterprise Requirement

R4.2. See Enterprise Requirement

R4.3. See Enterprise Requirement

R5. See Enterprise Requirement

R5.1. See Enterprise Requirement

R5.1.1. See Enterprise Requirement

R5.1.2. See Enterprise Requirement

R5.2. See Enterprise Requirement

R5.3. See Enterprise Requirement

R6. See Enterprise Requirement

6003.2.2 Business Units Regulated by NRC

See NSD-804

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6004 – Personnel and Training

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

This standard establishes the requirements for granting and monitoring electronic access, or unescorted physical access to SCADA systems; and establishes guidelines for determining appropriate levels of personnel risk assessment, training, and security awareness. This standard applies to all members of the Duke workforce, including third parties, contractors and vendors.

6004.1 Enterprise Requirements

R1. Awareness - Business Unit SCADA Cyber Security Function areas are responsible for promoting SCADA cyber security awareness to all users. Corporate IT Strategy and Compliance will provide items that meet this awareness program. Security Awareness responsibilities include:

1. The Business Unit SCADA Cyber Security Function is responsible for ensuring that Business Unit management is informed of the awareness training requirements.
2. Business Unit management is responsible for employee participation.
3. Corporate IT Security, working with the Business Unit SCADA Cyber Security Function Area, is responsible for defining and documenting the overall SCADA Cyber Security Awareness Program and supporting the efforts of Business Units.
4. The awareness program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
   - Direct communications, i.e., emails, memos, computer based training, etc.

Duke Energy

Duke Energy Policy Statement

IT 6004 – Personnel and Training

- Indirect communications, i.e., posters, intranet, brochures, etc.
- Management support and reinforcement, i.e., presentations, meetings, etc.

DR1. Training and Personnel Risk Assessment requirements outlined in this standard must be met before individuals are given access to SCADA systems.

DR1.1. Measurement - The SCADA Cyber Security Awareness Program must define the criteria and approach with which to measure the SCADA cyber security awareness level. The measurement approach must be executed by Corporate IT Strategy & Compliance on a periodic basis.

DR1.2. Communication - Company communications that contain information on SCADA cyber security training, policy update alerts, or other security or public displays to alerts must be posted on the Corporate IT Strategy and Compliance website or otherwise ensure that all users have access to the information.

R2. Training - The SCADA Cyber Security Awareness Program must consist of annual awareness training which should be reviewed annually and update as necessary. Security awareness training and employee acknowledgement should be a priority of Business Unit management. Training may vary according to needs and can be customized by Corporate IT Strategy and Compliance and/or Business Units and review the program annually updating as necessary.

R2.1. Training Implementation

All workforce employees (including vendors, contractors, and Third Parties) that have logical or physical access to SCADA systems must be directed to the Corporate IT Strategy and Compliance website to view the Policy, Standards, and Procedures or be provided a copy of the applicable policies and standards.

All employees with electronic or physical access to Company SCADA systems will receive training on elements of security awareness and periodic security awareness briefings

Non-disclosure agreements to protect training materials must be contained in the contract for each contractor or third party member.

IT 6004 – Personnel and Training

R2.2. Training shall cover the policies, access controls, and procedures as developed for SCADA systems covered by this standard, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of SCADA systems

R2.2.2. Physical and electronic access controls to SCADA systems

R2.2.3. The proper handling of SCADA system information; and

R2.2.4. Action plans and procedures to recover or re-establish SCADA systems and access to following a Cyber Security Incident, as applicable.

R2.3. The Business Unit SCADA Cyber Security Function shall document that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment - For SCADA systems classified as "Critical Infrastructure" personnel risk assessments on individuals must be conducted as defined by the Business Unit. SCADA systems classified as Operational must screen individuals in accordance with Human Resources (HR) policies.

R3.1. This requirement is not applicable.

R3.2. This requirement is not applicable

R3.3. This requirement is not applicable

R4. Access (Electronic and Physical) - The Business Unit SCADA Cyber Security Function or System Owner shall maintain access list(s) for all electronic and unescorted physical access to SCADA Systems. Access to SCADA systems (including their specific electronic and physical access rights to SCADA systems) will be determined by business need.

R4.1. The Business Unit SCADA Cyber Security Function or System Owner shall review the access list(s) at least annually. All SCADA system access must be removed within 7 calendar days of the effective date of a user transfer. Extensions must be approved and documented by the appropriate Business Unit SCADA Cyber Security Function or SCADA System Owner.

R4.2. All access (physical and electronic) must be disabled within 24 hours of the effective date of a user termination, and within 7 calendar days of the individual no longer requiring access to the SCADA system.

DR4.3 SCADA System Owners must comply with all regulatory requirements (including FERC 2004 Affiliate Code Ruling) with regard to granting access to SCADA systems.

DR4.4 Unless otherwise specified, SCADA system data falls under the "Confidential" classification as outlined in "IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6004 – Personnel and Training

DR5. Appropriate Use of SCADA Systems –

DR5.1 Non-business use of SCADA systems is not allowed. General purpose software (non-SCADA software) must not be loaded or used from dedicated SCADA equipment unless approved by Business Unit SCADA Cyber Security Function. (General purpose software is any software not required for the operation or support of the SCADA system. Examples of general purpose software include: e-mail, instant messaging, productivity software, games, etc.

DR5.2 To reduce legal liability and to ensure that software is used in an appropriate manner, employees and contractors must abide by software licensing agreements (Software License Management - IT 2010).

DR5.3 All software found that is not licensed or approved must be remediated through proper licensing or approval, or is subject to immediate removal in accordance with "IT 5002.4.1 Acceptable Use of Assets: Software".

DR5.4 Unverified system updates, including those from the Internet, must never be installed, nor should any downloads be accepted that were not expressly requested or previously planned (such as anti-virus signatures). For example, new versions of Internet Explorer must not be automatically downloaded. The SCADA System Owner is responsible for defining verification/validation plans for system updates.

DR5.5 The use of software for performing network reconnaissance and network support functions is strictly prohibited unless a specific business need exists and the Business Unit SCADA Cyber Security Function approval has been obtained.

6004.2 Business Unit Requirements

6004.2.1 Business Units Regulated by NERC

CIP-004 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6003.2 and are noted with "See Enterprise Requirements".

R1. See Enterprise Requirement

R2. See Enterprise Requirement

R2.1. See Enterprise Requirement

R2.2. See Enterprise Requirement

R2.2.1. See Enterprise Requirement

R2.2.2. See Enterprise Requirement

IT 6004 – Personnel and Training

R2.2.3. See Enterprise Requirement

R2.2.4. See Enterprise Requirement

R2.3. See Enterprise Requirement

R3. Personnel Risk Assessment - The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. For more information, see "6004 DR1". The Risk Assessment program, at a minimum must include:

R3.1. The Responsible Entity shall ensure that each assessment conducted includes, at a minimum, identity verification, i.e., Social Security Number verification in the U.S., and a seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall affirm and document the results of personnel risk assessments of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets and also for contractor and service vendor personnel with similar access. All personnel risk assessments must be conducted in accordance with Standard CIP-004.

R4. See Enterprise Requirement

R4.1. See Enterprise Requirement

R4.2. See Enterprise Requirement

6004.2.2 Business Units Regulated by NRC

See NSD-804

See also:

SCADA Cyber Security Standards and Procedures, "IT 5010-01 Standards Exception Procedure", and "IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6005 - Electronic Security Perimeters

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

The purpose of this standard is to establish requirements for identifying, isolating, and protecting SCADA systems, and for documenting the perimeter network(s) in which they reside (Electronic Security Perimeters). The minimum requirements for isolating SCADA systems and networks from general business IT systems, and other networks, are defined as follows:

6005.1 Corporate Requirements

DR1. Internet Connectivity - Internet connections are those points where connectivity exists between Duke Energy's network and the Internet. SCADA systems are allowed to transmit data indirectly to or from the Internet through the Duke Business network. Data produced by SCADA and used by another application is subject to the normal data classification standards established in "IT 5002.5.2" Security Classifications".

Specific requirements are as follows:

DR1.1. SCADA systems must not directly connect to the Internet. This restriction includes HMIs.

DR1.2. Indirect data transport required to and from the Internet must be sent via the business network.

DR1.3. All SCADA data, including control commands sent via the Internet, must be encrypted.

DR1.4. Non-business use of the Internet from SCADA systems is prohibited.

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6005 – Electronic Security Perimeters

R1. Electronic Security Perimeter -

SCADA systems must appropriately mitigate security risks regarding data transmissions to and from the Internet. The SCADA System Owner shall ensure that every SCADA System asset resides within a defined Electronic Security Perimeter. The SCADA System Owner shall identify and document the electronic security perimeter and all access points to it

R1.1. For Electronic Security Perimeters, all connections to other networks must be via a screening device (router or firewall) designed to strictly limit traffic to and from the other networks. Access points to the electronic security perimeter shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the network. Screening devices must not accept external connections that are from or that appear to be coming from internal addresses (provide anti-spoofing function).

For more information about the placement of intrusion detection systems, see section 6007 R.4.1.

R1.2. The SCADA System Owner or Business Unit SCADA Cyber Security Function shall maintain a procedure for securing dial-up access to the electronic security perimeter.

Dial-in access to SCADA equipment must be restricted to personnel or vendors that directly support the equipment *and be documented as part of an Electronic Security Perimeter*. Dial-in access to all Company SCADA assets must be controlled. Modem access must be approved by Business Unit SCADA Cyber Security Function. Records must be kept, including current lists of all telephone numbers connected to modems and all vendors that have been supplied a dial-in number. The following conditions apply:

- For dial-out, the modem must be set to originate (dial-out) only.
- The default-state of the modem must be inaccessible. It should be made accessible only when access is needed, and must be returned to an inaccessible state immediately after the connection ends.

The dial-in modems must be secured at all times by at least one of the following:

- A modem password is enabled, Strong passwords are required.
- The modem disabled when not in use and enabled only on request.

IT 6005 – Electronic Security Perimeters

- The modem is normally disabled when not in use
- Dial-back is enabled

R1.3. Non-secure Network Links - data connections such as spread spectrum radio, private band radio, microwave, satellite, and the public or leased telephone or data networks, are typically used to connect SCADA hosts to field equipment and to connect field equipment to another piece of field equipment, i.e., from one RTU to another RTU. These data connections cannot reliably be secured. SCADA System Owners must consider and document the means to mitigate this risk. For example, fail-safe shutdown processes for end nodes that cannot authenticate a shutdown command came from an authorized host. End points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

IP-capable field devices that cannot maintain similar physical access control as the host, i.e., from field HMI to SCADA host, must:

- require authentication
- pass through network screening that only allows network traffic for required functions, i.e., a firewall

These controls may not be required if approved and documented by the SCADA Cyber Security Business Function or SCADA System Owner and:

- When appropriate mitigation procedures are implemented for remote locations, (i.e., an alarmed remote location with appropriate alarm response procedures.)
- For Non-IP field devices, i.e., those devices using serial connections

R1.4. Only devices dedicated to the operation or support of the SCADA system are allowed within an electronic security perimeter. All devices within a electronic security perimeter shall be identified and protected pursuant to the requirements of this standard. All devices within the llectronic security perimeter rmust be within the same type of physical access control boundary

DR1.4. Only SCADA and system management, i.e., anti-virus, system backup applications are allowed to connect outside the isolated SCADA network. No general use applications, i.e., Internet browsing, drive mapping, and e-mail are allowed to connect outside the isolated SCADA network unless an application proxy such as Terminal Server is used.

R1.5. Electronic access to SCADA network equipment, including the network screening/isolation devices (routers/firewalls/etc.) must be treated the same as the electronic access to the SCADA equipment itself.

IT 6005 – Electronic Security Perimeters

R1.6. The electronic perimeters including all access points of SCADA systems must be clearly defined, documented, and approved by the SCADA Business Unit Cyber Security Function. Diagrams, including drawings, access lists, and firewall rules must be included. The access/screening devices configurations must adhere to corporate change management standards and must also include either a SCADA System owner or SCADA Business Unit Cyber Security Function approval.

R2. Electronic Access Controls -The SCADA System Owner or Business Unit SCADA Cyber Security Function shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all screening devices protecting isolated SCADA networks. All communication allowed across the screening device must be strictly limited. Access through the screening device must be strictly limited to only those locations and functions required for operation and support.

R2.1. All access must be denied by default. Only explicitly authorized network traffic will be allowed. The screening device must block all non-IP protocols used within the logically isolated network.

R2.2. Access must be documented (in a document external to the screening device itself) and meet the following minimums:

- Allow communication by specific machine-to-machine or limited address ranges.
- Allowing access from remote machines only as required by business purposes.
- All ports must be closed unless specifically required.

A DMZ must be provided to the electronic security perimeter when devices are accessed by externally initiated connections. All such devices must be located in the DMZ, for example, a terminal services server. Access from the DMZ to the electronic security perimeter must be limited to only those locations and functions required for operation and support.

DR2.2.1 For Critical Infrastructure SCADA Systems, System Owners must provide means to disconnect SCADA networks from other computer interconnections, especially those to the IT business network. In the case of a CIRT event, SCADA systems can then be temporarily disconnected from other networks. Network disconnection procedures shall be developed, and periodically reviewed, and table-top tested.

R2.3. See requirement R1.2 above.

R2.4. Where external interactive access into the isolated SCADA Network has been enabled; the SCADA System Owner or Business Unit SCADA Cyber Security Function shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party. The following controls must be implemented

a) Access with SCADA Control (Control indicates the ability to make system changes or manipulate devices)

IT 6005 – Electronic Security Perimeters

- Any external devices with control access to the SCADA network must be dedicated to the SCADA function. These devices must be physically controlled per the SCADA system classification.
- Also, these devices must be network tunneled (encrypted) to the SCADA network.

b) Access from an HMI, No Control (viewing or monitor only)

- HMI access to the SCADA network must be dedicated to the SCADA function, where possible. Access by non-dedicated devices must be controlled, where possible. Examples: connection via an internal terminal services server tunneling.

c) Machine-to-Machine

- Connection to external infrastructure, such as a mainframe, must be initiated from the electronic security perimeter, unless the devices being accessed by externally initiated connections are located in a DMZ, or otherwise specifically protected by IP-to-IP firewall rules. Example: a terminal services server must be located in a DMZ.

DR2.4.1. Remote Access to SCADA Hosts – This section describes access to systems by remote users crossing any network security perimeters.

- Remote connections to SCADA networks must terminate in a DMZ. This includes access from the Duke Business network to the SCADA network, as well as external access. Access via modem/dial-in is covered in **R1.2.**
- Remote access, i.e., network or VPN, to a SCADA system must be approved by the Business Unit SCADA Security Function.
- Remote access tools to SCADA system classified as "Critical Infrastructure" must utilize a two-factor authentication mechanism. The authentication method must be approved by the SCADA Business Unit SCADA Security Function.
- Remote access must be encrypted if the connection is over the Internet.

- Appropriate physical controls must be placed on the accessing (remote) device. It must not be left unattended and must be physically secured at all times. Portable devices must not be checked as luggage when traveling or left in open view when left in an unattended vehicle. Examples of acceptable physical security methods are a locked trunk, cable lock, locked room or desk.
  - Vendor IDs must only be authorized to the specific resources needed to achieve the business requirement of their connection. Vendor User ID's must be deactivated by default and activated only when required.

IT 6005 – Electronic Security Perimeters

DR2.4.2. "Read-only" or "view-only" access of SCADA data must be accomplished by one of the following methods:

1. The data is physically copied outside of the SCADA network to a separate shared data source (preferred).
2. Or, access to the SCADA data is allowed only via an authenticated process, i.e., Terminal Services Server, into the SCADA network DMZ (a separate firewall segment).
3. Or, access to the SCADA data is allowed via an authenticated application interface into the SCADA network DMZ.

DR2.4.3. Employees must access SCADA systems only from company-owned computers. Vendors must access SCADA systems only from company-owned or vendor-owned computers. No personal or "home" computers are allowed access.

Vendor access must be used only for specific vendor support or monitoring. A written statement signed by the vendor supporting this adherence to the following controls must be obtained prior to connecting to the SCADA equipment or network. All activities performed from this connection are subject to monitoring and logging.

Note: Duke Energy is not liable for software inappropriately licensed on non-Company computers.

Vendors, contractors or consultants must adhere to the following requirements when connected:

- Active and current virus protection on their machine
- Patches and maintenance levels for the operating system must be current with Duke Energy standards on their machine
- Connections to other networks, including the Internet, will not be allowed while also connected to Duke Energy resources
- Outbound VPN connections will not be established
- Sniffing software is not allowed, unless approved by the Business Unit SCADA Cyber Security Function
- Broadcast request services, such as DHCP server, are not allowed.

IT 6005 – Electronic Security Perimeters

R2.5. The required electronic access documentation (as specified in R.2, above) shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3 See 6004.1 R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner - Business Unit SCADA system owners are responsible for documenting the content of and implementing a logon banner. A login banner must include the following:

1. The information system is to be used only by authorized users.
2. By continuing to use the information system, the user agrees they are an authorized user.
3. Use of the information system constitutes consent to monitoring in accordance with SCADA Cyber Security Policy, Introduction, Terms and Roles – IT 6000.

The identification of any Company network, location, information system, application or host specific information must not appear until a successful login has occurred. A logon banner is not required if:

1. The system/device/component vendor does not support a logon banner
2. Or a logon banner interferes with the intended function of the SCADA system

R3. Monitoring Electronic Access – A process must be implemented for the monitoring and logging of electronic access to SCADA networks, which must be conducted 24 hours a day, 7 days a week.

R3.1. For dial-up accessible (modem) access points, a monitoring and logging mechanism must be enabled.

R3.2. All access at the electronic access points must be monitored 24 hours a day 7 days a week. Unauthorized attempts must be alerted to appropriate personnel. For more information, see 6007 R4.1

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6005 – Electronic Security Perimeters

R4. Cyber Vulnerability Assessment - The SCADA System owner or Business Unit SCADA Cyber Security Function (or shall delegate to Corporate IT Security) to perform a cyber vulnerability assessment of the electronic access points to the isolated SCADA network at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the SCADA network;

R4.4. A review of controls for default accounts, passwords, and network management community strings:

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance - The SCADA System owner or Business Unit SCADA Cyber Security Function shall review, update, and maintain all documentation to support compliance with the requirements of this standard (6005).

R5.1. The Busines Unit SCADA Cyber Security Function or SCADA System owner shall ensure that all documentation required by this standard reflects current configurations and processes and shall review the documents and procedures referenced by this standard at least annually.

R5.2. The Business Unit SCADA Cyber Security Function or SCADA System Owner shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Business Unit SCADA Cyber Security Function or SCADA System Owner shall retain electronic access logs for at least ninety calendar days. Logs related to security incidents shall be kept in accordance with the requirements of Standard 6008.

6005.2 Business Unit Requirements

6005.2.1 Business Units Regulated by NERC

CIP-005 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6005.2 and are noted with "See Enterprise Requirement".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

IT 6005 – Electronic Security Perimeters

R1.2. See Enterprise Requirement

R1.3. See Enterprise Requirement

R1.4. See Enterprise Requirement

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. See Enterprise Requirement

R2. See Enterprise Requirement

R2.1. See Enterprise Requirement

R2.2. See Enterprise Requirement

R2.3. See Enterprise Requirement

R2.4. See Enterprise Requirement

R2.5. See Enterprise Requirement

R2.5.1. See Enterprise Requirement

R2.5.2. See Enterprise Requirement

R2.5.3. See Enterprise Requirement

R2.5.4. See Enterprise Requirement

R2.6. See Enterprise Requirement

R3. See Enterprise Requirement

R3.1. See Enterprise Requirement

R3.2. See Enterprise Requirement

R4. See Enterprise Requirement

R4.1. See Enterprise Requirement

R4.2. See Enterprise Requirement

R4.3. See Enterprise Requirement

R4.4. See Enterprise Requirement

R4.5. See Enterprise Requirement

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6005 – Electronic Security Perimeters

R5. See Enterprise Requirement

R5.1. See Enterprise Requirement

R5.2. See Enterprise Requirement

R5.3. See Enterprise Requirement

6004.2.2 Business Units Regulated by NRC

See NSD-804

See Also:

SCADA Cyber Security Standards and Procedures, "IT 5010-01 Standards Exception Procedure", and "IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6006 - Physical Security

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

The purpose of this standard is to define the physical security requirements for Duke Energy facilities containing SCADA systems or facilities used in support of SCADA systems.

6006.1 Enterprise Requirements

R1. Physical Security Plan - Facilities housing Duke Energy SCADA system equipment are restricted to Duke Energy employees, business partners, contractors and vendors who support Duke Energy resources. No provision shall be made to allow the sharing of these facilities or allow routine access not in support of Duke Energy business.

Each SCADA System Owner must define and implement a physical security plan, approved by a senior manager or designee that includes the level of access management and monitoring controls that must be in place for each SCADA system or asset, which shall address, at a minimum, the following:

R1.1. Processes that ensure the perimeter of the physical security provided to a SCADA system is clearly defined, documented, and reviewed by the Business Unit SCADA Cyber Security Function. The physical security perimeter shall contain all Cyber Assets which are within the Electronic Security Perimeter.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

IT 6006 – Physical Security

R1.4. Procedures for the appropriate use of physical access controls. This includes visitor pass management, response to loss, and inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization must conform to 6004 R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Processes for updating the physical security plan within ninety (90) calendar days of any physical security system redesign or reconfiguration, including, but not limited to; the addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Processes to ensure that electronic systems used in the access control and monitoring of the Physical Security Perimeter(s) of SCADA systems shall be afforded at a minimum the protective measures specified in the 6000 standards for protecting the SCADA systems themselves.

R1.9. Processes for ensuring that the physical security plan is reviewed at least annually.

R2. Physical Access Controls -The SCADA System Owner or Business Unit SCADA Cyber Security Function shall document and implement the operational and procedural controls to manage physical access to the Physical Security Perimeter(s) defined for SCADA systems twenty-four hours a day, seven days a week. Buildings or other facilities that house Company computers and communications systems must be controlled with physical security measures that prevent unauthorized individuals from gaining access. Physical access to all Company computer, and/or control rooms, closets, areas, cabinets, or other rooms containing wiring or communications equipment must be limited to authorized personnel. Physical security of SCADA systems may be inherited from the physical security of the facility.

Access authorization to SCADA equipment must be based on a legitimate business need.

DR2.1 Systems providing physical access control must be protected to the same level as the SCADA equipment they protect.

DR2.2 Systems providing physical access must utilize a process for approving and documenting changes. If applicable, a centralized corporate process is preferred. This process must include either a SCADA System owner or SCADA Business Unit Cyber Security Function approval.

The SCADA System Owner or Business Unit SCADA Cyber Security Function must implement one of the following physical access methods for systems classified as Critical Infrastructure:

R2.1. Card Key - A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks - These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

IT 6006 – Physical Security

R2.3. Security Personnel - Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices - Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

DR2.5 For SCADA systems classified as Operational, the SCADA System Owner or Business Unit SCADA Cyber Security Function shall implement at least one physical barrier, i.e., locked door or cabinet.

DR2.6 Authorized personnel must not allow unknown or unauthorized individuals into areas containing SCADA equipment. Any unauthorized or unescorted personnel must be identified and escorted from the area. Company security must be notified of these actions.

DR2.7 Physical access to SCADA storage media, i.e., compact disks, diskettes, magnetic tape, hard drives, internal computer storage, printouts, or hard copy documentation libraries must be restricted to authorized personnel only.

DR2.8. SCADA equipment must not be left unattended with a privileged account logged in, unless that equipment is located in a physically secured area. Otherwise, users must log out of any privileged accounts or lock the system before leaving a non-secured work area. If possible, SCADA equipment must be configured with a password protected "screen saver", unless the equipment is located in a physically secured area. If used, the screen saver must require the entry of a password after no more than ten minutes of inactivity.

DR2.9. The use of scripts for the purpose of unattended logins will be allowed only if required for the operation or support of SCADA systems.

DR2.10. Any electronic devices or digital media not specifically used for the operation or support of a SCADA system must not be connected to any SCADA system. Examples include CDs, floppy drives, USB drives, external speakers, etc.

R3. Monitoring Physical Access - For SCADA Systems or assets classified as "Critical Infrastructure", the SCADA System Owner or Business Unit SCADA Cyber Security Function shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with physical security processes. One (1) or more of the following monitoring methods shall be used:

R3.1. Alarm Systems - Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points - Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

DR3.3 For SCADA systems classified as "Operational", monitoring of physical access to these systems must include the means to identify all personnel with access to the area.

IT 6006 – Physical Security

R4. Logging Physical Access - For SCADA Systems classified as "Critical Infrastructure", logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The SCADA System Owner or Business Unit SCADA Cyber Security Function shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging - Electronic logs produced by the SCADA System Owner or Business Unit SCADA Cyber Security Function's selected access control and monitoring method.

R4.2. Video Recording - Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging - A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

DR4.3 For SCADA systems classified as "Operational", logging of physical access to these systems must include the means to identify tampering, i.e., use of meter seals.

R5. Access Log Retention - The SCADA System Owner or Business Unit SCADA Cyber Security Function shall retain physical access logs for at least ninety calendar days. Log retention for reportable incidents is defined in 6008 R2.

R6. Maintenance and Testing of Physical Access Systems - For SCADA Systems defined as "Critical Infrastructure", Business Unit SCADA Cyber Security Function or SCADA System Owners are responsible for:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. The retention of testing and maintenance records for the cycle of 6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

6006.2 Business Unit Requirements

60062.1 Business Units Regulated by NERC

CIP-006 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6002.2 and are noted with "See Enterprise Requirement".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

R1.2. See Enterprise Requirement

IT 6006 – Physical Security

R1.3. See Enterprise Requirement

R1.4. See Enterprise Requirement

R1.5. See Enterprise Requirement

R1.6. See Enterprise Requirement

R1.7. See Enterprise Requirement

R1.8. See Enterprise Requirement

R1.9. See Enterprise Requirement

R2. See Enterprise Requirement

R2.1. See Enterprise Requirement

R2.2. See Enterprise Requirement

R2.3. See Enterprise Requirement

R2.4. See Enterprise Requirement

R3. See Enterprise Requirement

R3.1. See Enterprise Requirement

R3.2. See Enterprise Requirement

R4. See Enterprise Requirement

R4.1 See Enterprise Requirement

R4.2. See Enterprise Requirement

R4.3. See Enterprise Requirement

R5. See Enterprise Requirement

R6. See Enterprise Requirement

R6.1. See Enterprise Requirement

R6.2. See Enterprise Requirement

R6.3. See Enterprise Requirement

6004.2.2 Business Units Regulated by NRC

See NSD-804

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6006 – Physical Security

See Also:

SCADA Cyber Security Standards and Procedures, see "IT 5010-01 Standards Exception Procedure", and "IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6007 - Systems Security Management

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

This standard defines the requirements for developing methods, processes, and procedures to secure Duke Energy SCADA systems.

6007.1 Corporate Requirements

DR1. Test Procedures - The The SCADA System owner or Business Unit SCADA Cyber Security Function shall ensure that new SCADA systems and significant changes are tested prior to implementation. Testing of SCADA systems must not compromise the production systems.

For example, a test system should not be connected to production systems, and measures should be taken to insure test systems are physically and logically marked and at least logically isolated from production systems. A significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware where applicable.

R1. Test Procedures — The SCADA System Owner shall ensure that new SCADA systems and significant changes to existing SCADA systems within an Electronic Security Perimeter do not adversely affect existing cyber security controls. A significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

IT 6007 – Systems Security Management

R1.1. The SCADA System Owner or Business Unit Cyber Security Function shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. This requirement is not applicable.

R1.3. The SCADA System Owner or Business Unit Cyber Security Function shall document results from tests of cyber security controls.

R2. Ports and Services - Only those network protocols, services and applications required to support the SCADA function are to be enabled. Ports and Services must be configured to ensure maximum appropriate protection of the SCADA system and network. Refer to Business Unit specific procedures for guidelines on configuring ports and services.

R2.1. The SCADA System Owner or Business Unit Cyber Security Function shall enable only those ports and services required for normal and emergency operations, per 6005 R2.2.

R2.2. The SCADA System Owner or Business Unit Cyber Security Function shall disable other ports and services, including those used for testing purposes, prior to production use of all isolated SCADA networks.

R2.3. Services and protocols that are enabled must be subjected to a risk assessment process. This assessment is to identify the security risks associated with enabling the service and identify any countermeasures required to secure the service. Risk assessment methodology must follow generally accepted practices and must be commensurate with the significance of the device, component or system

DR2.4. Default SCADA system configuration settings that could potentially compromise SCADA system security must be changed prior to use

R3. Security Patch Management - To ensure configuration changes are tracked and properly managed, including tracking, evaluating, testing, and installation; Business Unit SCADA Cyber Security Function must document and adhere to a Patch and Vulnerability Management process.

R3.1. Corporate IT Operations shall document the assessment of security patches and security upgrades for applicability within three (3) calendar days of availability of the patches or upgrades. SCADA System Owners shall document the assessment of security patches and security upgrades for applicability within three (3) calendar days of availability of the patches or upgrades from SCADA or third party vendors, (not to exceed thirty (30) calendar days from the initial availability of the patch).

R3.2. SCADA System Owners shall document the implementation of security patches. In any case where the patch is not installed or will be installed at a date later than prescribed by Corporate IT Security, the SCADA System Owner shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6007 – Systems Security Management

R4. Malicious Software Prevention - Anti-virus software must be placed on all SCADA systems and kept updated and running at all times. SCADA systems must comply with IT Security Standard Virus Protection - 5203 where virus protection is possible. "Personal Firewall" software products are preferred for all computers on SCADA systems classified as "Critical Infrastructure", but are required on laptops, pursuant to IT 5006.5.3.2.

R4.1. Corporate IT Operations shall document and provide anti-virus prevention tools generally available for SCADA systems. For Critical Infrastructure SCADA systems, intrusion detection systems must be installed to monitor the SCADA network.

- Service level agreements with Corporate IT Operations for monitoring IDS sensors may be set up for specific SCADA requirements.
- IDS must be strategically placed to ensure all network traffic that traverses electronic security perimeter of the SCADA network is monitored.
- IDS systems should be configured for fail-safe operations as required by the SCADA system. For more information about the configuration and management of intrusion detection sensors, see "IT 5005.8.1.2 IDS Monitoring".

R4.2. Corporate IT Operations must document and implement a process for the update of anti-virus and IDS "signatures". SCADA System Owners must create and follow an update process that addresses testing and installing the signatures, if different from the corporate process.

R5. Account Management - The SCADA System Owner is responsible for ensuring that procedural controls are established and implemented that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The SCADA System Owner shall ensure that individual and shared system accounts and authorized access permissions are based on a legitimate business need.

R5.1.1. This requirement does not apply.

R5.1.2. Logs that create historical audit trails of individual user account access activity must be created and reviewed. See R6 below.

R5.1.3. SCADA system access must be reviewed on a periodic basis, at least annually. SCADA System Owners are responsible for removing all privileges no longer required by users per 6004 R4.

R5.2. The SCADA System Owner shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. Default SCADA accounts must be renamed, deactivated, or removed, prior to initial use, at the time of equipment or system installation or conversion. If possible, all default IDs must have a complex password defined to it prior to the change or deactivation.

IT 6007 – Systems Security Management

Passwords for default IDs must be limited to key staff. These User IDs must not be used unless accesses via personal IDs fail, or use of default IDs are required by the SCADA system.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts. Each Company computer and communication system User ID must uniquely identify only one user. Generic (shared or group) User IDs are not permitted, except as noted in R5.2.3. Users are also not allowed to share or otherwise expose their unique password.

R5.2.3. Generic (shared) IDs may be used for SCADA systems only if access to the system is physically controlled and the system has an electronic security perimeter,. Generic IDs are also known as shared or group IDs, meaning the account password is known by more than one person. For Critical Infrastructure systems, generic IDs cannot be used remotely unless the account privileges are "view only".

Generic ID passwords must be changed when personnel who have access to the password are re-assigned or terminated, or the password is compromised--otherwise passwords must be changed every 60 days or less.

Business Unit SCADA Security Function must approve a password change procedure for changing and communicating the password.

DR5.2.4. Privileged ID Usage and Controls – Privileged users are users with system administration or "super-user" privileges. Privileged users must have their access rights reviewed periodically by the SCADA System Owner to ensure access to SCADA information is appropriate. Privileged IDs must be used in lieu of default IDs, where possible. Privileged ID's must not be used for standard operations, unless technically required by the SCADA system.

DR5.2.5. Account Lockouts - Where possible, upon three consecutive authentication failures, users will be locked out of the resource in which they are attempting to gain access. The account will remain locked until manually reset by Corporate IT Operations, or the appropriate support group. This is not required for electronic security perimeters that are also physically protected systems classified as Critical Infrastructure, and where the account cannot be accessed from outside the physical control area (used for remote control/access).) When possible, the lockout counter for consecutive authentication failures will be reset after 30 minutes, i.e. Windows 2000, NT environments.

R5.3. At a minimum, password security to SCADA systems must be used unless:

1. The SCADA system is not capable of supporting password security.
2. Operational processes do not support the use of passwords.

IT 6007 – Systems Security Management

If not used, other risk mitigation, such as physical access protection, must be in place. Password construction is subject to the following, whenever possible:

R5.3.1. Each password shall be a minimum of eight characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least every 60 days, where possible.

DR5.3.4. SCADA System accounts with control privilege, system administrators, and other support personnel using privileged IDs must have passwords that are a minimum of nine characters in length and contain a mixture of letters, numbers, and at least two embedded special characters.

DR5.3.5. All IDs for devices, i.e., routers, switches and firewalls must have complex passwords. If possible, they should adhere to the password guidelines defined above for privileged IDs.

DR5.3.6. Initial passwords must also conform to this standard and not be easily associated with the Company or the user, i.e. social security number, User ID, employee number, address, numerical equivalent of name, etc. Initial passwords must be changed upon first use.

DR5.3.7. Users must not use cyclical or patterned passwords. For example, when changing passwords, users cannot add a number at the end of the password in sequence. Where possible, systems must use password history controls to maintain a password history of users. Users must not be allowed to re-use one of the passwords in their password history file. The history file must contain, at a minimum, the last 10 passwords of users and store them in hashed or encrypted form.

DR5.4. Passwords to SCADA devices and systems must be protected at all times. All passwords must remain confidential except in critical business situations.

DR5.5. Default SCADA passwords must be changed upon initial login where possible

DR5.6. SCADA password files must be encrypted where possible and access must be limited to those with SCADA system administrator privileges. If this is not possible, the Business Unit SCADA system owner must maintain control processes to protect password files. SCADA passwords that travel over the network must be encrypted, where possible, using a method approved by Corporate IT Security. Passwords and other sensitive data may be transmitted within a physically isolated network without encryption. User IDs and passwords being provided to external parties must be sent in an encrypted file. The password to open the file must be communicated separately from the file containing the User ID and password data.

IT 6007 – Systems Security Management

R6. Security Status Monitoring - SCADA System Owners must ensure that logs are activated and/or monitoring software is in place in order to capture suspicious activity and to monitor system events that are related to cyber security.

R6.1. The SCADA System Owner shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all isolated SCADA Systems.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The SCADA System Owner must maintain logs of system events, which must record the following data at a *minimum*:

1. User session activity including:
2. User IDs
3. Log-in success for initial login
4. Log-in failure
5. Log-in date/time
6. Log-out date/time
7. User privilege modifications
8. System start-ups and shutdowns

Other recommended logging includes Application(s) invoked by user.

SCADA systems must log all security relevant events, where possible. Examples of security relevant events include:

1. Users switching User IDs or system identity during an on-line session
2. Password guessing activities, attempts to escalate privileges
3. Modifications to system software
4. Changes to system logs or logging configurations

R6.4. Log files should be retained for 90 days, under normal circumstances. Log file archival processes should be approved and periodically reviewed by the SCADA System Owner.

Logs containing suspicious security events must be retained per 6008, R2.

R6.5. SCADA System Owners must review systems logs for suspicious security events periodically, if not automatically notified. Any suspicious security events found in system logs must be promptly reported to CIRT (IT Computer Incident Response - IT 5301.01). Daily or weekly reviews of

IT 6007 – Systems Security Management

security logs using an automated tool are required for SCADA systems classified as "Critical Infrastructure". The SCADA System Owner should document all log reviews.

DR6.6. Access to system logs is given only on a need-to-know basis.

DR6.7. Only authorized individuals, with approval Business Unit SCADA Cyber Security Function, are allowed to use network monitoring software or hardware.

R7. Disposal or Redeployment - The SCADA System Owner or Business Unit SCADA Cyber Security Function shall establish formal methods, processes, and procedures for disposal or redeployment of computer assets used by SCADA systems.

R7.1. Prior to the disposal of such assets, electronic storage media containing SCADA system information that contains data classified above "Public" (see IT 5200) must be disposed of through degaussing for magnetic media (e.g. floppy disks or tapes) or physical destruction for other media i.e., compact disks or recordable media. The tool must perform at least a single pass over the hard drive writing nulls on all writable areas.

R7.2. Prior to redeployment of such assets, to ensure data is not disclosed, it must be erased to the point that it is not accessible by any means. This includes if any of the following changes to SCADA equipment occur:

- equipment is surplused
- equipment lease is terminated
- Disk drive is upgraded in an existing machine
- Transfer of equipment occurs which invokes affiliate "code of conduct" issues

DR7.2. SCADA system information that contains data classified above "Public" in hard copy form must be disposed of through either shredding or incineration. It is the responsibility of the user in possession of the hard copy information to ensure proper disposal. For more information about data classifications, see "IT 5002.5.2 Security Classifications".

R7.3. This requirement is not applicable.

R8. This requirement is not applicable.

R8.1. This requirement is not applicable.

R8.2. This requirement is not applicable.

R8.3. This requirement is not applicable.

R8.4. This requirement is not applicable.

R9. Documentation Review and Maintenance - The SCADA System Owner is responsible for reviewing the actions and associated documentation required in this section annually for critical cyber infrastructure

IT 6007 – Systems Security Management

systems. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

6007.2 Business Unit Requirements

6007.2.1 Business Units Regulated by NERC

CIP-007 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6002.2 and are noted with "See Enterprise Requirement".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. See Enterprise Requirement

R2. See Enterprise Requirement

R2.1. See Enterprise Requirement

R2.2. See Enterprise Requirement

R2.3. See Enterprise Requirement

R3. See Enterprise Requirement

R3.1. See Enterprise Requirement

R3.2. See Enterprise Requirement

R4. See Enterprise Requirement

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. See Enterprise Requirement

R5. See Enterprise Requirement

R5.1. See Enterprise Requirement

IT 6007 – Systems Security Management

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. See Enterprise Requirement

R5.1.3. See Enterprise Requirement

R5.2. See Enterprise Requirement

R5.2.1. See Enterprise Requirement

R5.2.2. See Enterprise Requirement

R5.2.3. See Enterprise Requirement

R5.3. See Enterprise Requirement

R5.3.1. See Enterprise Requirement

R5.3.2. See Enterprise Requirement

R5.3.3. See Enterprise Requirement

R6. See Enterprise Requirement.

R6.1. See Enterprise Requirement

R6.2. See Enterprise Requirement

R6.3. See Enterprise Requirement.

R6.4. See Enterprise Requirement

R6.5. See Enterprise Requirement

R7. See Enterprise Requirement

R7.1. See Enterprise Requirement

R7.2. See Enterprise Requirement

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

IT 6007 – Systems Security Management

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. See Enterprise Requirement

6004.2.2 Business Units Regulated by NRC

See NSD-804

See Also

SCADA Cyber Security Standards and Procedures, "IT 5010-01 Standards Exception Procedure", and "IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6008 – Incident Reporting

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

This purpose of this standard is to define the requirements for discovery, classification, response, and reporting of Cyber (Computer) Security Incidents related to Duke Energy SCADA Systems.

6008.1 Corporate Requirements

R1. Cyber (Computer) Security Incident Response Plan - Due to the potential interconnectivity to IT business systems and SCADA systems, SCADA System Owners are responsible for documenting and reporting cyber security incidents. SCADA System Owners must be aware of and comply with any regulatory requirements for computer incident reporting/response. For more information, see "IT 5008 Information Security Incident Management".

Corporate IT Operations shall develop and maintain a Computer Incident Response Plan (CIRT), which shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. *This requirement is not applicable.*

R1.4. Processes for updating the Computer Security Incident response plan within ninety calendar days of any changes requiring updates to the plan.

R1.5. Processes for ensuring that the Computer Security Incident response plan is reviewed at least annually.

IT 6008 – Incident Reporting

R1.6. Process for ensuring the Computer Incident Response Plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

SCADA System Owners may elect to create an incident response plan specifically for their particular system.

R2. Cyber (Computer) Security Incident Documentation - Corporate IT Opertaions will keep relevant documentation related to reportable Computer Incidents pursuant to Requirement R1.1 for three calendar years.

6008.2 Business Unit Requirements

6008.2.1 Business Units Regulated by NERC

CIP-008 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6002.2 and are noted with "See Enterprise Requirement".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

R1.2. See Enterprise Requirement

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

R1.4. See Enterprise Requirement

R1.5. See Enterprise Requirement

R1.6. See Enterprise Requirement

R2. See Enterprise Requirement

6008.2.2 Business Units Regulated by NRC

See NSD-804

See Also:

SCADA Cyber Security Standards and Procedures, "IT 5010-01 Standards Exception Procedure", and

IT 6008 – Incident Reporting

"IT 5002.5.2 Security Classifications".

Duke Energy

Duke Energy SCADA Cyber Security Standard

IT 6009 – Recovery Plans for Assets

Applicability: Enterprise

Originator: Corporate IT Strategy and Compliance

Approval: Information Technology Management Team (ITMT)

Approval Date:

Revision Date:

Revision No:

Statement of Purpose

This purpose of this standard is to define the requirements for SCADA System disaster recovery plans and procedures.

6009.1 Corporate Requirements

R1. Recovery Plans -SCADA System Owners should maintain and periodically review a recovery plan for each SCADA system. The level of detail and period of review of this plan should be determined by the criticality of the overall system. These plans must be reviewed at least every 3 years for "Operational" SCADA systems and at least annually for "Critical Infrastructure" SCADA systems. These plans must encompass the recovery of the SCADA system due to a cyber security incident. It can be incorporated into an existing recovery or business contingency plan. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises - The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. This requirement is not applicable.

IT 6009 – Recovery Plans for Assets

R4. This requirement is not applicable.

R5. This requirement is not applicable.

6009.2 Business Unit Requirements

6009.2.1 Business Units Regulated by NERC

CIP-009 requirements are presented in this section. Some requirements will be met by compliance to Corporate Requirements listed in 6002.2 and are noted with "See Enterprise Requirement".

R1. See Enterprise Requirement

R1.1. See Enterprise Requirement

R1.2. See Enterprise Requirement

R2. See Enterprise Requirement

R3. Change Control - Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.

R4. Backup and Restore - The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media - Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

See Also

SCADA Cyber Security Standards and Procedures, "IT 5010-01 Standards Exception Procedure", and "IT 5002.5.2 Security Classifications".

Glossary of Terms

Access Controls - are methods to protect data from accidental or malicious modification, destruction, or disclosure. Some typical access controls are permissions such as:

- **No Access** – overrides any other access privilege
- **List** – view the contents of a folder or a database or other data structure
- **Read** – view data
- **Add** – copy a new file to a folder, add data to a data structure (file, database or computer)
- **Change** – modify the contents of, or overwrite a data structure
- **Full Control** – change plus modify permissions or auditing on a file, folder or other data structure

Other access can be functional, such as access to physical components via SCADA systems, such as ability to monitor or to monitor and control the SCADA system production devices, or to respond to system alarms.

Access Control List (ACL) - this is a list of users with access to a set of data and their rights to manipulate the data (i.e., list, read, add, change, etc.) or perform system functions

Attack - the act of trying to bypass security controls on a system or a method of breaking the integrity of encrypted information. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data.

Audit Services – Duke Energy organization responsible for providing oversight for compliance to corporate policy, standards, and procedures, governmental compliance, and where appropriate, industry best practices.

Authentication - verifying the eligibility of a workstation, originator, or individual to access specific information. It is providing assurance regarding the identity of a subject or object, for example, ensuring that a particular user is who he claims to be. This also applies to SCADA devices and control systems in determining the identity of a remote component.

Authorization - the privilege granted to an individual to access information or system functions, based up on the individual's clearance and need-to-know. Authorization is also the granting to a user, program, or process, the right of access.

Duke Energy

Duke Energy SCADA Cyber Security Standard

Glossary of Terms

Backup - copying data to another media for redundancy.

Backup Media - the material used to store backup data (i.e., CD-ROM, Magnetic Tape, Floppy Disk, etc.).

Business Unit - a functional/logical part of Duke Energy. For example, Duke Energy Americas.

Business Network - *the general purpose data network used by business systems, i.e., the Duke Energy* "WAN". This does not include the Duke Energy voice network.

Call-Back - *a procedure for positively identifying a remote terminal or computer, in a call back, the host system* disconnects the caller and then dials the authorized telephone number of the remote terminal to re-establish the connection. Call back is synonymous with dial-back.

Certification - the process of reviewing Internet, external and internal connections through the use of scanning tools, in addition to the manual review of configuration parameters and management processes for the environment(s).

Classification (Information or System Protection) - a determination that information requires a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

Control - the function of a SCADA system that provides the ability to change the physical status of equipment. Examples: open or closing a valve, starting a pump, opening a breaker.

Control Center or Control Room - a location that provides centralized command and control over a Business Unit's assets using a SCADA System. A center is typically manned 24 x 7. This includes any controlled environment where there are physical restrictions based on the same SCADA system classification as the control room.

Controlled environment - any area where physical control protects the SCADA assets.

Duke Energy

Duke Energy SCADA Cyber Security Standard

Glossary of Terms

Complex passwords - are passwords containing special characters

Critical – an asset or system essential to functional and safe operation

Cyber - related to information technology, especially logical discussions (as opposed to physical)

Data - numerical or other information represented in a form suitable for processing by computer.

Digital Certificate - an electronic document that links a user or computer with a public and private key pair that can be used for encryption, authentication, non-repudiation, etc.

Denial of Service (DoS) - an attack that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Direct Modem Connection - a modem connected directly to a device, system, server, or workstation therefore bypassing the centrally administered modem banks.

Dedicated SCADA Equipment - any single piece of equipment, but especially a computer, whose function is solely dedicated to the operation and/or support of the SCADA system. See also: "Multiple Use".

Demilitarized Zone (DMZ) - a perimeter network that adds an extra layer of protection between two networks. In a typical DMZ as shown below, traffic from the Outside Network cannot reach the Inside Network. It can only reach the DMZ. If data is needed on the Outside Network, it first must be copied to or proxied by the DMZ by resources on the Inside Network. DMZs can be incorporated between any two networks.

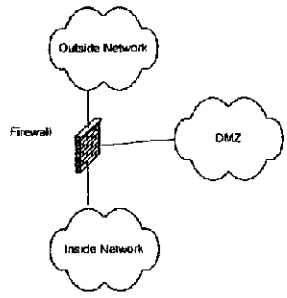


Figure 1

Duke Energy

Duke Energy SCADA Cyber Security Standard

Glossary of Terms

Electronic Data - data stored in terms of specific electrical states.

Electronic Security Perimeter – A protected computer network that is defined, documented, and isolated from other networks by perimeter equipment such as firewalls or screen routers. These are access points into the protected network that limit the traffic allowed into the network. An Electronic Security Perimeter is equivalent to a Logically Isolated System and to the same term used by NERC ("The electronic border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled."). See "Logically Isolated System".

Electronic Transmission - data sent and/or received via electrical currents or radio waves.

Encryption - the process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

Enterprise - In this context, enterprise describes something that encompasses the entire Company.

File Transfer Protocol (FTP) - a means to exchange files across a network.

Firewall - a specialized computer or software designed to protect networks by filtering and blocking access at the IP port or IP address level.

General Purpose Software/Hardware – Computer software/hardware that provides generic business functions not specific to SCADA operations.

Human Machine Interface (HMI) – the presentation component of a SCADA system which provides information to and accepts input from the human user of the SCADA system.

ID – in general, a computer logon Identifier or account. Specific kinds include

> **Generic ID** – ID used by more than one person (i.e., the password is not a secret to only one person) also known as a shared or group IDs.

Glossary of Terms

Network Device ID – unique control IDs used to administer network devices

Privileged ID (or Privileged Account) – A login account that has system administrator or "super-user" privileges allowing broad access and execution authority on a computer system.

Internet - a worldwide "network of networks" that use the TCP/IP protocol suite for communication.

Intranet - Internet technology is used to develop a private, TCP/IP based network within an organization for communicating to and between employees.

Logically Isolated System - a computerized system that is physically connected but isolated by network equipment from another computer network. Network equipment restricts the flow of information across the boundary of the isolated system. Logically Isolated systems are not directly connected to the Internet or to any other third party networks. With a firewall and a DMZ properly placed, the inside network would be considered logically isolated from the outside network. An "Electronic Security Perimeter" is equivalent to a "Logically Isolated System".

Logon Banner - an end-user message that appears before primary system access. The purpose of logon banners is to remind and inform the user of company computer access policy.

Malicious Code - software or firmware that is intentionally included or introduced in a system for the purpose of causing loss or harm.

Media - in general, any technology that enables the recording of data or information for later consumption (reading or communication). This consumption is normally repeatable.

Monitor – the function of a SCADA system to inform or collect data from end-node devices about a particular physical status point (end point).

Multi-use SCADA Equipment – any single computer, whose function is not solely dedicated to the operation and/or support of the SCADA system on a full time basis. This is normally a computer that executes both general purpose business system software and SCADA software.

Need-to-know - a principle that allows for the compartmentalization of information in order to restrict access to individuals whose roles require the subject data or knowledge.

Duke Energy

Duke Energy SCADA Cyber Security Standard

Glossary of Terms

NERC – North American Electric Reliability Council

The following terms are specific to, and within the scope of the NERC CIP Cyber Security Standards:

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

1. Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
2. Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter - The logical border surrounding a network to which Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter - The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled. (Generalize this for non-NERC users of 6006 Physical.)

Duke Energy

Duke Energy SCADA Cyber Security Standard

Glossary of Terms

Non-Operational Business Need – the data access needs of "marketing" or "casual" users of SCADA systems

Periodic - Recurring at regular, known intervals

Physically Isolated System - any computerized system that is not physically connected by any means to the Duke Energy computer network, the Internet, or any other network. "Physical connection" includes not only computer networks, but also modems or any other interface to any telephone system. The use of any broadcast wireless (radio, infrared, or any means of electromagnetic frequency) technology will preclude a system from meeting this definition. In Figure 1 above, the internal network is NOT physically isolated from the outside network because of the connection through the firewall.

Physical Security Perimeter -- The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled. If this perimeter cannot be established, then an alternate perimeter must be documented and deployed. A physical perimeter of a four-walled locked fence (of the type normally protecting a facility such as a substation) would suffice.

Plant Control System (PCS) – a SCADA system that is typically confined within the physical perimeter of a centralized facility, typically an energy conversion or processing plant.

Policy - high level statement of enterprise beliefs, goals, or courses of action adopted in support of principles and objectives. They provide a statement of position or intent in a specific subject area.

Procedure - provide specific details of how a policy and supporting standards are to be implemented in a given circumstance. They are documented step-by-step instructions for a particular area. May exist at any level of the organization to implement policies and accomplish tasks.

Production Change / Firecall ID - is used in an emergency situation to quickly restore a critical application to operation. This ID typically has elevated privileges, i.e. administrator vs. user. Emergencies include, but are not limited to, operating system failure, application malfunction(s), or timing issues that require immediate attention.

Glossary of Terms

Recovery - the process of restoring a SCADA system to operational status.

Remote Node - remotely located devices, such as relays or Remote Terminal Units (RTU), located in unmanned locations.

Risk - the likelihood that vulnerability may be exploited, or that a threat may become harmful. Risk is defined as the probability that an undesirable event will occur, resulting in financial or other loss, or otherwise create a problem.

Router - a device that interconnects networks.

SCADA (Supervisory Control and Data Acquisition) - a system that allows the monitoring and control of physical devices remotely. In the context of this series of standards and procedures, "SCADA" will be used as a generic term to represent any kind of computing system that monitors, or monitors and controls, physical entities. See "SCADA Cyber Security Policy – 6000".

SCADA Host – a computer whose purpose is to consolidate field equipment information. A SCADA host typically polls and sends controls to field devices, and may also store data to a historical data base. It also functions as a data server for HMI requests.

Screening Router - a router is used to selectively permit or deny traffic at a network level.

Scripted Logon – A process (program) that runs at computer power-on or restart, and which contains an automated mechanism to actually logon using an ID. No human intervention is required to access the computer.

Social Engineering – Any technique used to gain unauthorized access to SCADA systems or facilities that is not specifically cyber in nature. Social Engineering is associated with fraudulent activities involving gaining the confidence of an employee to gain computer access.

Standard - Mandatory specific actions, rules, or regulations designed to prove policies with the support structure and specific direction needed to be meaningful and effective.

Glossary of Terms

System Software – Non-application software such as Operating Systems, Network Operating Systems, system utilities, and application frameworks.

Telnet - protocol used for login to a computer host.

Test Equipment – dedicated equipment not normally connected to or a part of a SCADA system, but which is used for testing, diagnostic, and/or calibration purposes only during maintenance and/or repair on SCADA equipment.

Third Party - someone other than the principals who are involved in a transaction

Threat - any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Users - in general, someone that accesses the SCADA System. Specific kinds include:

Read-Only Users – users of the SCADA system who only require read-only access to SCADA system generated data. These users regularly access this data and continually use the data for business decisions or input into business systems.

Primary Users – the users of a SCADA system with direct and continual responsibility for using the SCADA system to oversee the monitoring, control, and operation of a physical process, i.e., SCADA system operators)

Casual Users – ad-hoc users that access read-only data from a SCADA system on an infrequent or non-regular basis

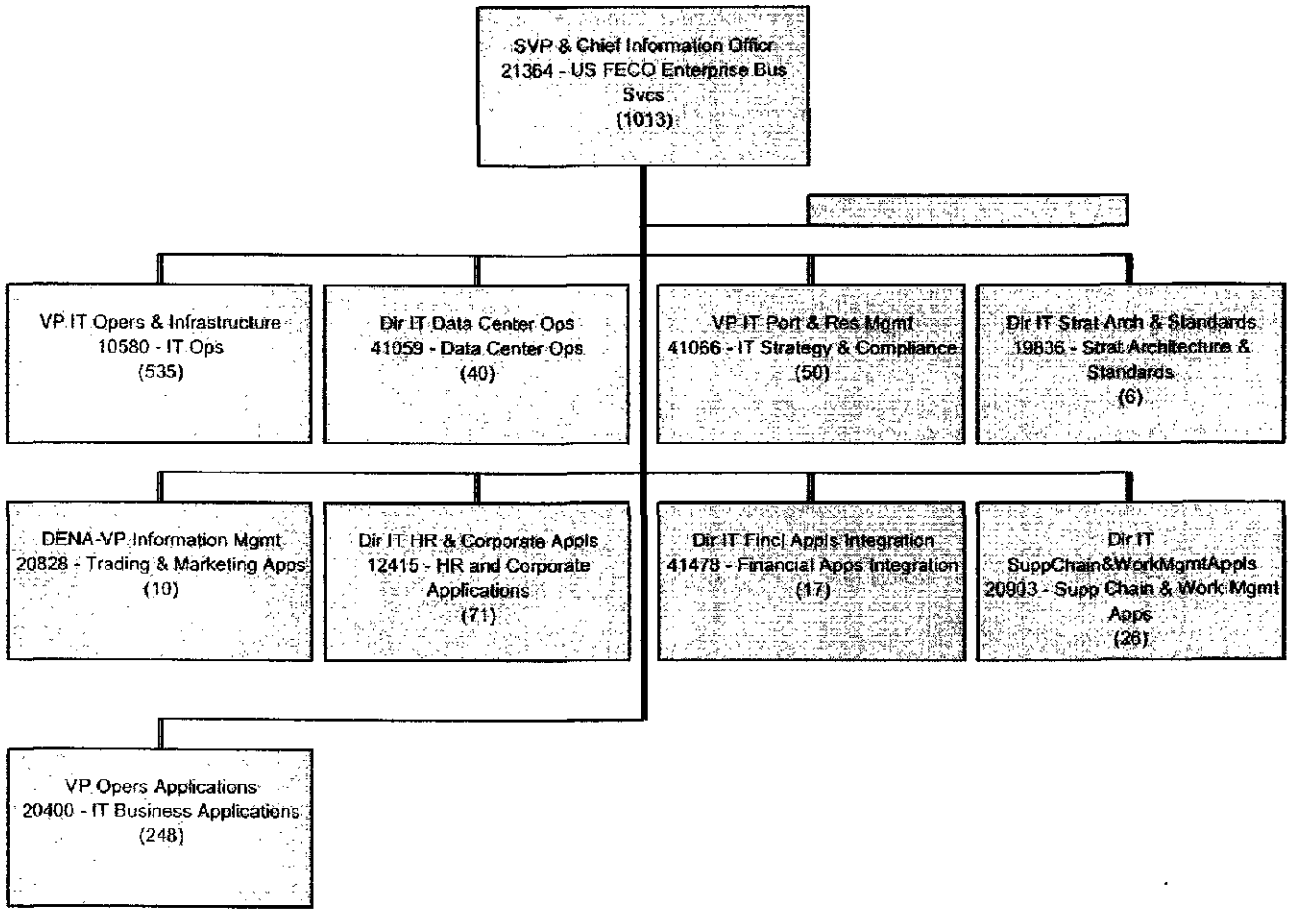
Virtual Private Network (VPN) - a VPN is used for highly confidential data transmission. It is an encrypted IP connection between two sites over the Internet.

Vulnerability - a weakness in computer information systems that could be exploited by gaining unauthorized access to information, disrupting critical processing, or violating a system security policy.

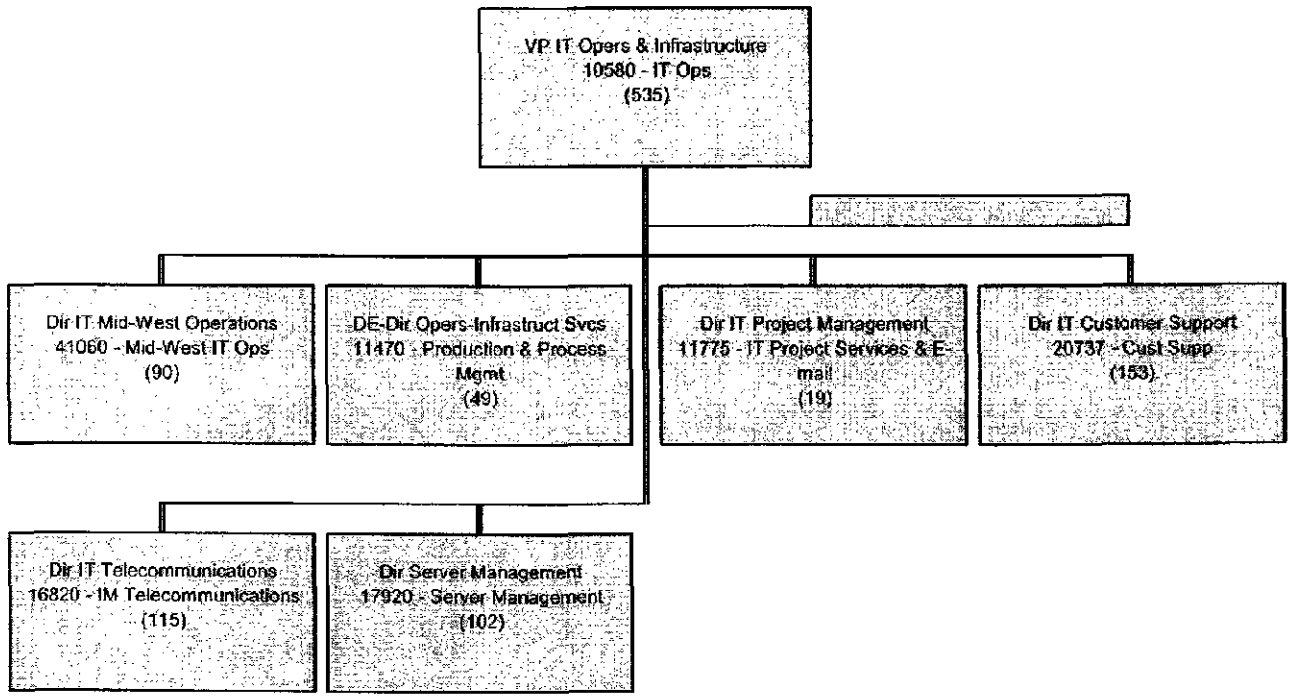
Glossary of Terms

DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

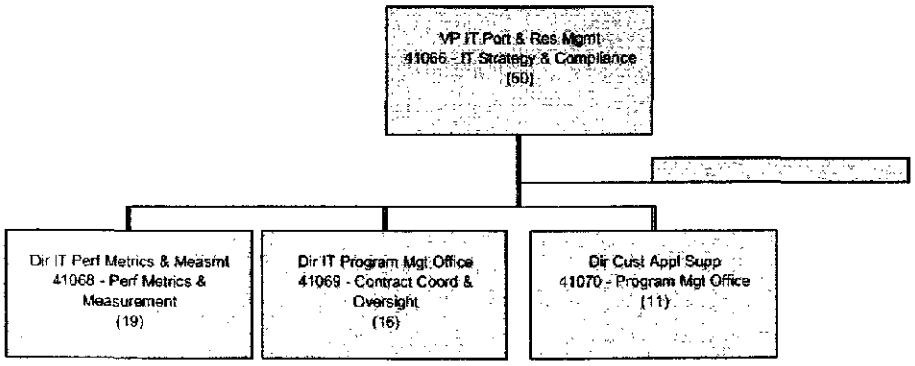
Senior Vice President & Chief Information Officer



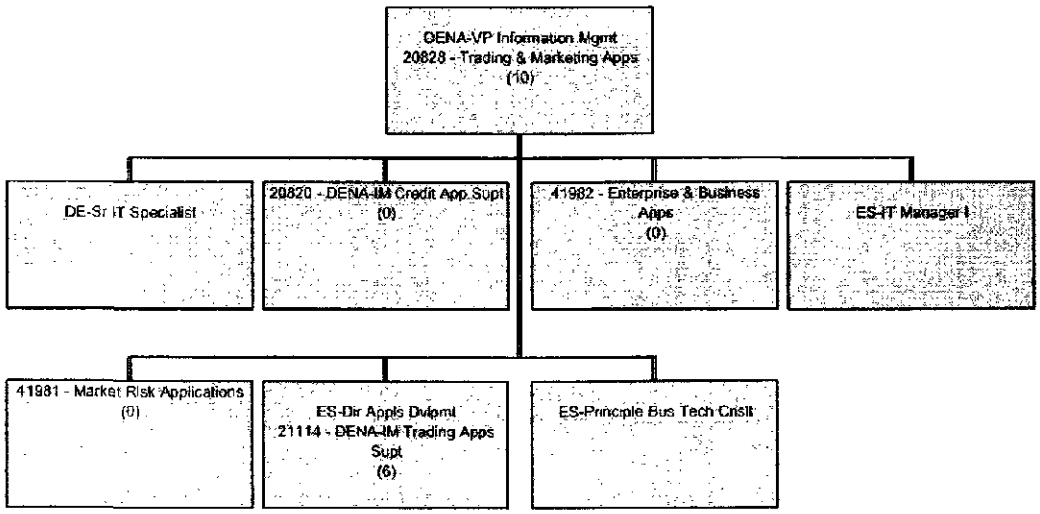
Vice President IT Operations & Infrastructure



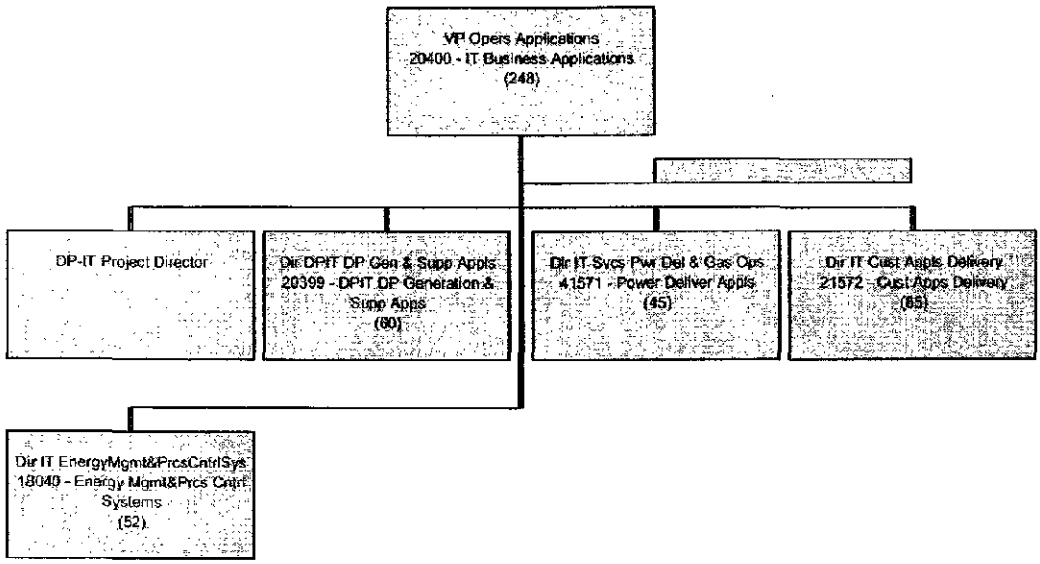
Vice President IT Portfolio & Resource Management



Vice President Information Management- DENA



Vice President Operations Applications



DUKE ENERGY
SUMMARY OF MANAGEMENT POLICIES, PRACTICES AND ORGANIZATION
ENTERPRISE OPERATIONS SERVICES DEPARTMENT
SFR Reference: Chapter II(B)(9)(e)(i,vi,vii)

I. Policy and Goal Setting

Enterprise Operations Services (EOS) sets policies for the respective departments/functions within this organization. Duke Energy's (the Company) policies are communicated to employees in both written and oral fashion and during departmental staff meetings.

Individual and team goals are developed each year for each department to create operational objectives. Creating operational objectives includes a process which identifies key targets and success factors, weighs them and combines them with desired behavioral, safety, customer satisfaction, and corporate financial goals. At the end of each year, achievements are evaluated and incentives are awarded proportionate to the level of overall achievement.

II. Strategic Planning

The executive management of the Company has the primary responsibility for establishing the Company's strategic plan. The Enterprise Operations Services organization has annual planning sessions to develop departmental strategic plans which are in support of the Company's strategic plan. Additionally, several Leadership Team meetings occur throughout the year to assess adherence to the established plan.

III. Organizational Structure

Enterprise Operations Services consists of the following six departments: Business Management Services, Enterprise Protective Services, Office and Creative Services, Real Estate Services, Travel and Project Services, and Change Management and Communications Services. Each of these department leaders reports to the Vice President of Enterprise Operations Services. All Enterprise Operations Services personnel are executive, managerial, supervisory, professional, technical, or administrative employees. Enterprise Operations Services also utilizes external

service providers to supplement the current workforce, and the workforce consists of both represented and non-represented employees.

Business Management Services includes the following areas: Financial and Data Management Services, Process Design and Performance Metrics, and Contract Management.

Enterprise Protective Services includes the following areas: Midwest Regional Management, Carolinas Regional Management, Preparedness Services, and Infrastructure Protection.

Office and Creative Services includes the following areas: Event Management Services, Creative and New Media Services, Copy and Print Services, and Document Services.

Real Estate Services includes the following areas: Portfolio Management, Transaction Management, Land Services, Facility Management Midwest, Facility Management Carolinas, Design Management, and Support Services.

Travel and Project Services includes the following areas: Aviation, Commercial Travel Services, Project Services, and Support Services.

Change Management and Communications Services provides change management consulting and communications support for Enterprise Operations Services departments.

The organization chart for EOS is attached as exhibit EOS-1.

IV. Responsibilities

Business Management Services has responsibilities for financial consulting, process consulting, metrics/measures reporting, Sarbanes-Oxley (SOX) 302 and 404 compliance, audit compliance, contract compliance, contract performance, and contract consulting for Enterprise Operations Services.

Enterprise Protective Services formulates and manages the strategic security, business continuity, and emergency response policies for the Company. These policies address physical security.

Office and Creative Services has responsibilities for comprehensive event and meeting support, online support services, graphics services, enterprise print and copy needs (including graphic services), and records management for the Company.

Real Estate Services is responsible for the operation, maintenance, design and construction of the properties under its jurisdiction in such a manner as to achieve effective and efficient business facilities expected by the Company's management, employees, and customers. Also, this Department is responsible for the valuation, purchase, lease, surveying, management and sale of all Company real property to adequately protect Duke Energy's interests and meet its needs. This Department provides oversight, and contract administration for the lease administration process.

Travel and Project Services is responsible for providing cost effective, safe and efficient corporate aviation travel for Duke Energy executives and commercial travel contracts for effective business travel for the employees of Duke Energy. This group also provides project management leadership to the department for department-wide projects such as workforce planning, training, etc.

Change Management and Communications Services supports overall department goals through effective change management consulting and communications services.

V. Practices and Procedures

The principal duties of the Business Management Services Department are:

- Financial Consulting in the areas of accounting, budgets, contracts, business case development, financial variance reporting, financial / accounting training, annual budget preparation, coordination and reporting, accounting reconciliations, funding request coordination, requisition processing, and invoice processing
- Process Consulting including process design, process improvement, process implementation, process monitoring, change management, EOS application planning and consulting, metrics/measures development and monitoring, management reporting, audit compliance, SOX 404 compliance which includes scope assessment, process documentation, management testing, deficiency remediation, and the assertion process, and SOX 302 process which includes quarterly assertions of changes in internal controls

- Contract Management includes contract compliance, contract administration, contract performance, research, and communication of best practices and benchmark data

The principal duties of the Enterprise Protective Services Department are:

- Business Continuity and Emergency Response including strategy and planning, assisting business units in contingency planning and plan preparations, and city/building evacuation plans
- Asset Protection including critical infrastructure identification and protection, security requirements, and regulation
- Investigations including fraud, theft, vandalism, workplace violence, threats, illegal substance investigations, and e-crimes
- Protective Services including Department of Homeland Security interface, U.S. Coast Guard Coordination planning, executive protection, strategic business investigations, technical services countermeasures, general security (uniformed guards), and event security planning

The principal duties of the Office and Creative Services Department are:

- Sports marketing and event venue management, event planning for internal and external events, audio-visual support, comprehensive event and meeting support for common conference and auditorium areas, video conferencing support, and event registration and surveying services
- Portal and external web program management, online support services such as web page design, content management and consultative services, graphics services such as graphic design, presentation design, technical writing, and proofing
- Management of enterprise print and copy needs ranging from the Copy Center, to all-in-one multi-function printers, to imaging/reprographics, to the desktop Printer strategy
- Record Management Program Office, operational records centers, electronic datafeed management (syndicated content), company archivist and other research services, and engineering document control

Copies of the records management policy and standards are attached as Exhibits EOS-2 and EOS-2.1

The principal duties of Real Estate Services are:

- Operating and maintaining the commercial facilities owned and leased by the Company

- Inspect all Company properties on an ongoing basis to identify needed maintenance, improve operational efficiency and establish programs to eliminate fire and other safety hazards
- Cooperate with operating departments in the design, construction, and furnishing of space in new and remodeled office, service, and garage buildings in accordance with building standards
- Assist the various departments housed in corporate buildings in making office and equipment layouts so that all space is efficiently used
- Maintain space allocation records (Facilities Services)
- Keep existing office furnishings in good condition and provide a pool of furnishings for use by various departments during periods of heavy workload
- Maintain contacts for the following:
    - local and national contacts for the purpose of keeping abreast of new concepts of building management, improved methods of operation, new and better materials, more efficient space utilization, and methods of reducing operating costs
    - in the office furnishings fields, keeping abreast of new technologies that can reduce costs and improve productivity. Provide centralized ordering and maintenance of office furnishings
    - in conducting departmental real estate operations, personnel work closely with all other Company departments, and, in particular, with the Engineering, Planning, Environmental, Legal, and in addition our own Facilities groups
- Serve as the Company's agents to purchase, sell and lease real estate, including surveying of real estate, and maintain records of real estate transactions; Representatives also act as rental agents and property managers for all temporary surplus property until property is either used or sold
- Ensure Duke Energy's leasehold rights are maintained through effective management and oversight of leased real estate assets

The principal practices and procedures used by the Travel and Project Services department include the following:

- Aviation Flight Operations Manual and the International Operations Manual management
- Compliance management in accordance with the Commercial Travel Process/Procedure and Employee Expense Procedure/Policy (i.e. policy / procedure interpretation)

- Oversight and reporting of commercial travel transactions
- Scheduling and monitoring executive travel transactions
- Travel contract management
- Assurance of positive traveler experience
- Scheduling and dispatching, including maintaining flight logs
- Hanger aircraft maintenance
- Net Jets management and other aircraft services
- Project management for departmental projects

A copy of the travel policy is attached as Exhibit EOS-3.

The principal duties of Change Management and Communications Services are:

- Managing department change/communications strategy and communications calendar
- Providing change management consulting and support for major department initiatives
- Coordinating and publishing a bi-monthly newsletter that support department strategy
- Managing internal web site content for corporate shared services information
- Ensuring corporate branding and communications standards are used in all department communications

VI. Decision Making and Control

The decision making process for Enterprise Operations Services revolves primarily around the needs of the Company. Overall direction and broad concepts for customer service and satisfaction are communicated by the Vice President of Enterprise Operations Services. The leaders of Enterprise Operations Services then provide more specific guidance to employees within each function.

All employees within each function are expected to make decisions and exercise control over their areas of responsibility within the parameters of those boundaries, reporting results to their immediate management on a regular basis.

All financial/purchasing decisions are made in accordance with each individual's proper delegation of authority.

VII. Internal and External Communication

Enterprise Operations Services maintains open channels of communication for exchange of information and ideas within each function and across functions. The EOS Leadership Team meets several times throughout the year to discuss strategies and results. Additionally, an electronic inter-departmental newsletter is circulated to all EOS employees on a bi-monthly basis.

Communication channels to other areas of Duke Energy include the Portal, e-mail, and hard copy memos. These methods are used to communicate instructional information related to new practices/tools, safety awareness, and general information. There are also processes in place to contact certain members of Enterprise Operations Services during non-business hours.

In addition to inter-departmental and inter-company communication, Enterprise Operations Services also communicates with the following major external parties via various methods:

- Federal Aviation Administration (FAA)
- Airport personnel in various cities, Fixed Based Operator (FBO), etc.
- Federal, state, and local law enforcement
- Department of Homeland Security
- Various intelligence agencies
- Hotels
- Sports Venues
- Department of Transportation
- Fire departments
- Building/land permit agencies
- City tax offices
- Department of Natural Resources
- Commission of Public Water Works
- Governmental County courthouses

VIII. Goal Attainment and Qualification

Enterprise Operations Services sets incentive goals on an annual basis. Results of these goals are reviewed and approved at the end of each calendar year. In addition, inter-departmental key performance indicators have been established for each

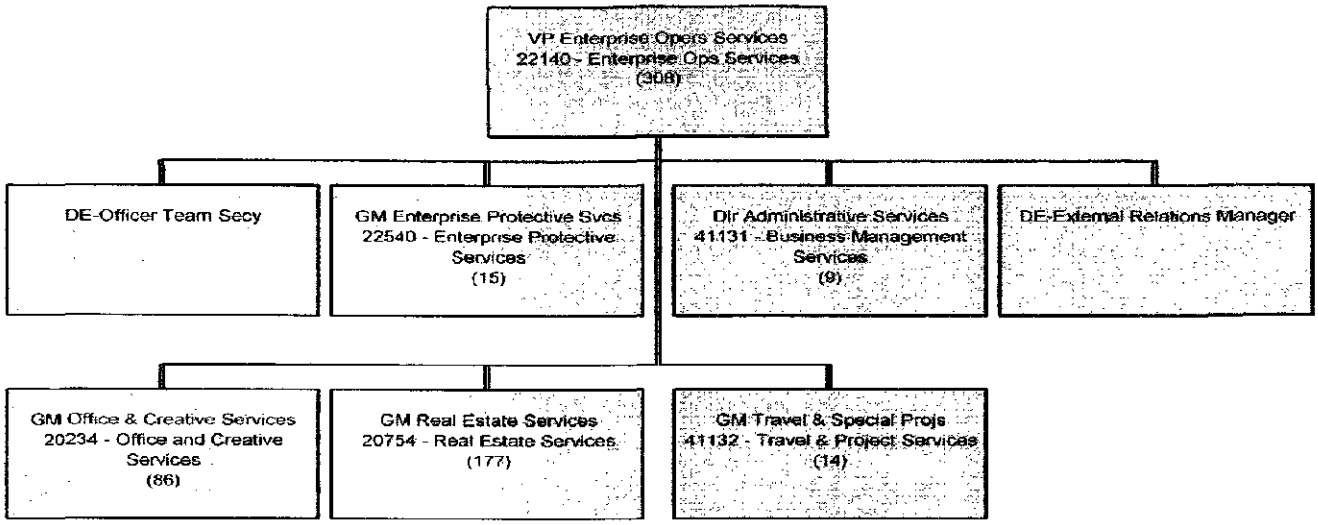
function, and they are reported on and shared with EOS employees on a monthly basis.

Specific projects or actions that have been identified as additional goals are monitored at functional staff meetings and Leadership Team meetings to assess status and results. Any results that are subjective in nature must be approved by the Vice President of EOS. Additionally customer satisfaction surveys are utilized for certain services and also to assess the overall satisfaction of internal Duke Energy customers with EOS's services.

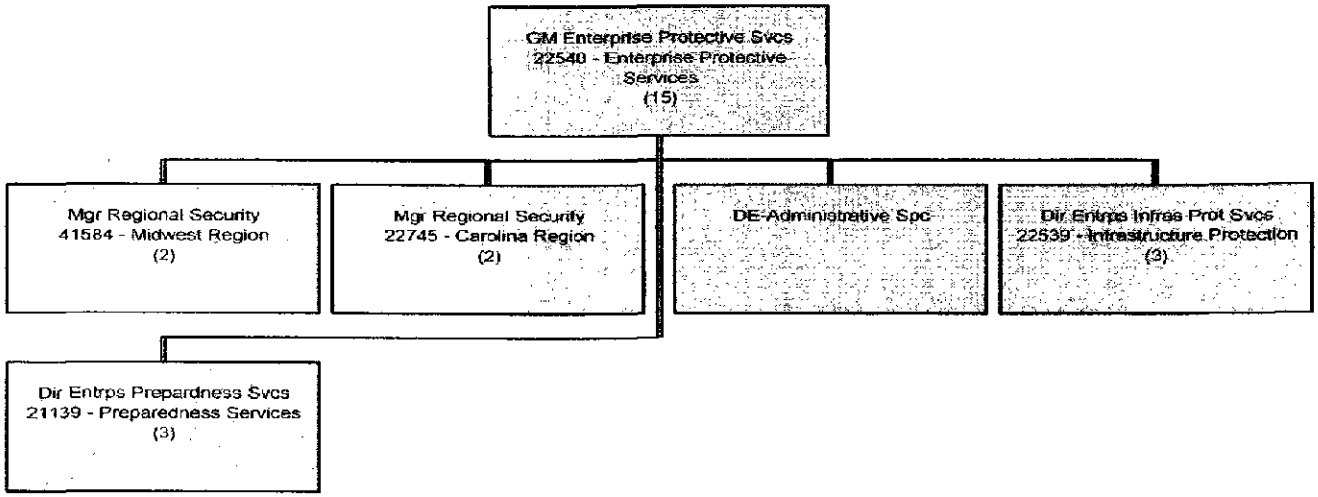
Goals and related results which have been identified for individual employees are also reviewed during the annual evaluation of these employees.

DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

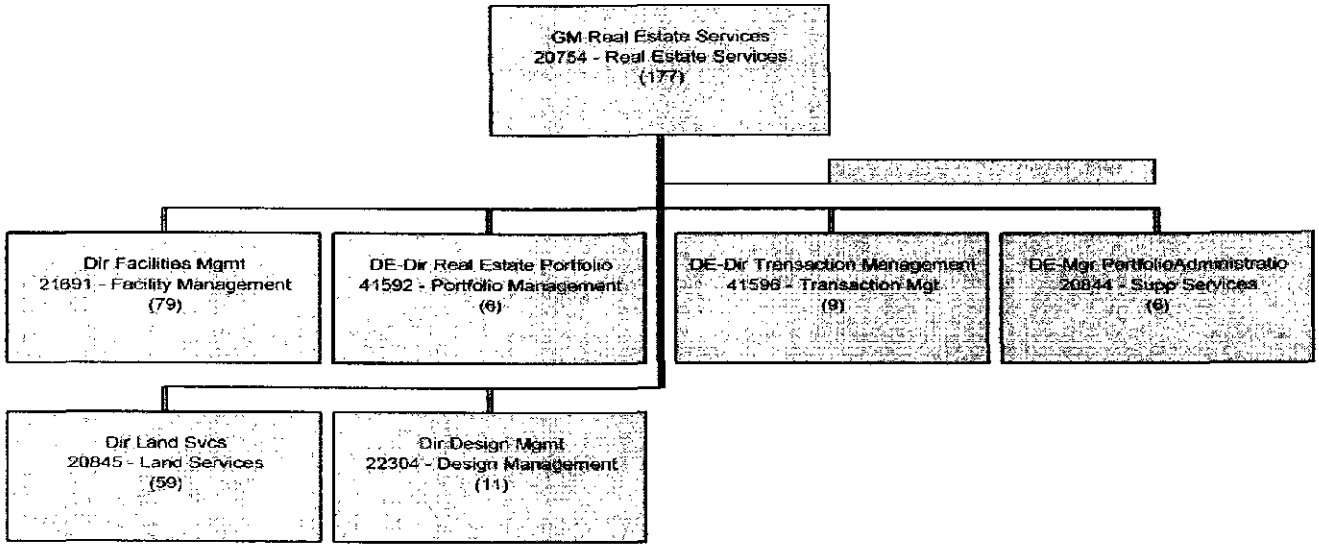
Vice President Enterprise Operations Services



General Manager Enterprise Protective Services



General Manager Real Estate Services



Records Management Policy

Applicability:	Applies to Enterprise
Originator:	Records Management Office
Approval:	DE-GVP Gen Consl & Secy
Effective Date:	08/31/2000
Revision Date:	08/29/2005
Reissue Date:	09/01/2005

Statement of Purpose and Philosophy

In any company, complete and accurate records are a necessary part of doing business. Duke Energy will comply with regulatory and business operational requirements in the management of the corporation's informational assets (business records). A comprehensive approach to records management is required to ensure all types of business records, regardless of media type, are managed appropriately.

Policy Expectations

This policy is to be consistently applied throughout Duke Energy. Any supplemental records management or retention directive is subordinate to this policy.

Duke Energy retains ownership of all records created for business purposes. Duke Energy employees must adhere to proper practices related to the creation, disclosure, retention and destruction of business records.

Accountability: Roles and Responsibilities

Records Management Program Office Responsibilities

The Records Management Program Office will be responsible for the direction, monitoring, and review of records management practices for Duke Energy. As such, they will be responsible for oversight of all Duke Energy records retention rules, including any Business Unit specific records retention rules.

The Records Management Program Office will also be responsible for coordinating with Functional / Business Unit teams to ensure the ongoing and effective records management program throughout the Duke Energy enterprise.

Functional / Business Unit Responsibilities

It is the responsibility of each Functional / Business Unit to create a Records Coordinator role and team that works in coordination with the Records Management Program Office. This is to ensure

that the Records Management Program objectives are achieved and that the applicable records management processes are sustained.

This team shall be responsible for representing their functional area to promote awareness and compliance with the Records Management Policy and Standard. They will also work with the Records Management Program Office to ensure Business Unit records retention rules are maintained current and correct.

Employee Responsibilities

It is the responsibility of Duke Energy employees to participate in training opportunities provided and ensure their daily practices comply with the Records Management Policy and Standard. Each Duke Energy employee is responsible to ensure that any original or copies of original Duke Energy records within their possession and/or control are managed in accordance with this policy and the related standard and any applicable records retention rules.

Business Travel Policy

Applicability: Applies to Enterprise
Originator: Corporate Travel and Services
Approval: Group Vice President, Duke Energy Business Services

Effective Date: 01/01/2001
Revision Date: 11/16/2006
Reissue Date: 11/16/2006

Statement of Purpose and Philosophy

This policy was established to ensure that the travel procurement process is conducted in compliance with all laws, regulations, and Duke Energy standards, and that all travel-related business is conducted in a fair, equitable, and highly ethical manner utilizing appropriate internal controls and best efforts to maintain confidentiality in our dealings with reputable and responsible suppliers.

Policy Expectations

Corporate Travel Arrangements

Employees are required to book business travel arrangements through Duke Energy's designated travel offices or through Duke Energy's designated on line booking tool. The corporation will not reimburse employees for air travel and car rental expenses not secured through the designated travel offices.

Preferred Providers

Duke Energy is continually seeking discount pricing agreements with business travel providers. Employees will be required to use car rental firms and hotels with which the enterprise has corporate or negotiated rates, whenever possible. Employees will be required to use preferred airline carriers for business travel in specified markets based on contractual commitments.

Accountability: Roles and Responsibilities

Travel and Project Services will provide guidance to travelers, travel arrangers, approvers, and auditors on cost-effective management of travel and entertainment expenses. Corporate Controller-Corporate Controls Group will be consulted on control issues.

The business/corporate unit head can approve individual exceptions to this policy, when necessary, to accommodate pressing business needs that the designated travel booking processes cannot serve.

Employees traveling on company business are responsible for reviewing and adhering to the enterprise travel procedures located on the Portal.

Travel and Project Services will provide periodic reports on compliance to the business units.

Duke Energy

Duke Energy Standard

Records Management Standard

Applicability:	Applies to Enterprise
Originator:	Records Management Program Office
Approval:	Group Vice President, General Counsel and Secretary
Approval Date:	08/29/2005
Effective Date:	09/01/2005
Revision Date:	08/29/2005
Reissue Date:	09/01/2005

Statement of Purpose and Philosophy

Information in our business is created, delivered and exchanged in many ways. Duke Energy employees create and maintain a variety of business records in many forms, including but not limited to: presentations, e-mail, paper documents, engineering drawings, video, and databases. All business records are the property of Duke Energy.

This Standard is intended to supplement the Duke Energy Records Management Policy by providing specific expectations for the management of Duke Energy records. This Standard is intended to be used in conjunction with the applicable records retention rules and departmental directives.

Standard Expectations

This Standard is to be consistently applied throughout Duke Energy.

All Duke Energy employees are expected to be familiar with this Standard and ensure they manage records within their responsibility consistent with the practices outlined in this Standard.

Records Creation

Documents should only be created when:

- There is a legitimate business need.
- The creator has the appropriate knowledge to create the document.
- The creator has the appropriate work authority to create the document.

Documents should always be thoughtful, precise and well written and **should not** contain:

- Speculation, conclusions or opinions that are without factual support.
- Words or phrases that are imprecise, and therefore susceptible to different or confusing interpretations.
- Promises or commitments that cannot be kept.
- Dramatic or inflammatory words or phrases.
- Statements that could do harm to the brand or reputation of the Company.
- Legal conclusions or opinions not approved by the Law Department.

Duke Energy

Duke Energy Standard

Records Management Standard

Documents that could have potential legal implications should always be reviewed by the Law Department.

Duke Energy

Duke Energy Standard

Records Management Standard

Access and Disclosure

Access and Disclosure of records should be managed in accordance with any requirements set forth by the following:

- Code of Business Ethics (COBE).

  Code of Business Ethics information is available on the Our Charter and Values gadget on the Duke Energy Portal Page.

- Protected Critical Infrastructure Information and Safeguards Requirements.

  Please refer to appropriate Business Unit requirements.

- Affiliate Rules and Standards of Conduct.

  Please contact your manager, business unit general counsel, or FERC compliance personnel for any questions related to applicable Affiliate Rules obligations for your job responsibilities.

- Data Privacy Obligations.

  Please contact your HR Consultant for any questions you have related to Data Privacy.

- Business Expectations Regarding Confidentiality.

  Please contact your manager for any questions you have on records and information that should be considered confidential or proprietary.

- Copyright Laws.

Employees shall ensure that any vendors or third parties that have business needs for Duke Energy records understand and comply with the Duke Energy Records Management Policy, this Standard, and applicable departmental directives for access and disclosure requirements.

Storage

Records shall be stored in accordance with or at locations prescribed in special storage guidelines noted in applicable records retention rules. In those cases where departments or functional areas have developed storage strategies, guidance should be readily available in the applicable records retention rules or department directive.

Business Continuity and Criticality

Acceptable records storage strategies shall be developed to ensure that any records deemed vital, or required from a Business Continuity standpoint are maintained and accessible when needed. This may include provision for off-site storage as necessary.

Retention

The Records Management Program Office shall govern the development and maintenance of records retention rules for Duke Energy. As much as practical, records retention rules will be developed for Duke Energy (enterprise rules).

Duke Energy

Duke Energy Standard

Records Management Standard

Business Unit specific records retention rules must be reviewed, approved and maintained by the Records Management Program Office.

Records retention rules will be classified as either:

- Legal Citation Rules – Legal citation rules have a legal / regulatory basis for their categorization and retention/disposition. Where similar or same record types are governed by multiple regulations, a single rule will be developed that aggregates the requirements of the multiple citations. Legal citation rules will take precedence over operational rules.

- Operational Rules – Operational rules do not have any legal / regulatory basis, but provide guidance to employees on expectations for recordkeeping. They should be broad in nature and kept to as few as possible.

Records shall be maintained for the time prescribed in the applicable records retention rule. Records shall not be maintained beyond the designated time, unless specific instructions and processes have been provided by the Law Department.

Special Legal Requirements

The following describes the expectations of the Legal Hold Order Process:

- A legal hold order process allows Duke Energy to exclude records from destruction when any legal, regulatory or compliance action is threatened or pending.
- Legal hold orders will be initiated by the Law Department and must be honored by the parties involved within the functional and business units. The Law Department will explain any obligations to suspend and or resume normal and routine retention efforts.
- All employees subject to a legal hold (and their management) are responsible for ensuring compliance with legal hold order instructions.

Disposal and Destruction

Methods of records disposal or destruction shall be chosen to ensure there is no risk of inappropriate disclosure. In cases of confidentiality or non-disclosure, paper records should be shredded or disposed of in a way that ensures no unwanted disclosure. For electronic records, methods prescribed by the Enterprise IT Security Standards (IT5000 Series) shall be employed.

Sustaining Processes

The Records Management Program Office is responsible for the coordination of activities to ensure effective records management processes. Such coordination includes, but is not limited to, the development of an annual Records Management Plan that includes:

- Calendar for Records Coordinator meetings.
- Schedule for periodic review and update of records retention rules.
- Development of scheduled projects and activities (such as clean-up days, training and communications) deemed appropriate for the maintenance and continuous improvement of Duke Energy records management processes.
- Calendar of Program compliance auditing and reporting.

Duke Energy

Duke Energy Standard

Records Management Standard

The Annual Records Management Plan shall be submitted to the Law Department for approval by the end of the first calendar quarter.

DUKE ENERGY
DUKE ENERGY OHIO
SUMMARY OF MANAGEMENT POLICIES, PRACTICES AND ORGANIZATION
Enterprise Field Services
SFR Reference: Chapter II (B)(9)(b)(v), Chapter II (B)(9)(e)(i)

I. Policy and Goal Setting

The Enterprise Field Services Department which includes Fleet, Meter Operations and Warehousing does not issue policy statements per se, but supports the corporate policies embodied in the Working Environment Policy Manual. These policies, which are provided to company employees, are supported through departmental directives, procedures and practices. All managers, superintendents, and supervisors are responsible for assuring that their subordinates are complying with corporate policy.

The managers and Directors establish department annual goals and objectives each year, with the assistance of the Vice President of Enterprise Field Services, based on the various business units' annual business plans. Department goals and objectives are reviewed throughout the Enterprise Field Services area, which in turn formulates organizational goals, which are then submitted to senior management for consideration and to ensure they support the corporate strategy. This information is used in developing department operating budgets and goals for the coming year. Generally these goals are to manage total operation and maintenance costs to effectively support the Fleet, Meter Operation and Warehousing needs of the company.

A status report of performance in accomplishing Department goals and objectives is submitted quarterly to the Group Executive and Chief Administration Officer and a final report for the year is submitted in January.

II. Strategic Planning

The Director of Strategic Business for Fleet, Meter Operations and Warehousing and key personnel, in consultation with the Vice President of Enterprise Field Services and senior clients, develop the overall process of strategic planning within the Enterprise Field Services department. These individuals establish goals, objectives and direction for the department.

Operational planning is strongly influenced by the corporate objectives. After receipt of the annual corporate objectives, the department begins developing each

group's operating budgets and goals for the coming year. This planning consists of prioritizing budget requests and identifying related personnel needs and allocation.

This department is primarily a service organization to the other departments throughout the Company. As such, Enterprise Field Services coordinates with Power Delivery and Power Generation to develop their service model.

III. Organizational Structure

The Director of Strategic Business, the Managers of Warehousing and the Vice President of Fleet and Meter Operations report to the Vice President of Enterprise Field Services.

Fleet has four divisions with the supervisors of these divisions reporting to the Director of Midwest Fleet Operations:

- Two divisions support several Transportation Service Centers in the greater Cincinnati area identified as North and South, each with an equal share of equipment or other responsibilities under each division supervisor. In addition, both divisions provide liaison support for PSI District Operations. These divisions provide operations, maintenance and repair support for all mobile vehicles of the Company;
- The Plainfield Division supports all of the PSI service territory in Indiana;
- The divisions discussed above are supported by Administrative Operations. With a supervisor, this division provides administrative, systems, and materials support for the department and systems support for the users of vehicle inventory and transportation systems;
- A Transportation Analyst provides daily support for the computerized Duke Energy Transportation System and the Vehicle System (VHS), and other data analyses and systems controls for the department. In addition this position serves as the lease administrator for Transportation equipment. This position also reports to the Director of Strategic Business; and
- A Transportation Vehicle Specialist provides direction for the design and specification of Transportation equipment along with vendor liaison. This position reports to the Director of Strategic Business.

The Company has eleven Transportation Service Centers (TSC). Each TSC has a day shift, and nine also have a night shift. Two Transportation Supervisors cover the activities of the day and evening shifts of the eleven Service Centers. They each report to the Director of Midwest Fleet Operations.

An organization chart is included as Exhibit TP-1.

Meter Operations has two divisions with the Director of these divisions reporting to the Vice President of Fleet and Meter Operation:

- One division supports the meter needs for both our Gas and Electric in the Midwest, Indiana, Ohio and Kentucky. The other division supports the electric meter needs in North and South Carolina. These divisions provide maintenance and repair support for all gas and electric meters of the Company;
- The Company has two meter operation centers – one in Cincinnati, Ohio and one in Charlotte, NC.

Please see the organization chart included as Exhibit TP-1.

Warehousing has four divisions with the Managers of these divisions reporting to the Vice President of Enterprise Field Services:

- Two divisions support the Midwest material needs for both the Power Delivery and Generation Departments. These divisions store and deliver materials for the Power Delivery and Generation Groups. There are 10 major storerooms strategically located in Indiana, Ohio and Kentucky.
- Two divisions support the Carolina's material needs for both the Power Delivery and Generation Departments. These divisions store and deliver materials for the Power Delivery and Generation Groups. There are 8 major storerooms strategically located in North and South Carolina.

Please see the organization chart is included as Exhibit TP-1.

IV. Responsibilities

The major objectives of Enterprise Field Service are to provide centralized, efficient, high quality support services to Duke Energy Ohio and its subsidiaries, and to Duke Energy Indiana.

The Fleet Services division's major responsibilities are as follows:

- Provide and manage transportation resource control systems that require accurate reporting and encourage efficient utilization, reduced investment, and operational care of transportation equipment;
- Provide transportation equipment and services to support operations in a manner that is competitive with outside contractors for lease alternatives and sufficient to safely satisfy normal and emergency operations;
- Distribute transportation costs equitably to the user vehicle assignments on the basis of actual operation, maintenance, depreciation, and other vehicle related costs;
- Responsible for all the activities related to replacing, servicing and maintaining the fleets of vehicles.

The Meter Operations division's major responsibilities are as follows:

- Provide and manage meter operations' resources, and encourage efficient utilization, reduced investment, and operational care of meter equipment;
- Provide meters and services to support operations in a manner that is competitive with outside contractors and sufficient to safely satisfy normal and emergency operations;
- Repair and refurbish the gas and electric meters

The Warehousing Division's major responsibilities are as follows:

- Provide Storing and handling of all materials required by Power delivery and Generation.

V. Practices and Procedures

It is the practice of Enterprise Field Services to have internal service level agreements with the business units using transportation equipment and/or having associated responsibilities. Certain duties are understood through these agreements and are described below as general, specific or associated.

General Duties

Generally, Enterprise Field Services duties include:

- Maintaining knowledge of utility mobile equipment and fleet management techniques through technical literature, participation in technical and trade organizations, such as, American Gas Association (AGA) and Edison Electric Institute (EEI), and visits to manufacturers' facilities;
- Specifying chassis, bodies, and mounted equipment to meet the requirements of Company vehicle assignments;
- Recommending timely vehicle replacements for a safe and capable fleet;
- Acquiring equipment, materials, and services required to own and maintain the fleet;
- Repair and refurbish gas and electric meters.
- Storing and handling and delivery of required materials for Power Delivery and Generation.

Specific Duties

Specific duties of Enterprise Field Services include:

- Hiring and training employees to support the various operations;
- Operating and managing Duke Energy's Transportation System (CTS);
- Preparing the Enterprise Field Services Budget;
- Specifying and ordering new vehicles;
- Managing the meter inventory and assuring refurbishment dates are met.

- Overseeing the material storage requirements and handling materials and assuring timely deliveries of material.

Associated Duties

The department supports and works closely with all departments who use the services provided by Enterprise Field Services. It also works closely with the Supply Chain Department in vendor equipment demonstrations, equipment order discussions, and stocks for the storerooms, and with Tax and Plant Accounting for fuel tax, highway use tax, vehicle life studies and fleet inventory records.

Other departments with which Enterprise Field Services interacts include the following:

- Risk Management division of Treasury Department for accident claims;
- Human Resources Department for driver safety records, driver records files and other employee matters;
- Treasury Department for lease/purchase analyses and coordination of Transportation Equipment Budget; and
- Payroll and Accounts Payable Departments for payroll summaries, work orders, sales orders, invoices, vehicle charge rates and transportation.
- Generation Stations for material requirements.
- Power Delivery for meter and material requirements.

VI. Decision Making and Control

The planning/decision making process depends largely on the value of expenditure and potential impact of the decision to be made.

Participative management is practiced at all levels. The idea of "team" is understood both through the daily activities of the work place and the special groups formed with exempt and non-exempt employees to reach specific objectives. Some examples of special teams are: training, regulatory compliance alternative fuels, cost reduction, vehicle specifications and internal service coordination with T&D Operations, Gas Operations and Supply Chain Services.

On a monthly basis the department staff meets for an activity review. Topics of the meeting are mostly short-term problems or plans. Any general topics are usually discussed and decided at special meetings. The broad resource categories of the department are:

- Personnel;
- Service Center Facilities;
- Equipment and Tools;
- Fuels;
- Budgets
- Systems; and

- Regulatory Compliance.

VII. Internal and External Communication

Internal communications within the department staff are frequent during each day. Supervisors visit the Service Centers several times each week and are in phone contact several times during each day to discuss current vehicle maintenance work loads and labor status. About every two months the Manager meets with the supervisors for general discussions of issues within their division. Every month a meeting with all supervisors is held to discuss the status of department activities and current topics.

It is the responsibility of the Supervisors to provide or conduct monthly safety meetings with all the department employees.

Performance discussions/evaluations between supervisors and subordinates are held at least twice a year. These provide the basis for recognizing good performance and identifying and clarifying expectations. Those reviews become the framework for merit increases and promotions.

Internal customer service level agreements were established with the business units served by the various operations, particularly looking at the elements important to achieving service excellence.

Internal communications with supervisors and other employees of other departments are on a personal basis in most cases because the Service Centers are normally located at the Operating departments' headquarters. External company communication is ordinarily with vendors for technical consultation and parts specifications.

VIII. Goal Attainment and Qualification

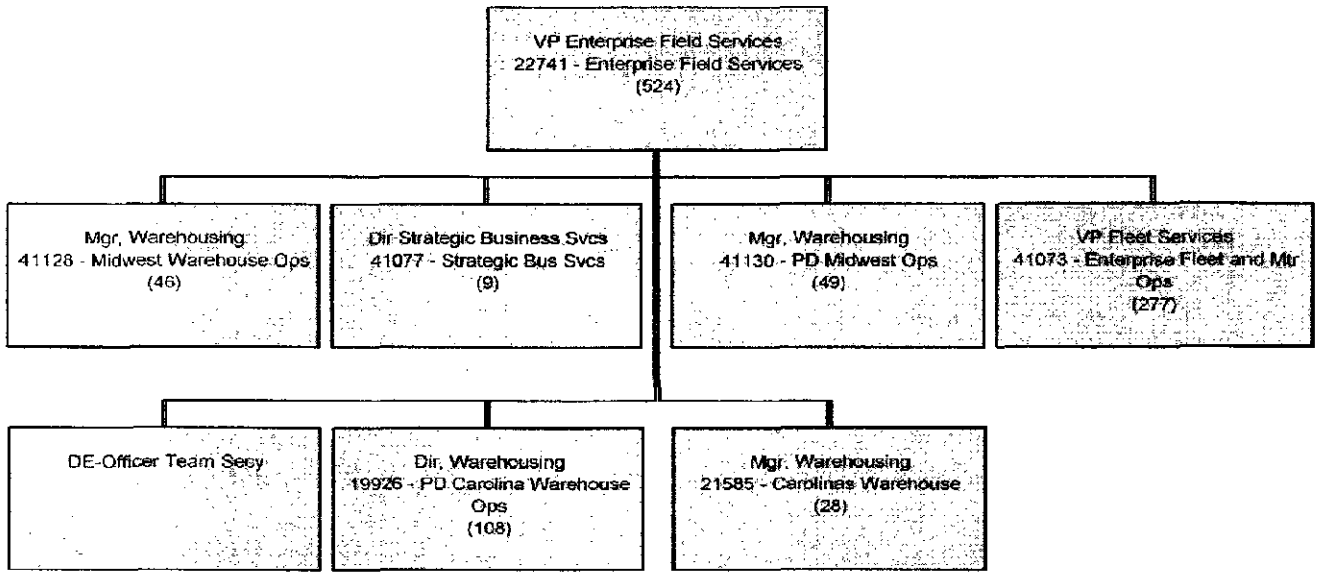
Goals of the Enterprise Field Services area in recent years have centered on production efficiency and cost reductions such as the following:

- In 2000 we entered into an alliance for our mounted equipment with ALTEC Industries, Inc. This has helped control costs associated with new and rental line and bucket trucks;
- In 2002 we implemented an automatic progression policy for the union mechanics in the Duke Energy Ohio service territory. This is an up or out program that not only requires experience but certain ASE certifications;
- In 2002 we outsourced the function of fuel purchase to Hightower Petroleum, Inc.;
- In 2006 we merged with Duke Energy and started capturing savings through the re-bidding of our lease contract for all vehicles and equipment.

- In 2006 we have entered into new contracts for Parts and Fuel both providing savings to the new Duke Energy.
- In 2006 we entered into a new contract for our mounted equipment with ALTEC Industries, Inc. This will helped control costs associated with new and rental line and bucket trucks;
- In 2005 we entered into an agreement with Reed City to handle material management.
- In 2006 we implemented the Integrated Supply Initiative in generation warehousing in the Midwest.

DUKE ENERGY MANAGEMENT STRUCTURE

Vice President Enterprise Field Services



UPDATED
Schedule S-4.2

DUKE ENERGY
DUKE ENERGY OHIO
SUMMARY OF MANAGEMENT POLICIES, PRACTICES AND ORGANIZATION
SUPPLY CHAIN
SFR Reference: Chapter II (B)(9)(b)(v)

I. Policy and Goal Setting

Corporate work policies are established by executive management and are embodied in the Working Environment Policy Manual and the Duke Energy Code of Business Ethics, which are provided to all employees. These policies, which establish guidelines by which Duke Energy employees are expected to conduct business, are supported by Supply Chain Services. In addition, employees of Supply Chain Services are required to adhere to all corporate policies directly relating to the various materials and contract services functions.

The annual goals for Supply Chain are established in conjunction with the annual business plans for Duke Energy. Supply Chain leadership works closely in conjunction with operational leadership to establish sourcing and service goals for the organization.

II. Strategic Planning

Supply Chain uses a planning process that is updated annually for annual budgeting purposes and for long range planning with regard to inventory levels, personnel, facilities and equipment needs. The operating units provide similar information through their business plan to assist the Supply Chain Departments in planning decisions regarding the sourcing of material and services.

The Supply Chain Departments have goals that support the Corporate business plan:

- Deliver savings through sourcing activities that directly contribute to the target financial goals;
- Performance driven, customer focused culture that emphasizes and delivers optimal cost and productivity;
- Create a streamlined organization focused on internal customer satisfaction and continuous improvement that delivers a low cost, high value portfolio of services; and
- Delivers continuous process improvements in back office operations and supply chain support systems.

III. Organizational Structure

The Supply Chain Departments report to the Vice President and Chief Procurement Officer. The Corporate/Enterprise Supply Chain supports corporate and enterprise-wide departments and supports the supplier diversity activities in the company. The Power Delivery Supply Chain supports the needs of the electric transmission and distribution and the gas distribution operations. The Power Generation Supply Chain supports the needs of the power generation facilities. Supply Chain Operations provides back office support, including Accounts Payable and systems support for the other groups and end users of supply chain systems.

The Corporate/Enterprise Supply Chain is organized into four major functions:

- Sourcing (including the purchasing function);
- Alliance Sourcing Center of Excellence;
- Supplier Diversity; and
- Asset Recovery.

Organization charts of the Corporate/Enterprise Supply Chain Department are attached as Exhibit SC-1.

The Power Delivery Supply Chain is organized into three major functions:

- Sourcing (including the purchasing function);
- Trucking and repair operations;
- Materials Planning and Integrated Supply management

The Generation Supply Chain is organized into three primary functions:

- Strategic Sourcing Origination and Structure
- Transactional purchasing;
- Strategic Program management, including Integrated Supply management and Craft Labor strategy.

Supply Chain Operations is organized into four primary functions:

- Corporate Accounts Payable;
- Transaction Support;
- Financial Controls; and
- Major Program/Project Management.

IV. Responsibilities

The Sourcing and Purchasing functions within the Corporate/Enterprise, Power Delivery and Generation Supply Chains have the responsibility for all sourcing, procurement and contracting activities with the exception of the non-strategic

material procured through the Integrated Supply function for Power Delivery and Generation.

The Alliance Sourcing Center of Excellence in the Corporate/Enterprise Supply Chain is responsible for management of various corporate alliance initiatives, including strategy development, sourcing and contract negotiation, and contract implementation.

The Supplier Diversity function in the Corporate/Enterprise Supply Chain is responsible for the development and implementation of various strategies to manage the identification and inclusion of diverse suppliers in the sourcing and purchasing process.

The Asset Recovery function in the Corporate/Enterprise Supply Chain is responsible for the recovery, liquidation and disposal of identified surplus and obsolete materials.

The Integrated Supply function within the Power Delivery Supply Chain is assigned the responsibility for managing the contract with our Integrated Supplier (IS). The IS has been contracted to perform the purchasing, inventory management and replenishment functions for approximately 70% of material required by the Power Delivery business unit. Contracts for strategic materials are negotiated by the Power Delivery Sourcing function, with the Integrated Supplier assuming responsibility for execution against those contracts.

The Material Planner function is responsible for working with the Power Delivery internal customers to address issues around design changes, new products, changes in delivery locations and date, and to work with the internal customer groups to improve business processes and practices.

The Integrated Supply function within the Generation Supply Chain is assigned the responsibility for managing the contract with our Integrated Supplier (IS). The IS has been contracted to perform the purchasing, inventory management and replenishment functions for certain maintenance, repair and operations (MRO) material required by the Generation business unit.

The Craft Labor program management function within the Generation Supply Chain is responsible for the overall program management associated with craft labor contractors, including contracting strategy, contract negotiation and implementation.

The Corporate Accounts Payable function in Supply Chain Operations is responsible for maintaining accounts payable systems to provide control over the proper disbursement of corporate assets, to provide Management with information for use in the decision-making process, to maintain the vendor master file and to assure that accounts payable records are accurately maintained.

The Transaction Support function in Supply Chain Operations is responsible for end user system support, system administration of supply chain systems, maintenance of the stock item catalog and change management and end user training.

The Financial Controls function in Supply Chain Operations is responsible for Sarbanes Oxley testing and documentation processes and operational auditing of the supply chain function; and

The Major Program/Project Management functions in Supply Chain Operations are responsible for large initiative project and program management associated with new systems and/or major process changes in the organization.

V. Practices and Procedures

The Supply Chain provides corporate leadership in supply chain management by challenging conventional methods and creating superior value in an environmentally responsible manner.

The responsibilities assigned to the Supply Chain Departments are discharged through the application of various practices and procedures. The principal practices or procedures are as follows:

- To source and procure material, equipment and services in accordance with prescribed specifications at the most favorable total cost of ownership, terms and conditions. To perform routine and emergency sourcing, competitive bidding, ordering, expediting and logistics operations;
- To maintain confidentiality of competitive bidding and prices;
- To develop competition among reputable and responsible suppliers, including minority suppliers, and to ensure that the Company receives quality products and services;
- To establish and maintain fair, equitable and ethical relationships with suppliers;
- To review, on a continual basis, all purchased materials and supplies and to add to stock or reduce stock or remove from stock as the review indicates;
- To establish and maintain information for inventory authorized by the operating departments for regular and special requirements;
- To create business processes and procedures that ensure processes are controlled and accurate;
- To leverage industry and trade best practices in the design of new business processes for the Company;
- To train others in the Company to utilize capabilities of our systems and in the general policies and guidelines related to purchasing

- To review of original source documents to assure that transactions bear valid approval for payment;
- To verify the existence of supporting documentation;
- To perform various accounting balancing activities for accounts payable accounts in the General Ledger; and
- To provide special studies and reports that meet customer, regulatory, legal and audit requests

The Supply Chain Departments directly support all other departments of the Company. Close working relationships exist through cross-functional teams and participation in materials standards committees.

Presently, the Company utilizes the Indus Passport system for all activities related to the Supply Chain Departments. This system is used to manage inventory investment and provides up-to-date information to support the Sourcing, Integrated Supply and Materials Planning functions. Aided by the Passport system, the Supply Chain Departments optimizes inventory management by:

- Establishment of inventory and service level targets;
- Usage forecasting;
- Calculation of economic reorder quantities (EOQ);
- ABC classification of inventory;
- Materials requirement planning;
- Purchase order tracking and expediting;
- Obsolescence reviews;
- Maintenance of the material catalog; and
- Blanket purchase orders.

Material requests for engineered work from the engineering design groups are generally passed electronically to the Passport system at the completion of the work estimate, allowing for advance planning of materials needs.

VI. Decision Making and Control

The Supply Chain Departments support decision-making at the lowest appropriate level within the Department. Decisions are vested throughout the department through management as appropriate. Guidelines for making decisions are provided by various Corporate policies, Departmental policies, and procedures and authorized approval levels.

Monthly reports of performance are used to monitor performance.

VII. Internal & External Communication

Supply Chain Department staff meetings between the leadership and their direct reports are held on a monthly or more frequent basis. Topics concerning

personnel, operations, facilities, equipment, goals and processes are discussed as necessary at each staff meeting. .

The Supply Chain Departments publish monthly updates to all employees of the performance metrics. Certain key control reports are emailed on a regular basis to supply chain employees for remediation, such as blocked invoices.

Daily reports on operations metrics are published on-line and are available to all Company employees. These metrics include inventory balances expediting reports and open purchase orders.

External communication with the Company's supplier base occurs on a daily basis through a variety of means. Bid quotes are obtained on an oral or written basis by our purchasing personnel or by use of the Frictionless e-sourcing tool. This tool is a controlled, on-line means of exchanging information, drawings, and questions and ultimately of obtaining pricing from our suppliers. A comprehensive supplier focused web site at Duke Energy.com is used to communicate important information to suppliers, including links to our supplier code of conduct, electronic tools, registration and diversity certification.

Many suppliers receive our purchase orders through an electronic marketplace. This marketplace increases our speed to transmit orders by using the internet and allows suppliers to send us electronic purchase order acknowledgements and, in the future, an electronic invoice.

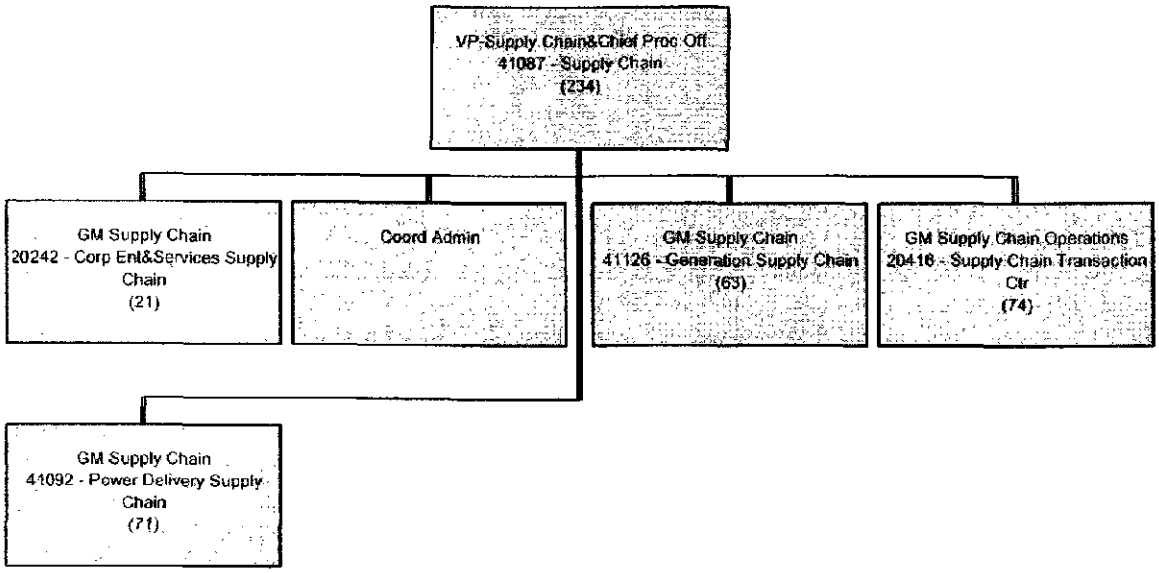
Suppliers and internal company users utilize the Supply Chain Help Desk to make inquiries and receive answers. This one-stop shop provides a centralized clearing house for the supply chain to understand user's issues and to work to answer supplier's questions in doing business with us.

VIII. Goal Attainment and Qualification

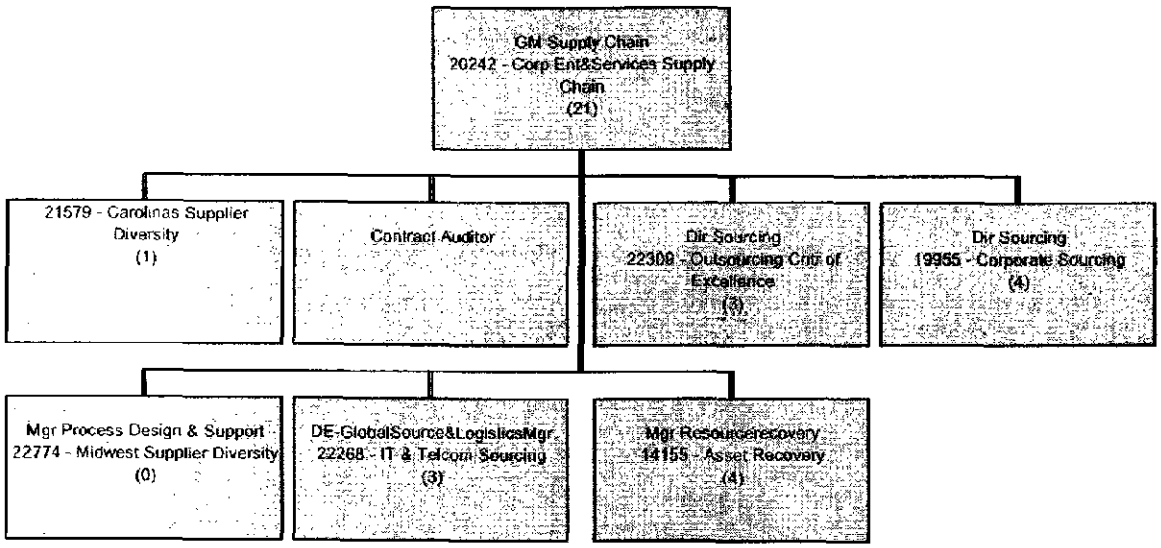
The Supply Chain Departments have developed a number of quantifiable indicators that are used to establish metrics which reflect our success in supporting Company goals and objectives. Goals are identified in the departments Short Term Incentive Plans. Listed below are a few performance metrics employed by the Supply Chain Departments:

- Savings achieved from sourcing activities;
- Integrated supplier performance;
- Supplier Diversity spend;
- Financial performance;
- Help Desk resolution performance; and
- Improvement in back office processes/streamlining procedures

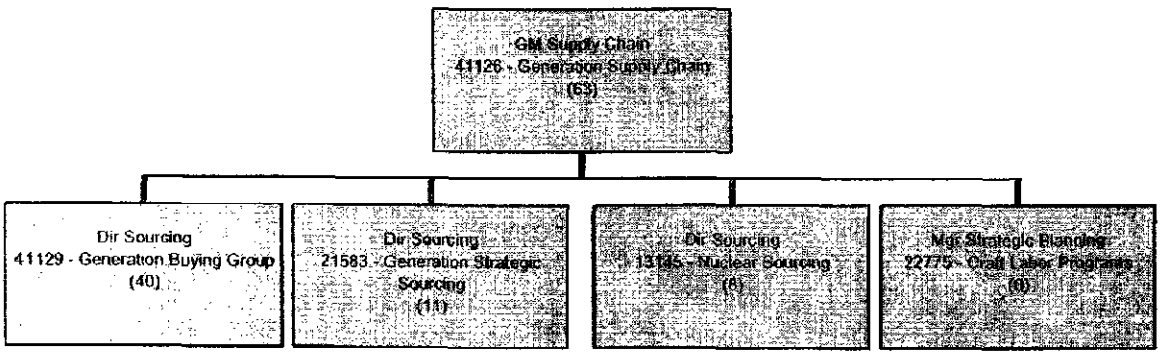
Vice President Supply Chain & Chief Procurement Officer



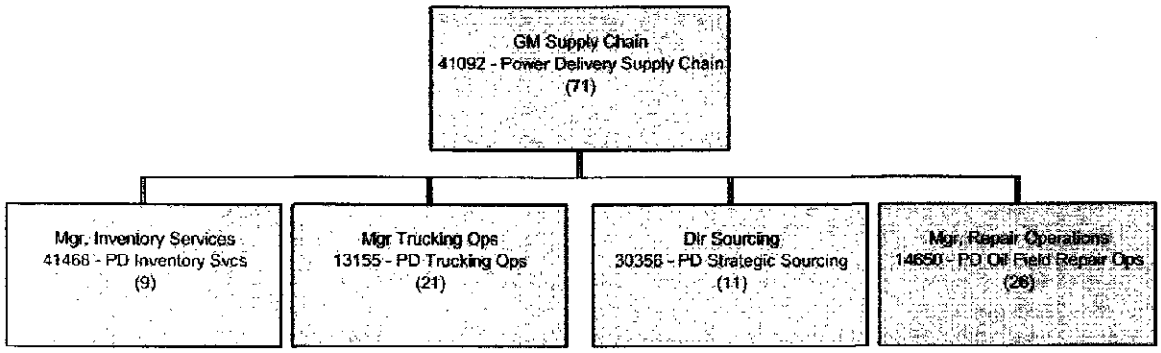
General Manager Supply Chain, Corporate/Enterprise



General Manager Supply Chain, Generation



General Manager Supply Chain, Power Delivery



CINERGY

BEFORE YOU BUY...

PURCHASING POLICIES AND GUIDELINES

PURCHASING DEPARTMENT

DECEMBER 1998

FOREWORD

The Purchasing function is one of the most common, yet vital, business activities. At Cinergy we remain committed to aggressive cost containment for the benefit of our customers and shareholders. By definition, purchasing involves securing products or services at a price acceptable to both the buyer and seller.

In practice, the Purchasing function encompasses locating, selecting, purchasing and/or contracting all materials, supplies, equipment and services used by our Corporation. To do so effectively and efficiently requires everyone's participation. We must continue to ensure that we are pursuing innovative ways to manage costs while maintaining an overall high quality of service.

With that in mind, this booklet has been prepared outlining the Corporation's Purchasing Policies and Guidelines. It is important that we comply with these policies and guidelines and that they become part of our everyday practice so that we continue to enhance our competitive position and the level of service provided to our customers.

James E. Rogers, Jr.
Vice Chairman, President and CEO

TABLE OF CONTENTS

1. **Standard of Business Conduct for the Purchasing Process**

Definitions 1-1

Responsibilities 1-2

Conflict of Interest. 1-3

Supplier Relations. 1-3

Gratuities 1-4

Antitrust. 1-5

Selling and/or Marketing. 1-6

Policy Interpretation. 1-6

2. **Purchasing Materials and Services**

Qualification of Suppliers and Contractors 2-1

Selection of Bidders. 2-1

Competitive Bidding. 2-2

Confirming Orders 2-3

Noncompetitive Procurements 2-4

Bid Evaluation 2-4

Supplier Diversity 2-6

Contract Compliance Program 2-7

Service Territory Buying Preference 2-8

Negotiations 2-8

Purchase Order Awards 2-9

Contacts 2-11

Conforming to Legal Requirements 2-11

Exceptions 2-11

3. **Requesting Quotations**

Less than $25,000 3-1

$50,000 or More 3-2

Sealed Bids 3-3

4. **Administering Contracts**

General Contract Definitions 4-1

In Practice 4-2

Responsibility 4-3

Procedures 4-4

Preliminary Planning Discussion 4-4

Contract Formulation 4-5

Negotiations 4-6

Contract Execution 4-7

Day-to-day Administration 4-7

Disputes 4-7

Amendments 4-8

5. **Making Foreign Purchases**

Justifying a Foreign Vendor 5-1

Evaluating Questionable Circumstance 5-1

Evaluating Bids 5-2

Awarding Bids 5-2

1. STANDARD OF BUSINESS CONDUCT FOR THE PURCHASING PROCESS

Cinergy complies with all federal, state and local laws, rules and regulations governing its operations. We encourage employees to conduct business with the highest legal and ethical standards. We want to continue to be responsible and responsive corporate citizens, acting in a moral, ethical and beneficial manner wherever we serve.

Definitions

The following standards of business conduct for the purchasing process reaffirm Cinergy's commitment to these principles. They apply to all Cinergy employees in both regulatory and non-regulatory activities who have a business need for products or services. *Purchasing* is Cinergy's Purchasing Department. *Suppliers* include any individual or organization furnishing material, items or services to Cinergy. *Vendors* include any individual or organization able to furnish or proposing to furnish material, items or services. *Clients* refer to the requisitioning Cinergy employees, departments or business units. *Purchasing Representatives* are authorized Purchasing Department Buyers and Sourcing Specialists. *Products* refer to equipment, materials and supplies, while *Services* involve professional or commodity services provided by a contractor.

Responsibilities

Cinergy will:

- Make sure all employees are aware of the standard of business conduct for the purchasing process.
- Make available continuing counsel on rules and regulations to any employee requesting it.

Supervisors will:

- Make sure all current and new employees under their supervision review and understand this policy and the non-union employee handbook section on the Code of Business Ethics and Conduct
- Stress to all employees the need for a continuing commitment to these principles.
- Make a personal commitment to ensure their organization operates with the highest principles of business ethics and conduct.

Employees will:

- Be alert and sensitive to situations that could result in illegal, unethical or otherwise improper actions, however inadvertent those actions may be.
- Advise fellow employees if it appears they are in violation of Cinergy rules and regulations. If an improper situation isn't corrected, you are obligated to speak with your supervisor. In the event you wish to remain anonymous, you may call 800-354-2714.
- Seek additional counsel from supervision if in doubt about responsibilities regarding this policy.

Conflict of Interest

As Cinergy employees, we are in positions of trust and should conduct ourselves accordingly. We must be particularly sensitive to the many situations, on and off the job, where a conflict of interest could occur. And we must recognize that sometimes even a perception of such conflict could cause harm.

If an employee or employee's relative (spouse, children, parents, brother, sister, in-laws) has an interest in any Cinergy supplier, any Cinergy employee must get prior written approval from the Vice President, Reengineering and Shared Services, before proceeding with any business transaction with that supplier. Stock ownership in the supplier company doesn't cause a conflict of interest as long as the company's stock is publicly or privately held and the employee's ownership is less than five percent of the company's outstanding stock .

Supplier Relations

Cinergy always employs the highest ethical business practices in source selection, negotiation, determination of awards and the administration of purchasing activities. We comply with applicable government laws and regulations at all times. And whenever possible we encourage, establish and maintain competition.

Cinergy insists that all commercial transactions involving suppliers and contractors be conducted at "arm's length". This means we try to prevent suspicion of favoritism or unethical practice on the part of employees or others responsible for, or who influence in any way, the outcome of such business activities. To that end, follow these guidelines:

- The identify of vendors invited to submit bids shouldn't be revealed to parties outside of Cinergy. Internally, discuss this information only with co-workers who need to know. This guideline does not preclude the holding of supplier

workshops or other similar meetings where the identity of bidders would become known.

- The appropriate Purchasing Representative notifies successful and unsuccessful bidders as to the results of their proposal. All other employees should refer requests for commercial information to a Purchasing Representative.
- No Cinergy employee is to reveal a competitive or current supplier's price information. We must refuse all requests by vendors for price information - the percentage they were high or low, the relative ranking of the bidders or any request that might in any way divulge price or the relative success of their bid. Report any such request to your supervisor and to the appropriate Purchasing Representative. Internally, discuss price information only with co-workers, consultants or engineering firms who need to know. Any deviation from this price disclosure policy requires the specific written approval of the Vice President, Reengineering and Shared Services.

Gratuities

Cinergy employees and members of their immediate families should neither accept nor offer gratuities. For this purpose, a gratuity is defined as entertainment, a favor or a gift that's more than nominal in cost. Gratuities are sometimes offered in return for or in anticipation of obtaining preferential treatment in the course of conducting business.

You may accept an occasional business meal when it's offered as a business courtesy without reference to unethical conduct or preferential treatment. You may return such a courtesy if your supervisor agrees.

Cinergy employees shall not solicit gratuities, favors or gifts from vendors. Occasional tickets to entertainment or sporting events, advertising novelties, or promotional gifts of nominal value may be accepted. However, the item should be one widely distributed to other individuals and firms under essentially the same business relationship with the offeror. Gratuities offered frequently from the same supplier are to be refused or returned.

Responsible management must review offers made by present or potential suppliers to provide expense-paid business trips. Generally, Cinergy bears the costs of flight on commercial aircraft and lodging. Employees shall decline all offers from suppliers regarding partially or fully paid-for pleasure trips.

During the time after bids have been received and we are evaluating bids, Purchasing employees and all other employees directly involved in the evaluation process should reject all gratuities offered by bidders to that project. Suppliers and contractors repeatedly or significantly failing to observe the provisions of this policy could be disqualified from conducting business with Cinergy.

Antitrust And The Foreign Corrupt Practices Act

The antitrust laws and the Foreign Corrupt Practices Act of the United States prohibit a wide range of transactions or practices.

Anyone with questions about how antitrust laws or The Foreign Corrupt Practices Act apply to a specific situation should consult a Cinergy attorney.

Selling and/or Marketing

Cinergy will not engage in unethical or illegal activity to win a contract nor pursue a business transaction to sell any product or service (including scrap and surplus sales), where unethical actions, or the appearance of unethical actions, are present. Cinergy will not engage in such business conduct and will not pursue that business any further.

When representing Cinergy, always make sure our contractual obligations are clearly defined. All information provided relative to Cinergy's products or services being offered for sale should be clear and concise.

Policy Interpretation

If you have any questions about how this policy affects your specific circumstances, contact the Vice President, Reengineering and Shared Services or talk with your manager or a corporate or business unit officer. The Company's intention is to avoid situations that could reflect unfavorably on our employees or our integrity and reputation in the business community. Failure of Cinergy employees to comply with these standards of business conduct could result in disciplinary action up to and including dismissal. If you observe or are aware of an ethics violation you should report it to your supervisor or responsible Cinergy/Business Unit management. The Company also has a toll free number (800-354-2714) where you can report violations anonymously.

2. *GUIDELINES FOR PURCHASING MATERIALS AND SERVICES*

Purchasing is the official department for acquiring Cinergy's equipment, materials, supplies and services, including contract construction for regulatory and non-regulatory activities. Insofar as practical, purchases are made at the lowest evaluated cost based on the total cost of ownership on the basis of competitive bids from selected, qualified vendors.

2.0 Qualification of Suppliers and Contractors

Normally, all suppliers and contractors permitted to bid on Cinergy procurements must qualify prior to bidding.

Exceptions to supplier qualification: When suppliers or contractors are expected to furnish products or services on a one-time basis, they need not be qualified by the Purchasing Representative and the client as appropriate. The requirement may also be waived by the Purchasing Representative in special circumstances when the qualifying process is not practicable in advance of bidding or when cost limits and risks are reasonable.

Selection of Bidders

Request for Quotation Purchasing has the responsibility to request and receive all bids from our vendors and contractors. When appropriate, Purchasing will have input in determining potential bidders.

Developing sources

PURCHASING works with its Clients continually to develop alternative sources to purchase our products and services and thus promote a competitive environment through evaluated cost analysis based on a total cost of ownership. It is important to plan ahead so as not to exclude potential sources because of unnecessary constraints, specifications or delivery date requirements.

Competitive Bidding

We request bids only from potential suppliers and contractors that the client or Purchasing Representative determines can, on an evaluated total cost of ownership basis, furnish the required product or service. We won't ask suppliers and contractors to submit bids if we have no intention of accepting their proposals. Try to allow 30 to 60 days in your schedule, depending on the complexity of the project, to obtain competitive bids, evaluate bids, negotiate and prepare the necessary contract documents.

Cinergy awards all purchase orders and contracts in accordance with competitive bid practices whenever practical. In keeping with this, we'll solicit bids from all qualified vendors deemed appropriate.

Cinergy does not publicize its intention to request bids, and it does not hold public bid openings. Vendors should submit bids only to authorized Purchasing employees. When bids are expected to exceed $100,000, we request they be submitted in a properly identified, sealed envelope, which we provide.

Bid Prices and technical information are considered confidential. They shouldn't be disclosed outside the company, unless as required by law or regulatory agencies or to a consultant or engineer/constructor under contract to perform bid analysis or related

work. Sharing bids or copies of bids other than with authorized individuals in the evaluation and award decision is not permitted.

Confirming Orders

A confirming order is not good business practice as it awards work without written documentation and often competitive bids are not obtained in accordance with Cinergy's policies. Confirming orders are to be avoided unless circumstances dictate they are necessary.

If, because of extenuating circumstances, a confirming order is necessary, ask the appropriate Purchasing Representative to place the confirming order. The Purchasing Representative will then place the order in accordance with legal and purchasing guidelines which, while not giving Cinergy the protection offered by a purchase order or contract, can be of some help if a problem occurs.

Confirming orders are not to be placed by employees other than Purchasing Representatives unless there are mitigating circumstances involved and your management has approved it. If you find yourself in such a situation, notify the appropriate Purchasing Representative when practical. A purchase requisition must be prepared to follow up confirming orders.

Confirming orders for all services, regardless of value, or for products valued at more than $500 may not be legally enforceable unless placed in writing. That's why it's important to follow up all confirming orders.

Noncompetitive Procurements

Single source procurements

Our basic procurement policy is for competitive bidding. The Purchasing Representative, with client's approval, may get some products or services from a single source on a noncompetitive basis when:

- It is in Cinergy's best interest
- No other qualified sources are available
- The dollar amount is so small it rules out the possibility of savings
- Enough evidence from previous bids and experiences available justify the Purchasing Representative placing an order.
- A single source procurement is authorized by the appropriate Purchasing Manager.

Substantiation for noncompetitive procurements

When competition is available, we must justify deviating from competitive bidding. The appropriate Purchasing Representative is responsible to make sure deviations from these guidelines are adequately substantiated and documented.

Bid Evaluation

Responsibility

The Purchasing Representative is responsible for coordinating the evaluation of all bids. Clients are responsible for evaluating technical or other factors as needed for a complete and well-substantiated recommendation.

Factors

In evaluating bids, Cinergy considers:

- Quality of product or service
- Compliance with contractual terms and conditions
- Delivery or schedule
- Price and commercial terms
- Agreement with specifications
- Vendor's management and financial integrity
- Unit prices and potential impact
- Utilization of Minority or Woman owned businesses (1st or 2nd tier)
- Other factors that may result in lowest overall cost

We do not allow a vendor or contractor to revise the base price of a bid unless there is a change in the scope and all bidders have an equal opportunity to revise their price, or unless the bidder has made an obvious error. A chance to meet a competitor's lower price with a supplementary bid undermines the integrity of our system and is strictly forbidden.

Late bids

We generally do not receive late bids. That's discriminatory because it favors the late bidder with more time to prepare an offer. If a bid arrives late, but bears a postmark prior to the due date from the U.S. mail or other recognized delivery service, the Purchasing Representative, with client's approval, when appropriate, decides whether to accept the bid. If a time extension is granted for the bid due date, the Purchasing Representative should notify all bidders and offer them the option to resubmit their bids on the revised date. Late bids should be sent back to bidders unopened.

Mistakes

Errors or omissions in proposals open up questions of fairness to all vendors bidding the project. Purchasing Representatives can request vendors to recalculate or submit additional supporting information when there are obvious errors in calculations or if items on the bid data sheets that don't affect total price are not completed. However, when a vendor draws attention to a mistake that materially alters either total price or technical merits, the Purchasing Representative should consult with his/her Manager and the client when appropriate. Changes will be decided on a case-by-case basis.

Alternate Proposals

At times a bid may offer an alternative or substitute product or service for the same use as the product or service specified. Purchasing Representatives recognize their responsibility to other vendors who bid conscientiously on exact specifications. Generally, we'll place the order with the vendor who has offered a preferred product -- whether it's to Cinergy's specification or to an alternative proposal. But to be fair, when we are preparing a request for quotation where it's likely alternative proposals would be acceptable, we will include a statement to that effect on the quotation form. Unsolicited proposals are usually not acceptable and will not be evaluated unless authorization is given by an appropriate Purchasing Manager, in consultation with the client if needed.

Supplier Diversity

We actively seek competitive bids for materials, supplies, equipment and services from minority and women owned vendors as defined by the Federal Acquisition Regulations. We evaluate bids and make awards on a nondiscriminatory

basis with no payment of premiums and no restriction of competition to minority and women owned vendors.

While we cannot promise procurements to minority and women owned businesses, we can make some assurances. As an equal opportunity buyer, we will provide qualified and certified minority and women owned vendors the opportunity to compete for our business. We will evaluate each proposal regarding proven qualifications, demonstrated performance and merit of specific offerings.

Cinergy remains an active supporter of the National Minority Supplier Development Council, the Indiana Regional Minority Supplier Development Council, The National Association of Woman Business Owners and the Cincinnati Minority Supplier Development Council. Cinergy actively participates in trade shows and other functions with the intention toward identifying and developing contacts and increasing business opportunities with minority and women owned vendors.

Contract Compliance Program

In compliance with the U.S. Department of Labor, Office of Federal Contract Compliance Programs conciliation agreement, Cinergy has committed to incorporate the equal opportunity clause in all purchase orders as well as leases and contracts having an annual value of $2,500 or more, as required by Executive Order 11246, as amended, and its implementing regulations. To comply with this conciliation agreement requires a purchase order or contract that contains the equal opportunity clause be sent to our suppliers and contractors with whom we anticipate placing more than $2,500 in yearly business.

Service Territory Buying Preference

Vendors or contractors residing in or furnishing products or services produced within Cinergy's service area receive buying preference when pricing and technical considerations are equal.

Negotiations

Purchasing Representatives are primarily responsible for preparing, formatting and conducting the commercial portion of procurement negotiations. The preparation, format and conduct of all procurement negotiations must strictly comply with procedures described here and those for administering contracts (see Page 3-10).

Cinergy generally does not negotiate a vendor or contractor base price in a competitive bid situation. However, Purchasing Representatives with appropriate client assistance may negotiate terms and conditions involving the procurement of equipment, materials, supplies and contracted services for commercial terms other than price -- for example, escalation, warranties, termination provisions, payment and shipping terms, technical considerations, etc. However, under at least one of the following conditions and with prior approval of the Purchasing Representative's Manager and/or the Vice President, Reengineering and Shared Services, a Purchasing Representative with appropriate client assistance may negotiate the base price if:

- It is determined that the cost of preparing specifications for formal quotations is unreasonable or is unwarranted because of prevailing circumstances.
- It's desirable to divide an award among several suppliers to maintain alternative sources of supply or otherwise benefit Cinergy.
- Complex procurements or alliance initiatives requiring consideration of alternative or cost-benefit pricing or total cost trade offs.

- Purchasing receives a bid from a single source, or a change is initiated against an original purchase order.
- The applicable Manager, Purchasing with consultation with the client when appropriate, determines it's in Cinergy's best interest to negotiate.

Purchase Order Awards

Authority and approvals

Under direction of the Vice President, Reengineering and Shared Services, applicable Purchasing Representatives are responsible for the award of all purchase orders, contracts and associated change notices and amendments based on authorized requests. Designated Purchasing Representatives possess specific dollar level approval authorization, according to their level of job responsibility as confirmed by the Authorized Approvals Manual.

Basis

If the basis of an award isn't evident, the Purchasing Representative will point it out and, if necessary, justify it on the bid tabulation sheet or another document placed in the file.

For example, if we award a purchase order on a noncompetitive basis, or if a vendor other than the low-dollar bidder is selected, the Purchasing Representative or the client justifies the award basis, as appropriate, and the Purchasing Representative ensures it is placed in the purchase order file where it is maintained at least until applicable legal statute of limitations expire.

Supplier

As appropriate, the Purchasing Representative lets bidders know if they were successful. Generally, we only tell bidders the name of the successful supplier or contractor. The Purchasing Representative may authorize you to tell unsuccessful bidders technical reasons that kept them from receiving an award. However, we never disclose the following information:

- Prices
- Proprietary data of successful or competing bids
- Standing of unsuccessful bidder among all bidders
- Percentage range of difference from award price
- Identity of other bidders

Purchase order and contract administration

In most cases, the client managing the work is responsible for administering the order or contract and making sure the supplier or contractor fulfills all contract requirements. The Purchasing Representative shall discuss with the client who is responsible for administering the work by name and make that known to all affected Parties. A copy of documentation the client sends or receives concerning commercial or important technical items should be sent to Purchasing to ensure the purchase order or contract file is complete. After award of a purchase order or contract, Purchasing remains responsible for issuing all change notices or contract amendments. Purchasing will continue to provide support and assistance in administering commercial aspects of the order or contract. Purchasing is responsible for submitting signed original copies of formal agreements to Corporate Records and copies to Legal Department, client, and Purchasing for file.

Contacts

Suppliers The appropriate Purchasing Representative is the primary Cinergy contact for all commercial relations with suppliers and contractors furnishing products or services, especially during bid evaluations.

Technical Sometimes contacts between suppliers or contractors and clients are necessary and desirable. You should coordinate such contacts through Purchasing by letting the appropriate Purchasing Representative know about all contacts that may concern current or future procurements as appropriate. Technical contacts between client departments and suppliers or contractors should not include discussions concerning price, commercial terms or contractual provisions while under bid evaluation.

Legal You should coordinate requests for legal review of terms and conditions, proposals or contracts through Purchasing. In most instances, we can resolve conflicting terms and conditions or other matters without Legal Department assistance.

Conforming to Legal Requirements

In all procurement activities, Cinergy complies with all applicable legal requirements. We require all suppliers and contractors we do business with to do the same.

Exceptions

We realize that sometimes extraordinary conditions arise, requiring responsible individuals to make immediate decisions that result in deviations from these guidelines.

If this happens to you, try to obtain prior approval from the authorized level of management and document your resulting procurement actions.

This action, however, should only* occur *in exceptional circumstances.

3. *GUIDELINES FOR REQUESTING QUOTATIONS*

The Company authorizes Purchasing Representatives to obtain competitive bids, whenever possible, in accordance with Company policy.

Less than $25,000

When a Purchasing Representative can acquire products and services for less than $25,000, the Purchasing Representative may order from any reliable source. We allow single-source procurements but require price checks with several vendors, documented in the Purchase Order file, when buying unfamiliar products or services.

As long as a bid is for standard and/or non-complex products and services greater than $25,000 but less than $50,000, the Purchasing Representative may accept verbal quotations consistent with Cinergy's policy on competitive bidding to maintain a competitive-bidding environment (see Page 2-2). However, we require written quotations for products and services costing more than $25,000 but less than $50,000 in the following circumstances:

- For all capital equipment
- From vendors whose quotations are likely to conflict with Cinergy's standard terms and conditions
- When permanent documentation is essential

To get a written quotation, a Purchasing Representative uses the department's "Request for Quotation" format. The RFQ should include, but not be limited to: quantity, description, delivery requirements, special conditions, drawings, specifications and applicable dates. If replies should follow a certain format, the Purchasing

Representative states that in the RFQ. The Purchasing Representative should be thorough, attempting to limit all known variables.

The Purchasing Representative should get quotations from at least two sources, if available. A single-source procurement can be made, but the Purchasing Representative, with input from the client, when appropriate, must justify that decision in writing. The justification must be included in that transactions file.

$50,000 or More

Products and services with estimated prices of $50,000 or more require written proposals. Just as in situations involving purchases of less than $50,000, the Purchasing Representative should be thorough and attempt to limit all known variables. The RFQ should state in writing the same kinds of information -- quantity, description, delivery requirements, special conditions, drawings, specifications, applicable dates and the format replies should follow.

When bids are expected to exceed $100,000 Purchasing Representatives must obtain sealed, competitive bids from at least three qualified and available sources. Each vendor or contractor is asked to return at least two copies of its proposal in a sealed bid envelope to an authorized representative of Purchasing . Purchasing Representatives will record all quotations on a bid tabulation sheet and attach it to the original requisition to serve as a backup document once the order is placed. All bids received and any applicable documentation, including the bid evaluation and recommendation, is placed in that transactions file.

Sealed Bids

Purchasing Representatives can request sealed bids when they think it's in Cinergy's interest to do so or when procurement value is expected to exceed $100,000.

Vendors or contractors must place at least the commercial portion of their proposal in a sealed bid envelope. The Purchasing Representative will provide the envelope when they send out the RFQ.

When received, sealed bids remain unopened until all bids are received or until the designated due date and time has passed.

4. GUIDELINES FOR ADMINISTERING CONTRACTS

The Purchasing Department coordinates the contracting process. Purchasing Representatives in Purchasing generally are responsible for the procurement of products and services in accordance with established procedures and within standard commercial terms and conditions. But when they administer contracts, they're primarily concerned with procurements requiring negotiated terms and conditions that may deviate significantly from our standards. In addition to this guideline, see the Corporate Policy on contractors, contract employees and consultants issued January 30, 1998.

General Contract Definitions

For our purposes, a formal contract is a procurement document agreed to and signed by two or more parties. It sets forth promises between the parties and can be enforced by law. It also provides a basis for evaluating and resolving all claims and disputes that arise between the parties.

As used within Purchasing, a contract for the procurement of products and services may take the form of:

Purchase order Includes any attached general specifications, terms and conditions, technical specifications, drawings, etc. Electronic versions may be utilized (i.e., Passport) when authorized by the applicable Purchasing Manager(see Pages 2-7 through 2-8)

Lease agreement Generally involves a third-party financing agreement

Uniquely drafted formal contract — A unique, negotiated agreement, a formal contract is specifically designed to address a particular procurement transaction. This type of contract is used because either the transaction isn't adaptable to Cinergy's standard commercial terms and conditions, or it is not normally intended for the other types of contracts described above.

In Practice

All procurement transactions for services and all product purchases for more than $500 in value must be finalized as written documents. That is, they require contracts as defined above, which must be executed as required in the Authorized Approvals Manual. No work is to be performed until a contract or purchase order has been approved.

Client senior management or the applicable Manager, Purchasing may, with knowledge of the risks that may be incurred, have the authority to cause work to begin prior to approval of any form of contract.

Form — The Purchasing Representative will coordinate with the client and Legal Department, as necessary, to determine what type of contract we will use to consummate a procurement transaction for the required products and services.

Participation Before beginning any negotiations with a vendor, the client needs to consult with his/her appropriate representative in Purchasing, to determine to what degree and in what manner Purchasing will participate in the negotiations. The Purchasing Representative may act as exclusive negotiator, a member of an interdepartmental team, or in an advisory capacity.

Exception Clients are encouraged to talk with vendors to determine the technical capability of their product or services. However, no commitment to any terms and conditions shall be made without approval of the appropriate Purchasing Representative.

Review Purchasing ensures contracts that vary significantly from our standard terms and conditions will be reviewed by Legal Department and other affected Cinergy departments prior to execution by the appropriate business unit.

Disputes The client should inform his/her Purchasing Representative whenever a dispute arises between the client and a contractor involving a claimed breach of contract or an interpretation of a contract that could alter its original intent.

Responsibility

Purchasing Representatives, with client involvement when appropriate, perform the contract administration function by:

- Representing the Vice President, Reengineering and Shared Services, as necessary in negotiating contract disputes.

- Renewing existing or formulating new contracts involving transactions not readily adaptable to standard terms and conditions or normally intended for contracts previously defined.
- Developing, reviewing and monitoring compliance with policies and procedures for administering contracts.
- Developing, updating, publishing, monitoring and interpreting standard terms and conditions for various kinds of procurements.

Client The business unit requisitioning the product or service is responsible for daily administration of the contract, at the working level, after it's executed and in place.

Procedures

Bidding procedures and procedures for processing contracts that take the form of purchase orders, change notices and lease agreements are explained in other parts of this manual. The procedures outlined below describe steps necessary to process unique contracts that require Purchasing's assistance in contract administration.

Preliminary Planning Discussion

When you decide to procure equipment, materials, supplies or services that require a uniquely tailored formal contract, set up a preliminary discussion with your appropriate representative within Purchasing. Procurements that require uniquely tailored contract involve:

- General commercial terms and conditions significantly different from our standard.
- A contract life of more than one year
- A dollar commitment of $1 million or more.

- Significant risk to Cinergy, regardless of contract amount or time duration.
- Innovative or unique provisions, rights, or obligations.

The preliminary discussion should cover matters including:

- The nature of the transaction and any special terms and conditions required.
- Target dates for preparation, bids, negotiation, evaluation, award, etc.
- The contract's general format. For example, will it be a purchase order with referenced documentation, a vendor contract as amended by Cinergy or Cinergy's contract as amended by the vendor?
- The extent of Purchasing's participation.

NOTE: Sometimes we receive a purchase order requisition that we feel should be processed as a unique contract. If this happens, we will contact you to arrange a preliminary meeting.

Contract Formulation

The client and Purchasing will:

- Prepare appropriate language to address the procurement's unique nature. Purchasing is generally responsible for commercial terms and conditions, and the client is responsible for technical terms and conditions.
- Evaluate, investigate and prepare a list of bidders for approval, if the contract will be bid.
- Review the proposed contract with Legal Department and with other appropriate management for proposed language, parameters for negotiating an agreement, and if needed, the evaluation criteria and the list of bidders.

Negotiation

Negotiation of a contract with an appropriately selected vendor is conducted by designated Purchasing Representatives and client departments as agreed upon in the preliminary planning meeting.

Agreements reached during negotiations must be within parameters approved during the formulation process. An impasse reached during negotiations, which the Purchasing Representative can resolve only by exceeding established guidelines, must be reviewed and approved by the authority that approved the initial guidelines. Any deviation from specifications will be approved by the client.

We conclude negotiated agreements with the understanding that before execution the agreement may be subject to additional review and approval by our Legal Department. Legal is responsible to review and approve the contract as to its acceptability as a valid contract and returns it to Purchasing. Purchasing may then forward it to other appropriate departments or business unit management for review, as necessary.

Contract Execution

Allow for up to 20 days in your planning process for contract execution as Purchasing must make sure appropriate departments review the contract before it's executed. Then, after a final agreement is negotiated, Purchasing prepares the contract document in sufficient copies and sends all copies to the vendor for approval. The vendor returns all copies of the contract to Purchasing. When we receive the vendor-executed contracts, we prepare a purchase order or contract that serves as an approval document authorizing the dollar expenditure with appropriate account distribution. When an appropriate Cinergy or business unit officer signs the contract,

we send one original to the vendor with a copy of the purchase order. We distribute Cinergy's original to Corporate Records and other copies to the client department, Legal Department, and any other affected departments, and to individuals with direct responsibility for day-to-day contract administration.

Day-to-Day Administration

The client must ensure the day-to-day administration of the contract with respect to such matters as:

- Monitoring and enforcing contractor performance of contract terms.
- Reviewing and approving invoices.
- Inspecting and accepting the contractor's product or service to ensure contract compliance.
- Resolving disputes that may arise (to the extent that the resolution does not alter terms and conditions of the contract).

Disputes

If you cannot resolve disputes within the intent of agreed-to terms and conditions, and a uniquely tailored contract is involved, contact your Purchasing Representative. If we issued the contract under a purchase order, you should refer the problem to the Purchasing Representative issuing the purchase order or the Purchasing Representative responsible for that commodity.The client, acting jointly with the Purchasing Representative, and with other departments that have input, will negotiate the dispute with the contractor in a manner similar to that used to negotiate the original contract. If a settlement is not attainable to the dispute, coordination with the Legal Department may be necessary.

Amendments

We must process a purchase order change notice or a contract amendment if a client wants to alter, add or delete any contract provision. Purchasing will prepare, exchange and assist the client in negotiation of any amendment language with a contractor.

5. *GUIDELINES FOR MAKING FOREIGN PURCHASES*

Because of special market conditions, it may be in Cinergy's interest to consider foreign vendors. A foreign vendor could be a private, semi-private or government entity. It is considered "foreign" if our payment for products and/or services results in a contribution to the gross national product of another country.

Justifying Foreign Vendors

Generally, we will solicit bids from qualified foreign vendors when:

- A single source or an insufficient number of domestic vendors is not available to allow a competitive bid situation for the product or service.
- Total evaluated value to be achieved by awarding a product or service to a foreign vendor is significant to Cinergy.
- Procurement information shows domestic vendors are unlikely to meet critical delivery or technical requirements.
- Procurement information shows the contractual terms and conditions demanded by domestic vendors would be unacceptable to Cinergy.
- Material or equipment available from a foreign vendor is better quality.
- No domestic vendor is available for the product or service you need.
- The Vice President, Reengineering and Shared Services or the Client determines that it is in the best interest of Cinergy to purchase from a foreign vendor.

Evaluating Questionable Circumstances

Sometimes a competitive bid situation will exist between a domestic vendor and its foreign competition. Then we may determine an evaluation factor that's attributable to foreign content and add that to the base proposal.

Evaluating Bids

We take a number of factors into account when evaluating bids from foreign sources. Among those factors are qualifications, inspection, communication and coordination complexities.

We also consider additional expenses naturally associated with doing business abroad. Those expenses may include:

- Shipping and transportation costs and time.
- U.S. Customs duty costs and other expenses of importing, such as customs broker fees.
- Added insurance protection.
- Monitoring and expediting expenses at the manufacturing location.
- Currency fluctuations and exchange rate.

And, since we must maintain what we purchase, we look at additional spare parts support, the spare part inventory held in the U.S., the potential cost of repairs and the availability of service or maintenance personnel.

Awarding Bids

We may place orders directly with the foreign vendor or a U.S.-based subsidiary or agent. We prefer delivery designated as FOB destination with the shipper acting as importer of record, responsible for paying customs duty and brokerage charges. However, if required, Cinergy can do this.

PRINCIPALS AND STANDARDS
OF PURCHASING PRACTICE

Advocated by NATIONAL ASSOCIATION OF PURCHASING MANAGEMENT. Loyalty to the Company, Justice To Those With Whom We Deal, Faith in Our Profession. From these principles are derived the N.A.P.M. standards of purchasing practice.

1. To consider, first, the interests of the Company in all transactions and to carry out and believe in its established policies.
2. To be receptive to competent counsel from our colleagues and to be guided by such counsel without impairing the dignity and responsibility of our office.
3. To buy without prejudice, seeking to obtain the maximum ultimate value for each dollar of expenditure.
4. To strive consistently for knowledge of the materials and processes of manufacture, and to establish practical methods for the conduct of our office.
5. To subscribe to and work for honesty and truth in buying and selling, and to denounce all forms and manifestations of commercial bribery.
6. To accord a prompt and courteous reception, so far as conditions will permit, to all who call on a legitimate business mission.
7. To respect our obligations and to require that obligations to us and to the Company be respected, consistent with good business practice.
8. To avoid sharp practice (auction bidding).
9. To counsel and assist fellow purchasing agents in the performance of their duties, whenever occasion permits.
10. To cooperate with all organizations and individuals engaged in activities designed to enhance the development and standing of purchasing.

Duke Energy Ohio
Cause No. 08-709-EL-AIR

Management Policies, Practices & Organization of Duke Energy Corporation

Schedule S-4.2

Volume 3 of 3

VOLUME 1 of 3

	Page Nos.
FINANCE	
Corporate Controller	
Accounting	5
Corporate Financial Controls	332
Commercial Business Financial Operations	338
Corporate Treasurer	
Treasury	345
Insurance & Claims	399
Risk Management	403
Financial Re-engineering	408
Tax	412
Investor Relations	419
Financial Planning & Analysis	424
O&M and Capital Budgeting and Regulated Business Support	428
Rates	433

VOLUME 2 of 3

	Page Nos.
STRATEGY, POLICY & REGULATORY ACTIVITIES	444
Technology	448
Environmental, Health & Safety	452
Energy Efficiency	457
Strategy & Planning	460
Business Relations	464
Economic Development	468
Government & Regulatory Affairs	473
Federal Government Affairs	478
Federal Regulatory Policy	483
Corporate Communication	487
SUSTAINABILITY & COMMUNITY AFFAIRS	
Sustainability & Community Affairs	491
Foundation	496
LEGAL	
Legal Department	502
Audit Services	515
Corporate Secretary and Ethics & Compliance	523
Securities and Financial Reporting	529
Human Resources	534
CORPORATE ADMINISTRATION	
Information Technology	546
Enterprise Operations Services	687
Enterprise Field Services	705
Supply Chain	713

VOLUME 3 of 3

	Page Nos.
U.S. FRANCHISED ELECTRIC & GAS BUSINESSES UNIT (FE&G)	
Customer Service	761
Gas Operations	
Gas Engineering	815
Commercial Operations	856
Construction & Maintenance	867
Gas Performance Support	874
Power Delivery	
Electric Systems Operations	884
Midwest Field Operations	898
Performance Support	923
Central Operations	934
Asset Management	944
Engineering & Technical Services	952
Enterprise Asset Management	981
COMMERCIAL BUSINESS UNIT (CBU)	
Corporate Development and Mergers & Acquisitions	986
Midwest Generation Operations	992
Coal Group	1010
Commercial Asset Management	
Commodity Logistics	1015
Generation Dispatch & Real Time Operation	1020
Portfolio Risk Management	1026
Commercial Analytics	1032
Regional Transmission Organization & Market Services	1039

MANAGEMENT POLICIES, PRACTICES & ORGANIZATION

OF

DUKE ENERGY CORPORATION

DUKE ENERGY OHIO

SCHEDULES S-4.2

U.S. FRANCHISED ELECTRIC & GAS BUSINESS UNIT

YEAR 2007

Schedule S-4.2

DUKE ENERGY
DUKE ENERGY OHIO
SUMMARY OF MANAGEMENT POLICIES, PRACTICES AND ORGANIZATION
CUSTOMER SERVICE
SFR Reference: Chapter II (B)(9)(d)(i,ii,iv,v)

I. Policy and Goal Setting

Customer Service supports the corporate policies and objectives as described in the Working Environment Policy Manual through the Department directives, procedures and practices. In addition, policies defined by the Federal Energy Regulatory Commission (FERC) and the Code of Business Ethics (COBE), are supported and followed within the Customer Service organization.

Policy making also occurs at the department level primarily through the Business Standards and Integration (BS&I) group. This group was formed in April, 2006 after the Duke Energy – Cinergy merger, to simplify existing processes and to maximize the effectiveness of Customer Service's systems and resources.

The BS&I team gathers input from all areas of Customer Service and also works with key stakeholders outside of Customer Service such as Gas Operations, Meter Operations, Meter Reading, Service Delivery, Customer Strategy and Electric Operations. The BS&I team works cohesively to establish policies and procedures that make the Customer Service business more efficient and cost effective.

Departmental policies are communicated to the management team at department staff meetings. The Management team then communicates these policies to their staff that in turn communicate the policies, where appropriate, to individual staff members. Department policies are often reviewed by supervisors and the work force in small group meetings. The purpose of the meetings is to ensure there is an understanding of the policies and their importance in relation to serving the customer.

Goal Setting

Annual and long-range goals and objectives are established by executive management and are embodied in the US Franchised Electric & Gas business plan. The senior vice president of Customer Service meets with the Customer Service management team to establish a business plan that supports the goals of the US Franchised Electric & Gas. Attached as Exhibit CUC-2, is an excerpt from the 2007 Customer Service Business Plan. The Customer Service management team is responsible to then develop business plans for their specific department, which supports the overall Customer Service plan. Non-union

employees are compensated according to the results of these goals combined with the results of Customer Satisfaction surveys, how well we did on achieving our major Customer Service initiatives, and overall performance of the Company as determined by earnings per share.

The Customer Service management team reviews the progress of the business plan and objectives monthly. The senior vice president of Customer Service also reviews progress against these goals with senior management on an as-needed basis relative to the importance of the goals/objectives in supporting the Company's objectives.

Some of the criteria used in the Customer Service Department's goal/objective setting process are:

- The goals must support and foster the corporate charter to create superior and sustainable value for our customers, employees, communities and investors through the production, delivery and sale of energy and energy services;
- While working to achieve our goals and objectives, we remain focused on our values of stewardship, integrity, safety, respect for the individual, high performance, and win-win-relationships;
- Appropriate targets and measurements must be developed;
- Goals/objectives must relate to company initiatives and be cost-effective; and
- Goals/objectives must effectively serve both external and internal customers.

Within our Call Center, our representatives are eligible for an incentive payment on a quarterly basis, based on individual performance. Individuals are measured on components such as call quality, adherence to schedule and availability. In addition, management incentive plans also include customer satisfaction goals and objectives.

II. Strategic Planning

To determine short and long-term strategy, the Customer Service leadership team reviews corporate objectives, customer feedback and employee feedback. The business plan includes initiatives that are to be accomplished over an 18 to 24 month time period. The business plan includes action steps to achieve the initiatives as well as milestones and timelines.

An example of Strategic Planning is our current technology plan, which details various technology enhancements that will take place in 2007 and 2008. These enhancements are designed to serve our customers more efficiently and cost effectively while providing our customers with added convenience. This list of enhancements includes the implementation of an Energy Data Management System, which will provide a single repository for all of our meter data and

supports the building of an advanced metering infrastructure. This system will enable us to transform our business processes related to meter data, and it will facilitate future merger transitions.

Within our call center, we have continued to make a number of technological improvements within the past couple of years. Our Automated Phone System enables customers to perform a number of self-service options such as, report an outage, Budget Billing setup and remove, BillPayer 2000 setup and remove, check the amount due and due date, verify amount and date of last payment, pay by phone, confirm amount and due date to prevent disconnection for non-payment, Fixed Bill enrollment, EZRead enrollment, enter gas and/or electric meter readings, update phone number in the billing system and make payment arrangements. Screen Pop is another feature that enables the customer service representatives to assist the customer more efficiently by automatically accessing the customer's account whenever the telephone number that the customer is calling from, matches the telephone number we have in our billing system. To help ensure accessibility during storms, we have contracted with Twenty-First Century Communications to augment our self-serve options of reporting outages. These features also provide information to the customer as it pertains to their outage such as, estimated restoration time/date, first outage call received time/date and the cause of the outage.

We have also introduced a number of self-service applications via our website at www.duke-energy.com. Customers can register for our Online Services and perform transactions, such as report an outage, view and pay bill online, check the amount and due date of current bill, access billing, payment and usage history, enroll in our Budget Billing Program, request service to be turned on or off, report electric trouble, utilize the Home Energy Calculator, submit meter reads and view meter reading schedules. Customers can also read important messages posted online about events as they are happening through our status messaging tool.

Other strategic planning is guided by the results of our customer satisfaction surveys. As customer data is analyzed, the results are forwarded to appropriate departments and management. Based on the results, recommendations and decisions are made and factored into our strategic planning.

III. Organizational Structure

Customer Service is headed by a senior vice president who reports to the Group Executive, President and Chief Operating Officer, US Franchised Electric & Gas. The department is divided into six areas: Call Center Operations, Customer Service Platforms, Revenue Services, Energy Data Management, Business Standards & Integration, and Customer Service Support. All six areas are headed by a vice president/general manager/director who reports directly to the senior vice president. Organizational charts are attached below as Exhibit CUC-1.

IV. Responsibilities

The major responsibilities of Customer Service include the following:

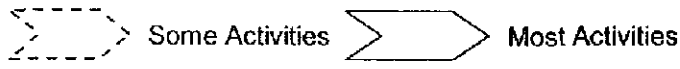
Customer Contacts

Customer Service has general responsibility for handling customer contacts by telephone and e-mail for residential and small business customers related to a wide variety of billing and service matters, complaints, adjustments, and gas and electric trouble calls. Also, telephone calls from builders and contractors regarding preliminary gas and/or electric service matters such as inspections, new meter installations, etc., are handled by Customer Service.

Customer Service also manages our customer service offices, where customers can walk in and make a payment, make payment arrangements, or discuss any billing matter with one of our customer service representatives. We also manage Pay Agents where customers can also make payments at a local retailer that typically offers extended hours of operation. In addition we have the responsibility to maintain and update all customer related web content on the Company's website as well as functionality for Online Services.

Revenue Services

In general, the Revenue Services area performs most of the functions in the Company's retail revenue process. As depicted in the following diagram, once customer accounts are created, Revenue Services performs most of the activities related to preparing the customers' bills, processing payments, managing collections and reporting revenue.



Billing

- Render timely and accurate bills;
- Resolve usage/billing exceptions accurately and timely;
- Support other departments with billing information necessary to aid in resolving customer inquires;
- Investigate billing problems and initiate billing in cases of un-metered or miscalculated gas/electric usage;
- Provide operational support for billing; and
- Maintain proper controls to ensure all accounts are billed as scheduled.

Credit & Collections

- Establish and implement credit and collection policies, in compliance with state regulatory requirements;
- Take action on past-due accounts (primarily residential);
- Investigate, and initiate billing and collection actions, in cases of fraud and meter tampering;
- Administer Percentage of Income Payment Plan, medical certification and life support programs; and
- Initiate account adjustments, claim filings, and collection efforts, if any, for customer bankruptcy filings.

Payments

- Apply payments to customer accounts in a timely manner;
- Validate system controls are operating appropriately and effectively;
- Administer, apply, and collect agency payments (Vouchers, PIPP Intents, etc);
- Provide Operational support for Payment related questions; and
- Maintain proper account records and controls to assure the integrity of reported gas and electric usage and revenue and accounts receivable balance.

Certified Supplier Business Center

- Manage the business relationships with gas and electric suppliers participating in Duke Energy Ohio's Customer Choice programs;
- Execute Customer Choice back-office operations; and
- Create and implement Customer Choice business processes and support other departments by providing Customer Choice information.

Regulatory Reporting and Complaint Resolution

Customer Service also works with the PUCO and Ohio Consumers' Counsel (OCC) to provide required reports such as the OSCAR report (detailed 96 column report regarding PIPP accounts, number of disconnects, number of reconnects, and more) and other reports upon request. This group also handles escalated complaint calls that are referred by the call center, the PUCO and OCC for resolution.

Customer Satisfaction

Customer Service works with the Customer Strategy Department to manage customer satisfaction surveys and to mine the data and determine customer improvement initiatives. Surveys include customer contact surveys for residential customers, new service installations, e-mail requests, Online Services, and e-Bill.

Energy Data Management

Customer Service has a dedicated group responsible for establishing and implementing an Energy Data Management System (EDMS). This system will provide a single repository for all of our meter data and will support the building

of an advanced metering infrastructure. Once implemented, this system will streamline the validation, estimation and exception process as well as remove complexity of meter device issues from downstream systems. In addition, the EDMS will provide scalability by providing economical support for meter data, processing and storage for 14,000,000 customers (19,000,000 meters) with incremental additions based on future mergers. It will provide flexibility by having automated processing of standard business rules for validation, editing, and estimating and aggregation and billing determinant calculations. It will provide simplification by providing consistent normalization of data, consistent and early exception management, and isolate complexity of meter infrastructure management issues from the Customer Information System and other systems. We expect to implement the EDMS to the Business and Industrial customers by mid-2007 and to the mass market by early 2008.

Customer Service Platforms

Customer Service is also responsible for continually evaluating our systems and technologies used throughout Customer Service, to ensure that we have the right systems and tools in place to run the business efficiently and cost-effective, both now and in the future. We have a group dedicated to working with key stakeholders throughout the organization to identify "pain points" (what's not working or what's causing breakdowns in business processes, etc.), and to research and evaluate what technology is needed to improve our business processes across the organization. This group is strategic in their approach to ensure that the most cost-effective measures are taken, and that technologies are scalable for future growth.

V. Practices & Procedures

Customer Service develops its operating procedures with supporting input from the various departments with which the department has close interaction. These interacting departments include Meter Operations, Regulatory Compliance, Legal Department, Corporate Communications, Information Technology, Gas Operations, Meter Reading, Communication Strategy & Energy Efficiency, etc.

Customer Service provides staff support for department-related projects that are developed on a corporate-wide basis. The conversion of our Customer Management System (CMS) is a good example of this. We also have a cross-functional Customer Satisfaction Council, focused solely on evaluating results of customer satisfaction and determining recommendations for improvement.

Operational guidelines are provided for use by the office and field work forces. Day-to-day operational decisions are made by the respective vice presidents/general managers/directors or senior vice presidents, as these decisions affect normal division operations. Unusual problems and events are discussed with the department senior vice president and affected vice president/general managers/directors. The vice president keeps the US Franchised Electric & Gas president informed of

significant events that could affect the overall operation of the department in a material way.

V. Decision Making and Controls

At monthly staff meetings held by the senior vice president with the vice presidents/general managers/directors, recent developments internal and external to the department are discussed and reviewed. Where appropriate, decisions are made which will enhance overall department operations.

The vice presidents/general managers/directors in turn have staff meetings with their employees as needed. Any decisions that affect the work force are discussed with the employees in small group meetings, and feedback is solicited and received.

Day-to-day decisions, as they pertain to the various jobs in Customer Service, are normally made by the employees performing the jobs. Certain guidelines are in place to assist employees in decision making. These guidelines are communicated to employees through online or printed training manuals and departmental procedures. Each employee's work is monitored by supervision to make sure decisions are consistent with policies and procedures.

Major decisions, such as the need to work overtime for a large number of employees, are made by supervisors, with the approval of the department manager. Information regarding especially significant decisions is forwarded to the senior vice president and the US Franchised Electric & Gas president in weekly or bi-weekly reports.

Specifically, the need for overtime in the call center is evaluated by workforce management. The dollars needed for planned overtime are tracked on a weekly basis and compared to the budget dollars for overtime. Workforce management approves overtime up to the budget amount. If the need for overtime exceeds our budget dollars for the week, a manager must approve the overtime.

The following are examples of controls that are in place to assist the department supervisory staff in their efforts of determining that the various systems and procedures are functioning properly:

- The Call Center telephone system has the capability of generating reports that enable management to tabulate each customer representative's activities on the telephone. In addition, supervisors of the Call Center are able to measure group productivity and effectiveness with this data;
- Another example of a control is the level of authority that various employees have when making a monetary adjustment to a customer's account. An employee must have documented approval from his/her supervisor to make an adjustment that is beyond the employee's authority;

- Further internal program controls exist involving certain billing adjustments, which are processed in the Customer Management System (CMS). These controls consist of the blocking out of entries by unauthorized employees;
- Customer and meter movement orders not processed within three working days from receipt in the Work Order group are given a high priority to follow-up; and
- Service Delivery monitors response time for Gas and Electric Trouble calls to ensure that we are responding in the appropriate amount of time. In addition, they measure the number of turn-on and turn-offs taken and the number worked. If there are any discrepancies or red flags in any of these reports, the necessary action is taken to correct the situation.

In addition, the installations of various internal electronic systems have enabled the department to develop better measurement of performance of our work force, as well as to utilize the system for training purposes in a more effective manner.

As mentioned in an earlier section, when appropriate, participatory management is being used in decision making processes. Recommendations from teams generally include control provisions, which are implemented, if approved, by departmental management.

VII. Internal and External Communication

Customer Service communicates internally with employees through meetings, e-mail, the Portal, This Week @ Duke Energy Newsletter, Duke Energy Ohio & Kentucky Weekly, and written procedures. In addition, bulletin boards are strategically located throughout the department. Periodically the president and/or senior vice president and vice presidents/general managers/directors will hold employee meetings to give employees the opportunity to voice their concerns and opinions. Lines of communication exist through various project teams and the Business Standardization & Integration group, which is used to resolve problems and encourage teamwork and cooperation across departments.

External communication occurs through a variety of channels including the following:

- Letters to customers;
- Bill messages;
- Bill inserts;
- Attendance at public hearings and meetings;
- Presentations at community meetings, agencies, rotary clubs, city council;
- Volunteer work in the community;
- Membership in professional and civic organizations;
- In-person at our customer service offices;
- E-Mail;
- Web site;
- Automated Phone Service;

- Telephone contact; and
- Contact with regulators and other agencies at our Ohio Collaborative meetings.

VIII. Goal Attainment and Qualification

Customer Service uses various statistical reports as a means of measuring operational effectiveness of the department. Some of the reports serve the dual purpose of measuring goal attainment as well as being control devices. Many of our process improvement initiatives are driven by the results of our customer satisfaction surveys as we analyze what customers are telling us in our various surveys:

Residential Customer Contact Survey
Customer Satisfaction is measured on a regular basis. Surveys are sent to residential customers that had a recent service contact. The surveys are mailed weekly by an independent research firm and measure satisfaction with 5 key processes. The surveys measure overall satisfaction using the following scale: Very Satisfied, Satisfied, Neither Satisfied nor Dissatisfied, Dissatisfied, and Very Dissatisfied.

New Service Installation Survey
Satisfaction with installation of new gas and electric service is measured on a regular basis at Duke Energy. Surveys are sent to builders, developers and/or customers that request new gas and/or electric service be installed. The surveys are mailed every week by an independent research firm and measure satisfaction with this key process for all customers. The surveys measure overall satisfaction using the following scale: Very Satisfied, Satisfied, Neither Satisfied nor Dissatisfied, Dissatisfied, Very Dissatisfied.

Online Services Survey
Duke Energy measures satisfaction of those customers that choose to conduct their business through the Company's Online Services. This web-based program allows customers to view and pay their energy bill online, enroll in Budget Billing, turn on/off service, submit meter reads, obtain billing and usage history. Overall customer satisfaction is measured using the following scale: Very Satisfied, Satisfied, Neither Satisfied nor Dissatisfied, Dissatisfied, and Very Dissatisfied.

E-mail Survey
The survey measures satisfaction for those customers that choose to contact Duke Energy through e-mail. Surveys are sent to residential customers that had a recent service contact. A link to an online survey is included with the final communication from the call center representative to the customer. The survey measures overall satisfaction using the following scale: Very Satisfied, Satisfied, Neither Satisfied nor Dissatisfied, Dissatisfied, and Very Dissatisfied.

J.D. Power and Associates Studies

J.D. Power and Associates, a firm well known for assessing the state of customer opinion and customer satisfaction in many key industries, performs annual studies of electric utilities' residential and business customer satisfaction. In addition, J.D. Power performs an annual study on gas distribution residential customer satisfaction. Duke Energy Ohio participates in each of these annual studies, and the satisfaction results indicate that Duke Energy Ohio is doing a very good job of consistently providing high-quality customer service.

The J.D. Power residential electric customer study, established in 1999, calculates overall customer satisfaction based on six performance areas: (1) company image; (2) price and value; (3) power quality and reliability; (4) billing and payment; (5) customer service and added in 2006, 6) communications. For the year 2006, the J.D. Power and Associates study measured customer satisfaction for the largest 76 electric utility holding companies in the nation, that serve over 92.8 million residential customers.

For 2006, the most recent residential customer study, Duke Energy Ohio outperformed the Midwest region average for customer service.

The gas study, implemented in 2002 measures customer satisfaction based on six performance areas which are: 1) Company Image; 2) Price & Value; 3) Billing & Payment; 4) Customer Service; 5) Field Service; and added in 2006, 6) Communications . The 2006 study measured satisfaction from customers of the 56 largest local gas distribution that serve between 49 million residential customers.

In the five years that the J.D. Power residential gas study has been conducted, Duke Energy Ohio's scores in overall satisfaction have outperformed the scores of the Midwest region average on company image, price & value, billing & payment, and customer service.

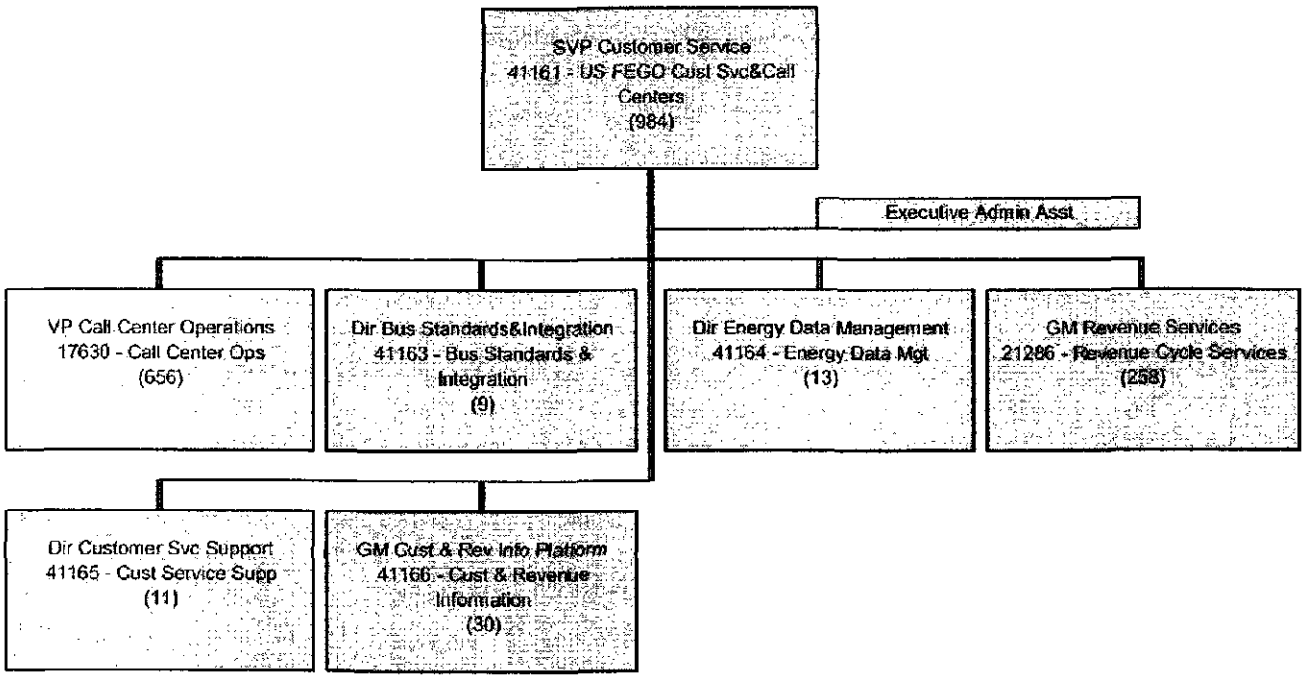
The following are some other examples of statistical reports within the department that are used to quantify the effectiveness of Customer Service activities:

- Residential Customer Contact Surveys; (attached Exhibit CUC-3)
- New Service Installation Surveys; (attached Exhibit CUC-4)
- Online Services Survey; (attached Exhibit CUC-5)
- E-Mail Survey; (attached Exhibit CUC-6)
- All Complaints & Inquiries Received by Customer Service Support 2006; (attached Exhibit CUC-7)
- Complaints Received from the PUCO 2006; (attached Exhibit CUC-8)
- Complaint Resolution Time 2006; (attached Exhibit CUC-9)
- Call Center Coaching Form; (attached Exhibit CUC-10)
- Midwest Contact Channels Report; (attached Exhibit CUC-11)
- New Service Contact Center Stats; (attached Exhibit CUC-12)
- Call Profile ½ Hour Report; (attached Exhibit CUC-13)

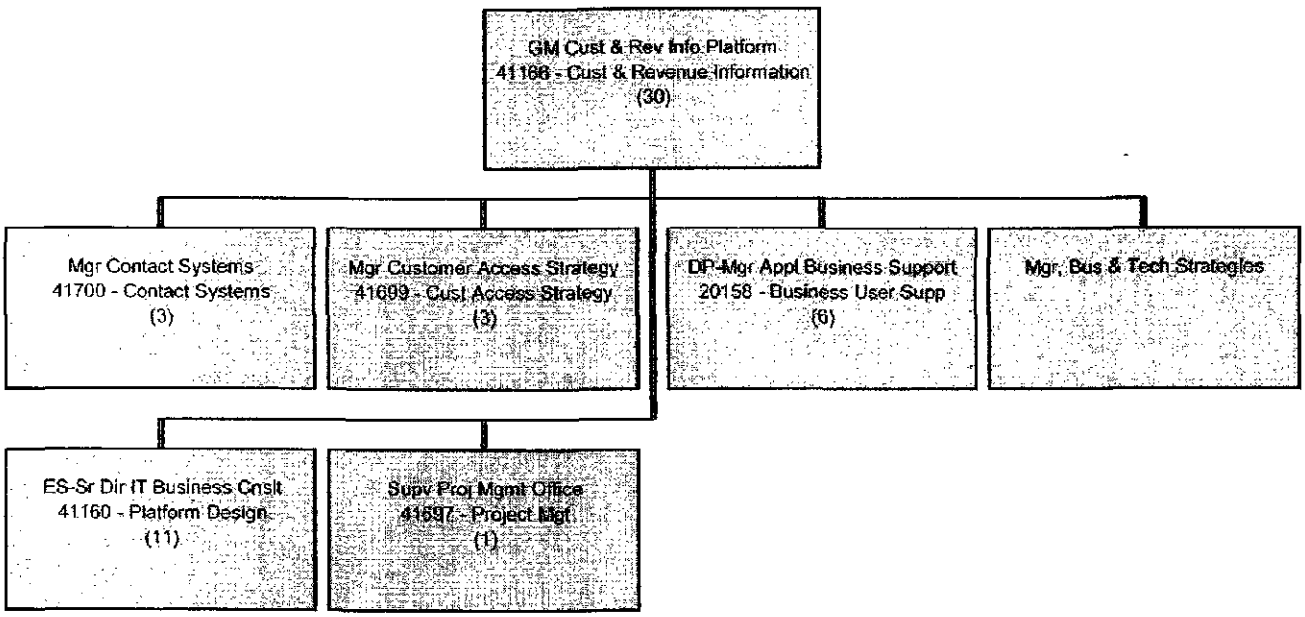
- Availability Report; (attached Exhibit CUC-14) and
- OSCAR Report (attached Exhibit CUC-15).

The vice president of Customer Service meets with the respective general managers/directors on a monthly basis for the purposes of providing information and receiving input on the current status of progress toward obtaining the goals of the department. The general managers/directors hold similar meetings with their respective supervisors.

Senior Vice President Customer Service

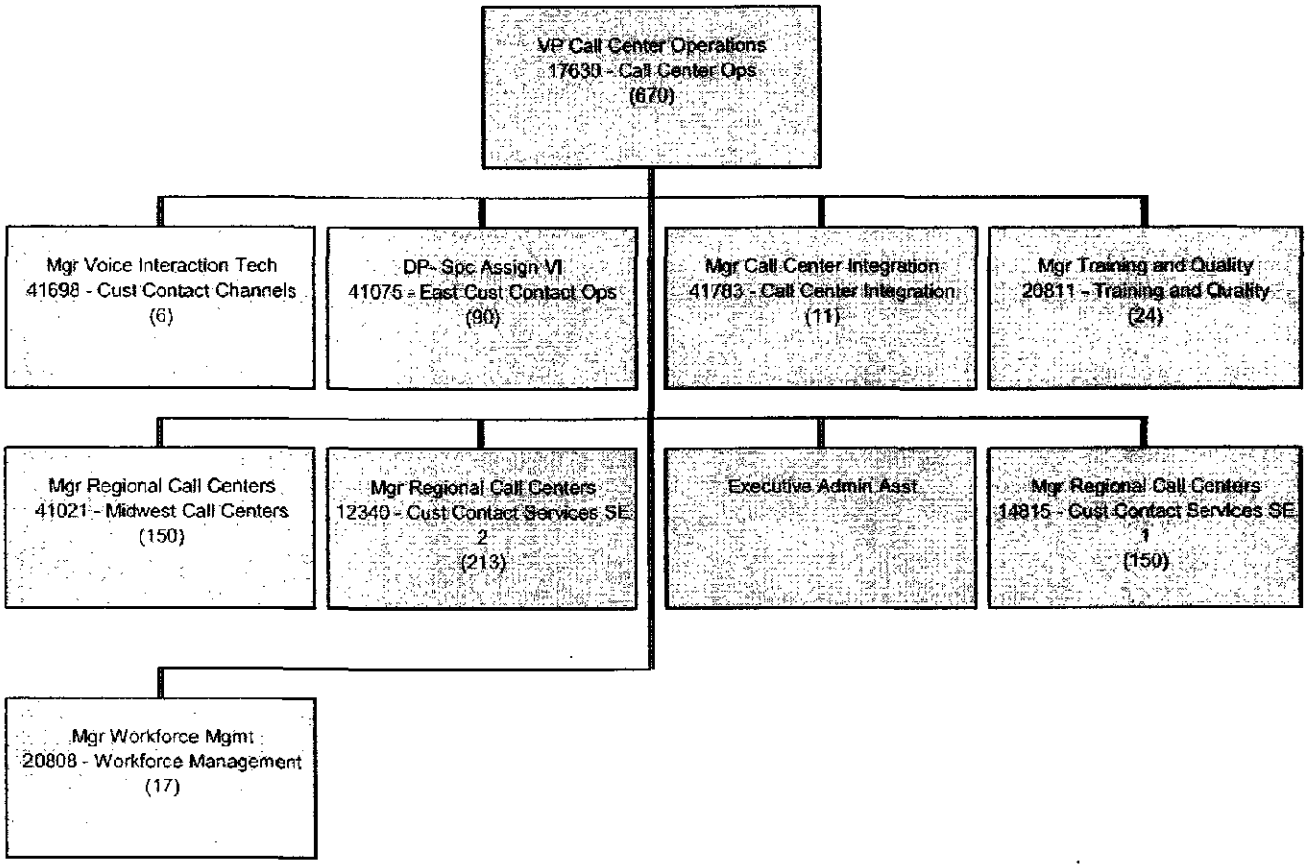


General Manager Customer & Revenue Information Platform



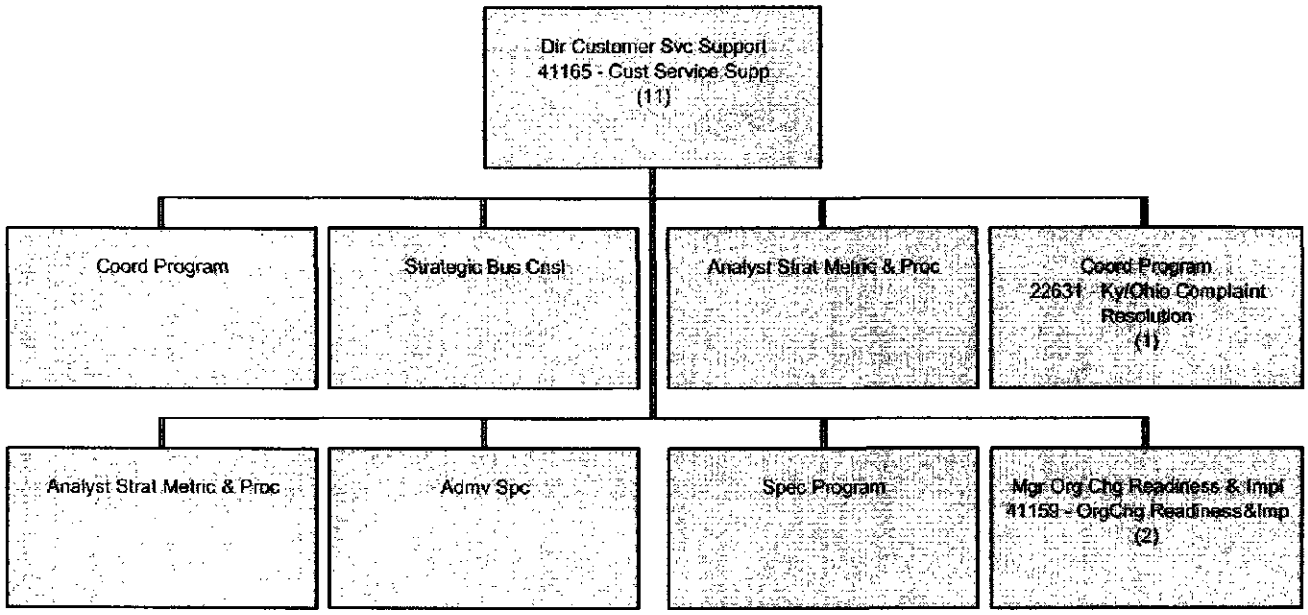
DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

Vice President Call Center Operations



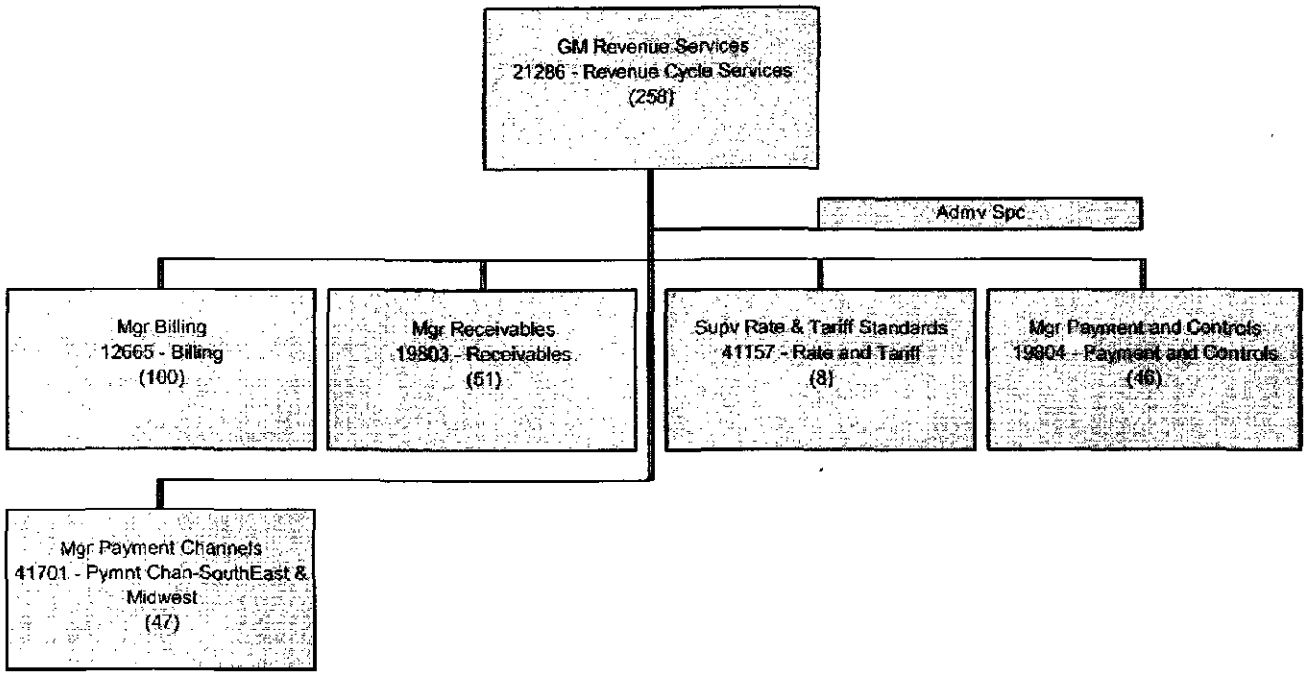
DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

Director Customer Service Support



DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

General Manager Revenue Services



Duke Energy

2007 Customer Service Business Plan

776

2007 Customer Service Strategies and Metrics

Duke Energy

Operational Objectives	Maintain Customer Satisfaction	Achieve Merger Savings Objectives	Prepare for the Future
Strategies	▸ Focus on safety for employees, contractors and customers ▸ Use customer survey tools to understand customer wants, needs, desires and irritants ▸ Focus on operational excellence ▸ Focus on reducing customer irritants ▸ Improve accessibility performance and options	▸ Move customers to lower cost contact channels ▸ Assure work is performed by best cost resources ▸ Increase resource flexibility and scalability ▸ Reduce charge-offs	▸ Focus on continuous process and management system improvement, simplification and standardization across all jurisdictions ▸ Implement technology plans ▸ Further develop bench strength ▸ Become a consolidator of energy usage data

Performance Metrics

- Safety Index
- Customer contact satisfaction
- Commission complaints
- Average speed of answer / Service levels
- One call resolution
- Number of estimated bills
- Bill accuracy
- Employee satisfaction
- Actual cost performance to budget
- Number of Duke employees
- Charge-offs
- Cost per customer
- Number of customer contacts by channel
- Project status

FTT

Customer Service High-level Initiatives

- Customer Service employees – Continue to focus on professional development and implement Customer Service Safety Improvement Plan
- Standardization and Simplification – Implement common business practices as we integrate processes and systems.
- Customer Information System enhancements – Provide a common face to customers and common tools for employees.
- Customer Contact Platform – Includes virtual contact routing, status messaging, IVR enhancements and web single sign on.
- Bill Payment Platform – Includes Pay Agents and Speedpay enhancements.
- Energy Data Management System – Provides a single repository for all meter data and supports the building of an advanced metering infrastructure.

778

Duke Energy®

OHIO/KENTUCKY

Dear DUKE ENERGY Customer:

Please help us provide you with the best possible service! Recently, you, or someone on your behalf, had contact with DUKE ENERGY regarding a service issue.

Please take a few moments to complete this survey and let us know how we did. We value your input in DUKE ENERGY's ongoing quality improvement process. The information you provide will help us to serve you better in the future.

John Kappesser
Customer Satisfaction Manager

To ensure your confidentiality, all surveys are collected and processed by Horan Data Services

Overall Summary - Thinking about [illegible]

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the amount of time you had to wait to speak to a representative?	O	O	O	O	O	O

Please indicate the reason you called Duke Energy to report a service failure:

O Smell of gas
O No electricity in your house
O Downed electric wire
O Replace a fuse/circuit breaker
O Flickering lights
O Power surges
O Tree limb or object on wire
O Damaged electric equipment
O Other

Overall, how long were you on the phone to describe your service request/concern?
O Under 1 minute
O 1-2 minutes
O 2-3 minutes
O 3-4 minutes
O Over 4 minutes

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the length of time [illegible]eded to answer your service request/concern?	O	O	O	O	O	O

[illegible]ow many phone calls did you make to resolve your service request/concern? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of calls it took to resolve your service request/concern?	O	O	O	O	O	O

If it took you more than one call to complete your service request/concern, please explain why: _____

In the past 12 months, how many brief (5 minutes or less) interruptions in your home electric service have you experienced? O 1 O 2 – 3 O 4 – 5 O 6 or more

In the past 12 months, how many lengthy (greater than 5 minutes) interruptions in your home electric service have you experienced? O 1 O 2 –3 O 4 –5 O 6 or more

Please indicate if your contact was reported through an Automated Phone System or with a Customer Service Representative?

O Automated Phone System O Customer Service Representative O Don't know

[illegible] Representative (If contact was through the [illegible])

Thinking about the Duke Energy representative who was most responsible for handling your questions/concerns, please indicate how satisfied you were that he/she...

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...was courteous and friendly?	O	O	O	O	O	O
...listened to you?	O	O	O	O	O	O
...understood your request/concern?	O	O	O	O	O	O
[illegible]d sufficient knowledge?	O	O	O	O	O	O
...treated you with respect?	O	O	O	O	O	O
...summarized any important information that you needed to know?	O	O	O	O	O	O
...explained whether or not you needed to be present for the service work completed?	O	O	O	O	O	O
...will complete your service request as promised?	O	O	O	O	O	O
Overall how satisfied were you with the Duke Energy Representative most responsible for handling your request?	O	O	O	O	O	O

[illegible] Phone System

Thinking about Duke Energy's Automated Phone System, please indicate how satisfied you were with...

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...the information given?	O	O	O	O	O	O
...the ease of finding the menu option you needed?	O	O	O	O	O	O
Overall, how satisfied were you with Duke Energy's Automated Phone System?	O	O	O	O	O	O

Thinking about the Duke Energy service representative who visited your home to complete your service request, how satisfied were you that he/she...

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...arrived quickly?	O	O	O	O	O	O
...displayed a sense of urgency?	O	O	O	O	O	O
...was courteous?	O	O	O	O	O	O
...was knowledgeable?	O	O	O	O	O	O
...treated your property with respect?	O	O	O	O	O	O
...was easily identified as a Duke Energy Service Representative?	O	O	O	O	O	O
...successfully resolved your problem?	O	O	O	O	O	O
Overall, how satisfied were you with the service representative who visited your home?	O	O	O	O	O	O

How long were you without service?

O Under 1 hour O 1-2 hours O 2-3 hours O 3-4 hours O Over 4 hours O Does Not apply

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the length of time it took to restore your service?	O	O	O	O	O	O

What information were you given regarding your electric/gas outage? Please select the best choice.

O *Informed if outage was /was not reported* O Estimated restoration time O No information given O Does Not apply
O Duke Energy crew or outage status O Cause of outage O All of the above

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the information given?	O	O	O	O	O	O

Did you receive a follow-up phone call verifying that your power was restored? O Yes O No O Does Not apply

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
What is your overall level of satisfaction with the way Duke Energy handled your service request/concern?	O	O	O	O	O	O

Would you like a Duke Energy Representative to contact you? O Yes O No

Phone Number: _____ **Name:** _____

Thinking about Duke Energy as a company, using a scale of 1 to 10, with a 1 being Unacceptable, 5 being Average and 10 being Outstanding, how would you rate Duke Energy on...

	Unacceptable 1	2	3	4	Average 5	6	7	8	9	Outstanding 10
...the overall power quality and reliability of your electric service?	O	O	O	O	O	O	O	O	O	O
...the value of service for the amount of money you pay?	O	O	O	O	O	O	O	O	O	O
...the overall billing and payment process?	O	O	O	O	O	O	O	O	O	O
...your overall customer service experience?	O	O	O	O	O	O	O	O	O	O
...their overall reputation as a utility company?	O	O	O	O	O	O	O	O	O	O
...Overall how would you rate Duke Energy as a provider of services to your home?	O	O	O	O	O	O	O	O	O	O

Finally, the following questions are for classification purposes only and will not be used for any other purpose than to help Duke Energy continue to improve its customer service. Please select the category that best describes your situation.

What is your age?

O 18-34 O 35-49 O 50-59 O 60-64 O 65-74 O Over 74

Please indicate your annual household income:

O Under $15,000 O $15,000 - $29,999 O $30,000 - $49,999
O $50,000 - $74,999 O $75,000 - $100,000 O Over $100,000

THANK YOU FOR YOUR RESPONSES!

Duke Energy®

OHIO/KENTUCKY

Dear DUKE ENERGY Customer:

Please help us provide you with the best possible service! Recently, you, or someone on your behalf, had contact with DUKE ENERGY regarding a service issue.

Please take a few moments to complete this survey and let us know how we did. We value your input in DUKE ENERGY's ongoing quality improvement process. The information you provide will help us to serve you better in the future.

John Kappesser
Customer Satisfaction Manager

To ensure your confidentiality, all surveys are collected and processed by Horan Data Services

Please select the one category that best describes your service request: (Choose only one)

O Check the accuracy of your meter or meter reading O Light a pilot light O No heat
O Conduct an inspection of your service O Other_____

Overall, how long were you on the phone to make your service request?

O Under 1 minute O 1-2 minutes O 2-3 minutes O 3-4 minutes O Over 4 minutes

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the length of time needed to answer your service request?	O	O	O	O	O	O

How many phone calls did you make to complete your service request/concerns? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of calls it took to complete your service request?	O	O	O	O	O	O

*If it took you more than one call to complete your service request/concern, please explain why:*_____

How many times were you transferred to another Duke Energy representative? O None O 1 O 2 O 3 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of times transferred?	O	O	O	O	O	O

The Phone Representative

Thinking about the Duke Energy representative who was most responsible for handling your questions/concerns, please indicate how satisfied you were that he/she ..

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...was courteous and friendly?	O	O	O	O	O	O
...listened to you?	O	O	O	O	O	O
...had sufficient knowledge?	O	O	O	O	O	O
...treated you with respect?	O	O	O	O	O	O
...summarized any important information that you needed to know?	O	O	O	O	O	O
...explained whether or not you needed to be present for the service work to be completed?	O	O	O	O	O	O
...will complete your service request as promised?	O	O	O	O	O	O
Overall, how satisfied were you with the Duke Energy Representative most responsible for handling your service request?	O	O	O	O	O	O

MSME

More on Back

[illegible]

Thinking about the Duke Energy service representative who visited your home to complete your service request, how satisfied were you that he/she...

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...arrived on the agreed upon date?	O	O	O	O	O	O
...if necessary, notified you of any schedule changes or delays?	O	O	O	O	O	O
...was courteous?	O	O	O	O	O	O
...was knowledgeable?	O	O	O	O	O	O
...took time to listen to your questions/concerns?	O	O	O	O	O	O
...treated your property with respect?	O	O	O	O	O	O
...was easily identified as a Duke Energy Service Representative?	O	O	O	O	O	O
Overall, how satisfied were you with the service representative who visited your home?	O	O	O	O	O	O

How many visits were required to complete your service request? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with this number of visits?	O	O	O	O	O	O

[illegible]

	Same day	Next day	2 Days	3 Days	4 or more days
From your scheduled appointment date with Duke Energy, what was the length of time for your service request to be completed?	O	O	O	O	O

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
Gave a date that was convenient to complete your service request?	O	O	O	O	O
How satisfied were you with the length of time it took to complete your service request?	O	O	O	O	O
What is your overall level of satisfaction with the way Duke Energy handled your service request?	O	O	O	O	O

[illegible]

Would you like a Duke Energy Representative to contact you? O Yes O No

Phone Number: _____-_____-_____ **Name:** _____ _____

[illegible]

Thinking about Duke Energy as a company, using a scale of 1 to 10, with a 1 being Unacceptable, 5 being Average and 10 being Outstanding, how would you rate Duke Energy on...

	Unacceptable 1	2	3	4	Average 5	6	7	8	9	Outstanding 10
...the overall power quality and reliability of your electric service?	O	O	O	O	O	O	O	O	O	O
...the value of service for the amount of money you pay?	O	O	O	O	O	O	O	O	O	O
...the overall billing and payment process?	O	O	O	O	O	O	O	O	O	O
...your overall customer service experience?	O	O	O	O	O	O	O	O	O	O
...their overall reputation as a utility Company?	O	O	O	O	O	O	O	O	O	O
...Overall how would you rate Duke Energy as a provider of services to your home?	O	O	O	O	O	O	O	O	O	O

[illegible]

Finally, the following questions are for classification purposes only and will not be used for any other purpose than to help Duke Energy continue to improve its customer service. Please select the category that best describes your situation.

What is your age?

O 18-34 O 35-49 O 50-59 O 60-64 O 65-74 O Over 74

Please indicate your annual household income.

O Under $15,000 O $15,000 - $29,999 O $30,000 - $49,999
O $50,000 - $74,999 O $75,000 - $100,000 O Over $100,000

THANK YOU FOR YOUR RESPONSES!

Duke Energy®

Ohio/Kentucky

Dear DUKE ENERGY Customer:

Please help us provide you with the best possible service! Recently, you, or someone on your behalf, had contact with a DUKE ENERGY representative on the phone.

Please take a few moments to complete this survey and let us know how we did. We value your input in DUKE ENERGY's ongoing quality improvement process. The information you provide will help us to serve you better in the future.

John Kappesser
Customer Satisfaction Manager

To ensure your confidentiality, all surveys are collected and processed by Horan Data Services

I. Call Summary - Thinking about your most recent telephone call to Duke Energy, please tell us the following about that call:

Please select one category that best describes the reason you called Duke Energy: (Choose only one)

O To discuss payment arrangements	O To discuss an estimated bill	O Moved/changed address
O To ask about a high bill	O To reconnect service	O To ask about due date/bill amount
O To discuss Budget Billing	O To clarify information on the bill	O Did not get a bill
O To discuss e-Bill/electronic payment	O Other _____	

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the ease of contacting Duke Energy by telephone?	O	O	O	O	O	O

When you called Duke Energy, how long did you wait to speak to a representative?
O 0-10 seconds O 11-20 seconds O 21-30 seconds
O 31-60 seconds O Over 60 seconds

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the amount of time you had to wait?	O	O	O	O	O	O

How many phone calls did it take you to resolve your question/concern?
O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of calls it took to resolve your question/concern?	O	O	O	O	O	O

If it took more than one call to resolve your question/concern, please explain why: _____

How many times were you transferred to another Duke Energy representative?
O None O 1 O 2 O 3 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of times transferred?	O	O	O	O	O	O

Overall how long were you on the phone resolving your question/concern?

O Less than 1 minute O 1-3 minutes O 4-6 minutes O 7-9 minutes O Over 10 minutes O Does not apply

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the length of the phone call?	O	O	O	O	O	O

II. Phone Representative

Thinking about the Duke Energy representative who was most responsible for handling your call, please indicate how satisfied you were that he/she ....

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...was courteous and friendly?	O	O	O	O	O	O
...listened to you?	O	O	O	O	O	O
...had sufficient knowledge?	O	O	O	O	O	O
...treated you with respect?	O	O	O	O	O	O
...offered choices/options that were useful to you?	O	O	O	O	O	O
...summarized information you needed to know?	O	O	O	O	O	O
...was sensitive to your situation?	O	O	O	O	O	O
...will complete your service request as promised?	O	O	O	O	O	O
Overall, how satisfied were you with the Duke Energy representative who handled your questions/concerns?	O	O	O	O	O	O

More on Back

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
What is your overall level of satisfaction with the way Duke Energy handled your question/concern?	O	O	O	O	O	O

Would you like a Duke Energy Representative to contact you? O Yes O No

Phone Number: _____-_____-_____ **Name:** _____

Thinking about the bill you receive each month from Duke Energy, how satisfied are you that...	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...your meter reader acts in a courteous manner?	O	O	O	O	O	O
...your meter reader makes a good effort to read your meter on a monthly basis?	O	O	O	O	O	O
...your meter reader treats your property with respect?	O	O	O	O	O	O
What is your overall level of satisfaction with your Duke Energy meter reader?	O	O	O	O	O	O
...the bill is accurate?	O	O	O	O	O	O
...the bill is easy to understand?	O	O	O	O	O	O

If your bill was not easy to understand, please explain why: _____

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
What is your overall level of satisfaction with the format of your Duke Energy Bill?	O	O	O	O	O

Over the past 12 months, which Duke Energy bill payment method do you prefer to use most often?

O eBill/online bill payment O Mail in payment O Pay in person (Duke Payment Center)

O Bank Draft (Automatic Payment Plan/Bill Payer 2000)

Thinking about the payment method that you use most often how satisfied are you that...	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
...Duke Energy offers convenient bill payment options?	O	O	O	O	O
...your monthly payments are accurately applied to your account?	O	O	O	O	O
What is your overall level of satisfaction with the payment method that you prefer to use most often?	O	O	O	O	O

Thinking about Duke Energy as a company, using a scale of 1 to 10, with a 1 being Unacceptable, 5 being Average and 10 being Outstanding, how would you rate Duke Energy on...

	Unacceptable 1	2	3	4	Average 5	6	7	8	9	Outstanding 10
...the overall power quality and reliability of your electric service?	O	O	O	O	O	O	O	O	O	O
...the value of service for the amount of money you pay?	O	O	O	O	O	O	O	O	O	O
...the overall billing and payment process?	O	O	O	O	O	O	O	O	O	O
...your overall customer service experience?	O	O	O	O	O	O	O	O	O	O
...their overall reputation as a utility company?	O	O	O	O	O	O	O	O	O	O
...Overall how would you rate Duke Energy as a provider of services to your home?	O	O	O	O	O	O	O	O	O	O

Finally, the following questions are for classification purposes only and will not be used for any other purpose than to help Duke Energy continue to improve its customer service. Please select the category that best describes your situation.

What is your age?	O 18-34	O 35-49	O 50-59
	O 60-64	O 65-74	O Over 74
Please indicate your annual household income:			
	O Under $15,000	O $15,000 - $29,999	O $30,000 - $49,999
	O $50,000 - $74,999	O $75,000 - $100,000	O Over $100,000

THANK YOU FOR YOUR RESPONSES!

Duke Energy®

Ohio/Kentucky

Dear DUKE ENERGY Customer:

Please help us provide you with the best possible service! Recently, you, or someone on your behalf, had contact with a DUKE ENERGY representative regarding the turn on, turn off or transfer of service.

Please take a few moments to complete this survey and let us know how we did. We value your input in DUKE ENERGY's ongoing quality improvement process. The information you provide will help us to serve you better in the future.

John Kappesser
Customer Satisfaction Manager

To ensure your confidentiality, all surveys are collected and processed by Horan Data Services

When you called Duke Energy, how long did you wait to speak to a representative?

O 0-10 seconds O 11-20 seconds O 21-30 seconds O 31-60 seconds O Over 60 seconds

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
How satisfied were you with the amount of time you had to wait?	O	O	O	O	O

How many phone calls did you make to complete your service request/concern? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
How satisfied were you with the number of the phone calls it took to complete your service request/concern?	O	O	O	O	O

If it took you more than one call to complete your service request/concern, please explain why: _____

How many times were you transferred to another Duke Energy Representative? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the number of times you were transferred?	O	O	O	O	O	O

When you called Duke Energy, how long were you on the phone to make your service request?

O 1-3 minutes O 4-6 minutes O 7-9 minutes O 10-12 minutes O Over 13 minutes

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with the length of time needed to answer questions or complete your service request?	O	O	O	O	O	O

The Duke Energy Representative

Thinking about the Duke Energy representative who was most responsible for handling your call, please indicate how satisfied you were that he/she

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...was courteous and friendly?	O	O	O	O	O	O
...listened to you?	O	O	O	O	O	O
...had sufficient knowledge?	O	O	O	O	O	O
...treated you with respect?	O	O	O	O	O	O
...offered choices/options that were useful to you?	O	O	O	O	O	O
...summarized any important information that you needed to know?	O	O	O	O	O	O
...explained whether or not you needed to be present for the service work to be completed?	O	O	O	O	O	O
...will complete your service request/concern as promised?	O	O	O	O	O	O
Overall, how satisfied were you with the Duke Energy representative most responsible for handling your service request/concern?	O	O	O	O	O	O

Duke Energy's Suggestions

Were you asked to speak with a representative to confirm your request and offer other services? O Yes O No O Don't know

Did you sign up for additional services? O Yes O No

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
Overall, how satisfied were you with the confirmation portion of this call?	O	O	O	O	O	O

More on Back ☞

TOME

Thinking about the Duke Energy service representative who visited your home to complete your service request, how satisfied were you that he/she...

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...arrived on the agreed-upon date?	O	O	O	O	O	O
...if necessary, notified you of any schedule changes or delays?	O	O	O	O	O	O
...was courteous?	O	O	O	O	O	O
...was knowledgeable?	O	O	O	O	O	O
...took time to listen to your questions/concerns?	O	O	O	O	O	O
...treated your property with respect?	O	O	O	O	O	O
...was easily identified as a Duke Energy Service Representative?	O	O	O	O	O	O
Overall, how satisfied were you with the service representative who visited your home?	O	O	O	O	O	O

How many visits were required to complete your service request? O 1 O 2 O 3 O 4 or more

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
How satisfied were you with this number of visits?	O	O	O	O	O	O

	Same day	Next day	2 Days	3 Days	4 or more days
From your scheduled appointment date with Duke Energy, what was the length of time for your service request to be completed?	O	O	O	O	O

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
Gave a date that was convenient to complete your service request?	O	O	O	O	O
How satisfied were you with the length of time it took to complete your service request?	O	O	O	O	O
What is your overall level of satisfaction with the way Duke Energy handled your service request?	O	O	O	O	O

Would you like a Duke Energy Representative to contact you? O Yes O No

Phone Number: _____-_____-_____ **Name:** _____

Thinking about Duke Energy as a company, using a scale of 1 to 10, with a 1 being Unacceptable, 5 being Average and 10 being Outstanding, how would you rate Duke Energy on .

	Unacceptable 1	2	3	4	Average 5	6	7	8	9	Outstanding 10
...the overall power quality and reliability of your electric service?	O	O	O	O	O	O	O	O	O	O
...the value of service for the amount of money you pay?	O	O	O	O	O	O	O	O	O	O
...the overall billing and payment process?	O	O	O	O	O	O	O	O	O	O
...your overall customer service experience?	O	O	O	O	O	O	O	O	O	O
...their overall reputation as a utility Company?	O	O	O	O	O	O	O	O	O	O
...Overall how would you rate Duke Energy as a provider of services to your home?	O	O	O	O	O	O	O	O	O	O

Finally, the following questions are for classification purposes only and will not be used for any other purpose than to help Duke Energy continue to improve its customer service. Please select the category that best describes your situation.

What is your age?

O 18-34 O 35-49 O 50-59 O 60-64 O 65-74 O Over 74

Please indicate your annual household income.

O Under $15,000 O $15,000 - $29,999 O $30,000 - $49,999
O $50,000 - $74,999 O $75,000 - $100,000 O Over $100,000

THANK YOU FOR YOUR RESPONSES!

Duke Energy®

OHIO/KENTUCKY

Dear DUKE ENERGY Customer:

Please help us provide you with the best possible service! Recently, you, or someone on your behalf, made a payment at a DUKE ENERGY payment center or pay station.

Please take a few moments to complete this survey and let us know how we did. We value your input in DUKE ENERGY's ongoing quality improvement process. The information you provide will help us to serve you better in the future.

John Kappesser
Customer Satisfaction Manager

To ensure your confidentiality, all surveys are collected and processed by Horan Data Services

I. Initial Contact - Thinking about your most recent [illegible]

Please select one or more of the following statements that explain why you chose to pay your bill at a Duke Energy Payment Center or pay station/pay agent

O You prefer to do business in person
O To avoid late payment charges
O To avoid disconnect
O To request reconnection or reestablish service
O To avoid postage costs
O Other________________
O Location
O Convenience

When you visited the Duke Energy Payment Center, please indicate how you made your payment:

O At the drop box
O At the counter
O Drive through window

w many visits did it take you to complete your payment O 1 O 2 O 3 O 4 or more

How satisfied were you with the number of visits?

Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
O	O	O	O	O	O

What time of the day did you visit the payment center?

O 8am-10am
O 10am-12 noon
O 12 noon- 2pm
O 2pm- 5pm
O After 5pm

How many times have you visited a Duke Energy Payment Center in the past 12 months?

O 1-3
O 4-6
O 7-9
O 10-12
O 13 or More

How satisfied were you with the convenience of paying your bill at the Duke Energy Payment Center?

Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
O	O	O	O	O	O

How long were you in the center to pay your bill?

O 5 minutes or less
O 6-10 minutes
O 11-15 minutes
6-20 minutes
O Over 20 minutes

How satisfied were you with the amount of time?

Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
O	O	O	O	O	O

II. Duke Energy Representative [illegible] (If you used the drop box, please skip [illegible])

Thinking about the Duke representative you worked with at our payment center please indicate how satisfied you were that he/she...	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...was courteous and friendly?	O	O	O	O	O	O
...listened to you?	O	O	O	O	O	O
Overall, how satisfied were you with the Duke Energy Payment Center / Paystation/ Pay Agent representative who assisted you?	O	O	O	O	O	O

OBPME

More on Back ☞

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
What is your overall level of satisfaction with the service you received at the Duke Energy Payment Center?	O	O	O	O	O	O

Would you like a Duke Energy Representative to contact you? O Yes O No

Phone Number: _____-_____-_____ **Name:** _____

Thinking about the bill you receive each month from Duke Energy, how satisfied are you that...	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied	Does Not Apply
...your meter reader acts in a courteous manner?	O	O	O	O	O	O
...your meter reader makes a good effort to read your meter on a monthly basis?	O	O	O	O	O	O
...your meter reader treats your property with respect?	O	O	O	O	O	O
What is your overall level of satisfaction with your Duke Energy meter reader?	O	O	O	O	O	O
...the bill is accurate?	O	O	O	O	O	O
...the bill is easy to understand?	O	O	O	O	O	O

If your bill was not easy to understand, please explain why: _____

	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
What is your overall level of satisfaction with the format of your Duke Energy Bill?	O	O	O	O	O

Over the past 12 months, which Duke Energy bill payment method do you prefer to use most often?

O eBill/online bill payment O Mail in payment O Pay in person (Duke Payment Center)

O Bank Draft (Automatic Payment Plan/Bill Payer 2000)

Thinking about the payment method that you use most often how satisfied are you that...	Very Dissatisfied	Dissatisfied	Neither	Satisfied	Very Satisfied
...Duke Energy offers convenient bill payment options?	O	O	O	O	O
...your monthly payments are accurately applied to your account?	O	O	O	O	O
What is your overall level of satisfaction with the payment method that you prefer to use most often?	O	O	O	O	O

Thinking about Duke Energy as a company, using a scale of 1 to 10, with a 1 being Unacceptable, 5 being Average and 10 being Outstanding, how would you rate Duke Energy on...

	Unacceptable 1	2	3	4	Average 5	6	7	8	9	Outstand 10
...the overall power quality and reliability of your electric service?	O	O	O	O	O	O	O	O	O	O
...the value of service for the amount of money you pay?	O	O	O	O	O	O	O	O	O	O
...the overall billing and payment process?	O	O	O	O	O	O	O	O	O	O
...your overall customer service experience?	O	O	O	O	O	O	O	O	O	O
...their overall reputation as a utility company?	O	O	O	O	O	O	O	O	O	O
...Overall how would you rate Duke Energy as a provider of services to your home?	O	O	O	O	O	O	O	O	O	O

Finally, the following questions are for classification purposes only and will not be used for any other purpose than to help Duke Energy continue to improve its customer service. Please select the category that best describes your situation.

What is your age?	O 18-34	O 35-49	O 50-59
	O 60-64	O 65-74	O Over 74
Please indicate your annual household income.			
	O Under $15,000	O $15,000 - $29,999	O $30,000 - $49,999
	O $50,000 - $74,999	O $75,000 - $100,000	O Over $100,000

THANK YOU FOR YOUR RESPONSES!

Duke Energy®

To Our Valued Customer:

Installing new services for our customers is one of the most important things we do at Duke Energy. We recently completed a new service installation project for you, and we want your feedback. Our goal is to improve the new service installation process, and your input is extremely valuable.

Please take a few minutes to complete this survey on your recent new service installation project with Duke Energy. The location of the new service we installed for you is printed beneath your name and address for your reference when completing the survey. A postage-paid envelope is enclosed for returning the survey.

(If you are not the person most familiar with Duke Energy's performance on this project, please forward this survey to the appropriate individual in your organization.)

Thank you for completing the survey. Your opinions are very important to us.

If you have any questions about the survey, please contact John Kappesser at (513) 287-1774.

Sincerely,

John Kappesser

John Kappesser

Customer Satisfaction Manager