Large Filing Separator Sheet

Case Number: 07-589-GA-AIR
07-590-GA-ALT
07-591-GA-AAM

Date Filed: 7/18/2007

Section: 5 of 7

Number of Pages: 185

Description of Document: Vol. 4, Vol. 5 and Vol. 6
Schedules S-4.2

These groups perform a control function by agenda, with regular scheduled items to review ongoing operations and decisions. The IT PMO in particular is a control function for project work. In addition, various compliance activities and audits are conducted of projects, scheduled and routine work by the compliance function within IT, by the internal audit department, and by various third-party auditors (for example, annual SOX certification).

VII. Internal and External Communication

Internal Communication

Internal communications are accomplished through a wide variety of departmental meetings and other communications mechanisms.

All levels of management within the department conduct regular staff meetings which serve as the primary means to collect and disseminate information within the department. From time to time, the CIO will issue department wide communications discussing major initiatives or events. All hands management meetings are sometimes conducted to discuss topics appropriate for management.

Within the Company, the IT function sometimes writes and publishes articles of general interest on the Company's web-based internal Portal. Items concerning IT security that affect the workforce at large are a good example of this type of communication. Relationships exist across the application divisions with various functional areas of the business and they work closely together day to day. Within the Customer Support division, both a Company-wide Help Desk and a Deskside Consulting function provide assistance to the workforce for IT-related matters.

The Portal includes an IT Home page which serves as a reference library for the IT Department on strategy, policy and service information. The IT Standards page provides technology architecture and standards information to IT practitioners and end-users of IT alike. The IT Security page provides information related to policy, standards, best practices, processes, key contacts other useful reference information which is of interest to both IT professionals and end-users.

External Communication

The IT department communicates externally primarily through relationships with suppliers of IT products and services. These include responding to solicitations, issuing Requests for Information/Quotes/Proposals, or other communication related to the execution of work under various contracts for products and services.

Personnel in the IT department participate in various community programs such as Duke Energy's annual Global Services Event, local Chamber of Commerce activities, educational programs, and other events and activities.

VIII. Goal-Attainment and Qualification

Department employees participate in a Short Term Incentive (STI) plan administered by Corporate Human Resources. These plans are developed annually and consist of a combination of corporate measures, departmental and/or operational measures. Goals within a plan have levels of attainment which include a minimum threshold for any payout, target and maximum payout levels.

Financial measures are certified by Corporate Finance. Project documentation, deliverables from projects, published service level data are examples of quantitative data that is collected, submitted and filed with certified incentive plans at year end. Two levels of management including the Senior Vice President and CIO are required to certify an incentive plan. This documentation is input into the payroll process and become auditable business records.

Exhibit IT-1

Information Technology Asset Management Policy - IT 2000

Applicability:	Applies to Enterprise
Originator:	Chief Information Officer
Approval:	Group Vice President, Duke Energy Business Services
Effective Date:	12/31/2001
Revision Date:	09/20/2000
Reissue Date:	07/06/2004

Statement of Purpose and Philosophy

Duke Energy recognizes that information is an essential and valuable corporate asset that is deeply embedded in our Business values of integrity, stewardship, and accountability. The availability, accessibility, security, and integrity of information within Duke Energy, and between other companies, customers, suppliers, and other key stakeholders, are vital to our Business values and objectives.

Policy Expectations

All accesses to, uses of, and processing of Company information must be consistent with related policies, standards and procedures.

- Use of information resources must comply with the *Duke Energy Code of Business Ethics* and with *Federal* and *State Codes of Conduct.*
- An inventory of major Enterprise information assets must be maintained to define, locate, and manage business critical information.
- Systems development and maintenance must be performed using a life cycle methodology that includes appropriate security consideration for information assets in accordance with Information Technology 5007 - Information Systems Acquisition, Development, and Maintenance.
- All users of Company information must comply with the control requirements specified by Information Technology Security Policy, Standards, and Procedures - IT 5000 Series.
- Information will be retained in accordance with periods established by Records Management Policy

Accountability: Roles and Responsibilities

Senior management has the responsibility for the stewardship of information assets within their business units.

This policy and associated standards and procedures apply to all Duke Energy Employees and any other authorized individuals (e.g., contractors, vendors, consultants).

Key Terms

Information Assets : Information or information technology that provides value to Duke Energy.

Exhibit IT-2

Software License Management Policy - IT 2010

Applicability:	Applies to Enterprise
Originator:	Chief Information Officer
Approval:	Group Vice President, Duke Energy Business Services
Effective Date:	06/01/2001
Revision Date:	03/22/2000
Reissue Date:	07/06/2004

Statement of Purpose and Philosophy

A cornerstone of Duke Energy's values of integrity and accountability is to behave ethically and meet the sprit and the letter of the law. This Policy establishes Duke Energy's position on appropriate licensing and protection of computer software. Unauthorized use of software may subject users and/or Duke Energy to both civil and criminal penalties.

Policy Expectations

Duke Energy will respect all software copyrights and adhere to terms of all software licenses to which Duke Energy is a party. This includes licensed software, shareware, freeware, and personally owned software, residing on all Duke Energy technology assets including but not limited to mainframes, servers and workstations. This also includes Duke Energy licensed software on non-company owned technology assets.

It is the policy of Duke Energy that computer software assets will be appropriately licensed and protected from unauthorized use, disclosure, tampering, or theft.

Accountability: Roles and Responsibilities

Duke Energy will adhere to the following guidelines for all software purchased by Duke Energy or used on Duke Energy technology assets:

- Use all software in a manner consistent with the applicable license agreement
- Duplicate licensed software and related documentation for use on Duke Energy premises or elsewhere only as authorized by agreement with the licensor
- Acquire software only through authorized channels
- Maintain complete records of all software in use for purposes of inventory, registration, support and upgrade for purchased software by Duke Energy
- Use only authorized software on Duke Energy equipment

Enterprise-Wide Software License Management

A corporate IT department will be designated to coordinate the management of software licenses for generally used products where economic benefit can be achieved. They will administer the allocation of these licenses to business units and ensure usage consistent with the applicable license agreement. Processes, procedures and controls to ensure complete compliance with the statement and guidelines of this policy and associated enterprise standards for all software in use. The Business Unit will maintain current information necessary to demonstrate compliance.

Audit Services

As a part of its normal reviews, Duke Energy Audit Services will perform periodic audits to ensure the Business Unit is in compliance with this Policy.

Individual Users

All individuals with access to Duke Energy assets will ensure they comply with all software agreements and copyright laws. The use of illegal copies, pirated software or related materials is strictly prohibited. Violations of this policy should be reported management for appropriate disciplinary action. Employees should contact their supervisor or local information technology support team if they have any questions on license compliance.

Exhibit IT-3

Technology Change Control - IT 3010

Applicability:	Applies to Enterprise
Originator:	Chief Information Officer
Approval:	Group Vice President, Duke Energy Business Services
Effective Date:	07/19/2000
Revision Date:	07/19/2000
Reissue Date:	07/06/2004

Statement of Purpose and Philosophy

Information technology is a valuable function that requires proper controls to ensure Duke Energy's values of integrity and accountability are not compromised. A formal change control policy for information technology ensures all changes are authorized, documented and made at the approved time in the approved manner.

Policy Expectations

This policy provides the discipline and management of the technology production environment by controlling all changes made to it. This policy applies to changes made to software and hardware, and is relevant to voice communications systems and data communications systems. Technology change procedures and standards apply to all technology changes, including vendor-supplied and in-house.

Change control procedures and standards describe the process to request approve, test and migrate a change into a production environment. All activities related to the development, procurement, operation, and maintenance of Information Technology in support of the Nuclear policies and procedures are also subject to the requirements of the Duke Energy Corporation Topical Report, Quality Assurance Program.

Accountability: Roles and Responsibilities

This policy and associated standards and procedures apply to all Duke Energy Employees and any other authorized individuals (e.g., partners, contractors, vendors, consultants) working with Information Technology.

A formal written change control process must address the following objectives:

- Technology changes move from a test environment into production only after receiving proper authorization from the technical/production manager and the client owner of the change.
- The approver must not be the developer of the change and must be management level.
- A process must be implemented to notify affected parties prior to making the change.

- Technology change processes will address a method for tracking who is responsible for releasing the change, a description of the change and when the change was made. These change control processes must include proper approval and testing of all changes, and preparation of supporting documentation prior to moving changes into a production environment.

- Documentation reflecting changes to production computer and communications systems must be prepared prior to the change being implemented into production. Exceptions due to emergency changes must be documented for approval within a reasonable time frame specified in the procedure.

Key Terms

Production: A technology system relied on by any Duke Energy business unit to conduct business and to make business decisions.

Technology Change : New implementations, upgrades, replacements or enhancements to technology system such as telecommunications, networks, operating systems, servers, mainframes, applications, and databases.

Exhibit IT-4

Duke Energy SM

INFORMATION SECURITY POLICY, STANDARDS, AND PROCEDURES

IT 5000 SERIES

Version 1.0

May 1st, 2006

Exhibit IT-4

IT 5000 Series

Version 1.0 of the IT 5000 Series aligns Duke Energy with the International Standard Organization's Code of Practice for information technology (ISO 17799:2005) and incorporates the best security practices as established by the merger of Duke Energy and Cinergy on April 1st, 2006. The IT 5000 Series is comprised of the IT 5000 Policy and supporting Standards and Procedures. The Information Security Policy (Section 5000) represents Executive Management's commitment to the IT Security and authorizes the IT 5000 Series as the governance documentation for the Enterprise. The supporting Standards are organized in the subsequent sections of the IT 5000 Series (5001 - 5010) with references to specific procedures.

The IT 5000 Series are the property of Duke Energy. Reproduction, distribution, or unauthorized use is strictly prohibited without the expressed written consent of Duke Energy. Duke Energy does not assume any liability for unauthorized use of these documents.

Exhibit IT-4

Duke Energy.
IT 5000 Series

Table of Contents

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-4

Table of Contents

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-4

Table of Contents

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-4

Table of Contents

Exhibit IT-4

Table of Contents

Exhibit IT-4

Duke Energy Policy Statement

IT 5000 – Enterprise Information Security Policy

Applicability: Enterprise
Originator: Corporate IT Strategy and Compliance
Approval:

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

Statement of Purpose

Information and the associated information technologies are one of Duke Energy Corporation's (Duke Energy) most valuable assets and are essential for maintaining and improving Duke Energy's competitive position. The IT 5000 Policy is Executive Management's "Statement of Commitment" to protecting Duke Energy's information assets, and serves as the official, authorized governing policy for Enterprise IT Security. The purpose of this policy, and the supporting standards and procedures, collectively known as the IT 5000 Series, is to state the Enterprise requirements for the protection of information assets, and to ensure the confidentiality, integrity, and availability of company information.

Policy Expectation

This policy applies to all employees, contractors, vendors, agents, third parties, or any other person(s) who have access to Duke Energy information assets or facilities housing information assets. It is expected that they will understand and comply with the policies, standards, and procedures addressed herein, and further that it is the responsibility of all users to protect company information assets at all times. Information assets remain the property of Duke Energy, regardless of location, point of access, or mode of transfer from one point to another, and are subject to the security polices defined in the IT 5000 Series.

IT 5000.1 Information Security Policy

a) The IT 5000 Policy, Standards, and Procedures define the minimally acceptable requirements for the protection of Duke Energy information assets.

b) Corporate IT Strategy and Compliance is responsible for Duke Energy's IT Security Program. In this role they are responsible for the IT 5000 Series and for maintaining a consistent enterprise-wide approach to information protection.

c) Each Business Unit is responsible for implementation of the security requirements defined in the IT 5000 Series documents and to provide support to Corporate IT Strategy and Compliance.

d) Access to information assets by individuals or information systems will only be granted in support of specific business needs and will be controlled through the IT 5000 Series documents. All Information assets will be assigned a security classification of confidential, unless otherwise stated.

e) In protecting its information assets, Duke Energy will comply with applicable laws and regulations; provided, however, that Duke Energy may require a higher level of security.

f) Persons who use Duke Energy information assets are subject to monitoring. Persons who violate Duke Energy policy are subject to disciplinary action, up to and including, termination.

g) Enforcement of IT Security policy, or lack of enforcement by Corporate IT Strategy and Compliance or other governing bodies, is not an indication of acceptance of a non-compliant practice.

Duke Energy proprietary and confidential: Internal use only.

Exhibit IT-4

IT 5000 – Enterprise Information Security Policy

IT 5000.2 Review of the Information Security Policy

To ensure consistent and current alignment with enterprise goals, legal and regulatory compliance, and maintenance of an effective enterprise security posture, Corporate IT Strategy and Compliance is responsible for measuring enterprise compliance with, and the effectiveness of, the IT 5000 Series documents through an enterprise compliance program. The IT 5000 Series documents will be reviewed to ensure they provide relevant guidance for the security of Duke Energy's information assets.

Exhibit IT-4

Duke Energy.

Duke Energy Standard

IT 5001 – IT Security Program Structure

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 IT 5000 Policy is Executive Management's "Statement of Commitment" to protecting Information assets, and serves as the official, authorized governing policy for Enterprise IT Security. Approved by the **Executive Committee (TBD)**, the IT 5000 Policy, and the supporting Standards and Procedures, define the minimally acceptable requirements for information security, and provide a consistent enterprise-wide approach to information asset protection.

IT 5001.1 IT Security Program Structure

The IT 5000 Series is comprised of a Policy (IT 5000), supporting Standards (IT 5001- 5010) and Procedures.

IT 5001.2 IT 5000 Series Maintenance Program

The IT 5000 Series Maintenance Program must ensure the IT 5000 Series (Policy, Standards, and Procedures) are properly controlled, revised, approved and disseminated. The Maintenance Program must comprise of the following components:

a) An organizational structure that includes representation from cross-functional and organizational boundaries.

b) A Change Management Process that includes modification triggers and levels of approval.

c) Communications Management to include effective dates and compliance expectations.

For more information, see "IT 5001-01 IT 5000 Series Program".

IT 5001.3 Information Security Hierarchy: Roles and Authorities

This section defines the security program governance hierarchy.

IT 5001.3.1 Internal Organization

The Corporate Information Security organization is comprised of the following:

Chief Information Officer (CIO) – the CIO has authority to develop and implement Information Security policies and procedures for the enterprise.

Director of IT Security Strategy and Compliance – the Director of Corporate IT Strategy and Compliance has been delegated authority to act on behalf of the CIO on items of Information Security.

Corporate IT Strategy and Compliance – Corporate IT Strategy and Compliance is composed of information security subject matter experts (SME) and reports to the Director of Corporate IT Security.

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-4

IT 5001 – IT Security Program Structure

IT 5001.3.2 Management Commitment to Information Security

The approval of the IT 5000 Policy demonstrates management's commitment to Information Security.

IT 5001.3.3 Information Security Coordination

Coordinated groups are the committees or Business Unit areas that provide, or support, a security function.

Information Technology Management Team (ITMT) – chaired by the CIO and comprised of IT leaders from the major Business Units.

Information Security Council - chaired by the Director of Corporate IT Strategy and Compliance and comprised of management level representatives from the Business Units and/or functional areas; the ISC chair and/or the ITMT member nominates members and the ITMT endorse them.

Information Security Council Working Team (ISC WT) – chaired by a member of Corporate IT Strategy and Compliance department and comprised of SME's from the various functional areas; the ISC and/or ITMT members assign members.

Business Unit Information Security Function (BUISF) – individual or group assigned by each Business Unit; familiar with the IT 5000 Series documents and the business and operational requirements of the specific Business Unit.

IT Security Operations – Organizationally, accountable to the CIO.

IT Security Administration – Organizationally, accountable to the CIO.

Audit Services – IT Audit Services reporting to the CCO (Chief Compliance Officer).

IT 5001.3.4 Allocation of Information Security Responsibilities

CIO – has ultimate accountability for IT Security for the enterprise and is the final authority on matters of information security. See the ETIS SS&C Charter for specific responsibilities.

Director of IT Security Strategy and Compliance – the Director of Corporate IT Strategy and Compliance has been delegated authority to act on behalf of the CIO on items of Information Security.

Corporate IT Strategy and Compliance – corporate department composed of information security subject matter experts (SME). Provides security strategies and measures corporate compliance.

IT Security Operations – provides operational services consisting of intrusion monitoring, virus monitoring, spam prevention, CIRT, procedures investigations, Internet monitoring, and scanning services.

IT Security Administration – provides administrative services consisting of IT account management and access account administration.

Audit Services – reviews business activities to confirm compliance as part of their normal corporate role and reports the results to the CIO, Corporate IT Security, and the responsible Business Unit.

ITMT – approves modifications to the Policies and Standards and endorses modifications to Procedures; responsible for communicating IT Security related issues that affect their organizational areas of responsibilities, and approving exceptions that may effect the enterprise. See the 'ITMT Operating Guidelines' for specific responsibilities.

Exhibit IT-4

IT 5001 – IT Security Program Structure

ISC – endorses modifications to the policies and standards, approves modifications to procedures, and is an active member of the BUISF. See the ISC Charter for specific responsibilities.

ISC WT – reviews, designs, develops, or modifies the IT 5000 Series documents. See the ISC Charter for specific responsibilities.

BUISF – provides Business Unit coordination with Corporate IT Strategy and Compliance on issues concerning functional implementation of the IT 5000 Series documents. Responsibilities include but are not limited to the following:

a) Provide communications, awareness, and compliance assistance within the Business Unit.

b) Identify, develop and approve Business Unit specific information security standards and procedures, when corporate standards and/or procedures do not exist.

c) Review and document exceptions to the IT 5000 Series. Exceptions that have the potential to impact systems beyond the business unit must be processed using the enterprise exception processes, see "IT 5010-01 Standard Exception".

5001.4 Departmental Names

Policy and Standard Designation	Departmental Name
Corporate IT Strategy and Compliance	Corporate group that is responsible for the development and implementation of IT security strategy, policies, and standards. As well as the development and implementation of IT Compliance programs.
Corporate IT Security Operations	IT Security Operations: Corporate group responsible for IDS, Virus protect, CIRT Process, etc.
Corporate IT Security Admin	IT Security Admin: Corporate group responsible for access account administration (NAM), GPO management, etc.
Corporate Security	Corporate Security group that is responsible for asset protection programs, available security training and other services for employees and management to help safeguard Duke Energy Corporation facilities and assets.

Table 1-1: Departmental Names

Exhibit IT-4

IT 5001 – IT Security Program Structure

5001.5 Acronyms

Acronym	Identifier
ACL	Access Control List
ASP	Application Service Provider
BUISF	Business Unit Information Security Function
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CoBE	Duke Energy Code of Business Ethics
COTS	Commercial off the Shelf
DAE	Duke Application Environment
DMZ	Demilitarized Zone
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ID	Identifier
IT	Information Technology
SDLC	System Development Life Cycle
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network
WIP	Workforce Identification Process
SME	Subject Matter Expert

Table 1-2: Acronyms

Exhibit IT-4

Duke Energy.

Duke Energy Standard

IT 5002 – Asset 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 defines the requirements for the management and use of Duke Energy information assets.

IT 5002.1 Responsibility for Assets

Access to and the use of Duke Energy information assets implies certain user responsibilities. Persons who use these company information assets consent to the provisions of, and agree to comply with the requirements IT 5000 series.

IT 5002.2 Inventory of Assets

Each Business Unit is responsible for maintaining an inventory of their information assets. The inventory must identify the asset, the assigned owner or manager and be reviewed annually.

IT 5002.3 Ownership of Assets

Every component of an information system must have an individual assigned as the Owner. The Owner is responsible for ensuring Duke Energy information assets are properly managed and compliant with federal, state, and local laws, regulatory requirements, and the IT 5000 Series. Ownership responsibility must be reviewed annually or whenever there is a change in job responsibilities.

Note: Ownership is a functional definition, all Information Assets are the sole property of Duke Energy, whether internally developed or purchased.

There are six categories of ownership responsibility:

1. Information Sponsor – a vice president or manager of a Business Unit who is accountable for information security in their Business Unit and new or acquired entities. The Information Sponsor ensures that ownership responsibilities within their Business Unit are clearly defined and maintained and the necessary resources have been allocated to support Enterprise Information Security.

2. Information System Owner- a Duke Energy employee in a management position who is responsible for a specific Information System. The Information System Owner is responsible for the confidentiality, integrity, and availability of an Information system. The Information System Owner is responsible for ensuring the system has a defined business need and all aspects of the system; hardware, software, and information are properly managed. The Information System Owner may retain the responsibilities of the Information Owner and Information Technology Manager or may delegate all or part of the responsibility to others.

3. Information Owner - a Duke Energy employee in a management position who is responsible for specific information. The Information Owner is accountable for establishing security classifications and access

Exhibit IT-4

authorization. Responsibilities include, but are not limited to, "IT 5002.5 Security Classification", "IT 5005 Communications and Operations Management" and "IT 5006 Access Controls". The Information Owner will perform these tasks or may delegate them to one or more Custodians.

4. Information Technology Manager – a Duke Energy employee in a management position who is responsible for specific information technology. The Information Technology Manager is accountable for management of the hardware, software, and networking assets that are required to manage information. Responsibilities include, but are not limited to, "IT 5004 Physical and Environmental Security", "IT 5005 Communications and Operations Management", "IT 5006 Access Controls", "IT 5007 Information Systems Acquisition, Development and Maintenance", and "IT 5009 Business Continuity Management". The Information Technology Manager will perform these tasks or may delegate them to one or more Custodians.

5. Custodian - a Duke Energy employee, joint venture participant, partner, contractor, vendor, agent or third party, or other authorized person who is responsible for support or maintenance of one or more component of an information system. Custodians are Subject Matter Experts (SME's) in their particular areas, and have been delegated responsibilities based on agreements with Information Owners or IT Asset Managers.

6. Information User - members of the Duke Energy workforce who use information asset(s) during the course of their work. Information Users are responsible for using information assets responsibly and only for authorized purposes. Information Users must take precautions to prevent the unauthorized disclosure of company information and must report suspected unauthorized disclosures or violations.

IT 5002.4 Acceptable Use of Assets

Information assets that the company provides the workforce must be used to facilitate and support company business objectives. Appropriate use of these assets is the responsibility of all members of the workforce.

IT 5002.4.1 Software

Each member of the workforce must abide by software licensing agreements in accordance with the "IT 2010 Software License Management Policy". The use of software on company information systems must be approved by management, see "IT 5007 Information Systems Acquisition, Development, and Maintenance", prior to installation. Any software that is loaded outside normal IT processes, i.e., workstation images, DAE-loaded, or other Business Unit software delivery processes; or that is not properly licensed or approved is subject to:

a) *Non-support, which may include re-imaging of the workstation (and removal of the software and potential* loss of local information) to restore working functions.

b) In the case of security issues, any restrictions, up to and including immediate and unannounced removal.

Additionally parties responsible for loading and/or using improperly-licensed software may be subject to disciplinary actions up to and including termination of employment or contract. For additional information, refer to "IT 5003.3.2 Disciplinary Process".

IT 5002.4.1.1 Monitoring or Remote Control Software

The use of monitoring or remote control software must be reviewed by Corporate IT Strategy and Compliance and is restricted to registered departments or groups.

Exhibit IT-4

IT 5002 – Asset Management

IT 5002.4.2 E-mail

E-mail communications generated on or received by Duke Energy systems remain the property of the company. Any E-mail messages sent, posted, or received are considered Duke Energy property and are subject to monitoring. Authorized personnel within the company have the right to access, review, copy, or delete, with out prior notification, any message or attachment within the E-mail system. General information about the appropriate use of e-mail can be found in "IT 4010 Appropriate Use of Email". Specific information about the security of email is described as follows:

Individual Accounts – e-mail accounts that are established for individual use. Each individual is accountable for the e-mail sent from their account. Sending messages from someone else's e-mail account, except under properly delegated arrangements, is prohibited.

Confidentiality and Integrity – Information sent via e-mail over the Internet with a security classification of "Confidential" must be encrypted and information with has a security classification of "Internal Use Only" must be reviewed by the Information Owner to determine the appropriate controls to ensure information confidentiality and integrity. The IT Security Methods gadget located on the Portal provides guidelines for encrypting e-mail information.

Auto-Forward – functionality that automatically forwards email to a Non-Duke address is not allowed.

Personal E-mail Accounts – personal accounts such as Hotmail and AOL must not be accessed when connected to a Duke Energy network.

Scanning – Inbound and outbound e-mails must be routed through the Duke Energy e-mail scanning infrastructure.

IT 5002.4.3 Logon Scripts

The use of auto-logon scripts is not allowed for any account type.

IT 5002.4.4 Hardware

All equipment, or hardware, provided by Duke Energy is the property of Duke Energy. The issuance and use of equipment must be authorized by management. Each member of the workforce must abide by the "IT 2000 Information Technology Asset Management" and "IT 5004 Physical and Environmental Security" policies.

IT 5002.4.4.1 Non-Duke Equipment

Non-Duke equipment is not allowed to be remotely or locally (direct or wireless) connected, to any Duke Energy information asset. If a specific business need arises where a vendor, contractor or consultant requires an Internet connection an isolated connection can be provided. For additional information, see "IT 5006.4 Network Access Control".

Note: This does not preclude the use of Non-Duke Equipment to access Portal or remote web-based services, i.e., email services.

IT 5002.4.5 Internet

Access to the Internet from Duke Energy networks is only allowed when using Duke Energy approved hardware and software. Users are responsible for maintaining the security of information sent over the Internet as determined by the information security classification.

Exhibit IT-4

IT 5002 – Asset Management

IT 5002.4.5.1 Disclosure

Information disclosed using the Internet (discussion groups, company web sites) must be in accordance with the Code of Business Ethics.

IT 5002.4.5.2 Inappropriate Activities

Internet activity is considered public and users must conduct their activity in accordance with company policies and standards and the Code of Business Ethics. Internet activity may be monitored for inappropriate use and violations are subject to disciplinary action.

IT 5002.5 Security Classification

Security Classification is used to establish the controls necessary for protecting information assets and provides for a common understanding of the information asset's value in terms of confidentially, integrity and accessibility.

IT 5002.5.1 Classification Guidelines

A Security Classification must be assigned to all information assets within a system to ensure the information is appropriately secured. The Information System Owner is responsible to ensure a security classification is assigned, the necessary controls are applied, and that both the classification and security controls are maintained.

The Information System classification is determined by the classification of the information that is being stored, processed or transmitted within the information system. It may also be determined based on the service the system provides, such as security camera or badge systems. Information Owners and Information System Owners must provide the Information Technology Manager with the appropriate system classification rating.

a) Information Classification - the Information Owner must initially classify the information based on the information's attributes and in compliance with Duke Energy's Records Management Standard. If one of the information attributes merits a higher classification than the rest, then the entire information is subject to the higher security classification. The Information Owner must review the information classification annually and whenever there is a change to an information attribute.

b) Information Technology Classification - the Information Technology Manager must ensure the same classification is assigned to the information technology assets as assigned to the associated information or system service. Shared assets or services must be classified based on the highest classification level assigned to an individual component within the system.

IT 5002.5.2 Security Classifications

Information must be assigned to one of the following Security Classifications

a) Public - Information designed for the distribution both to Duke internally and to the public. This information requires minimal security protection and is easily reproduced, i.e., marketing brochures.

b) Internal - Information primarily designed for Duke's internal use that can also be disclosed to external parties with minimal adverse consequences to the enterprise. Internal information includes general business-related information that does not fall under higher classifications, i.e., procedure manuals.

c) Confidential – Information available internally, and only on a 'need to know' basis. Confidential information has a very limited distribution to specific individuals, under strict security controls. Confidential information

Exhibit IT-4

pertains to customers, employees, financial planning, strategic planning, etc. It is intended for use only by specific groups of employee, i.e., payroll information, financial forecasts, security files, etc. This information is highly sensitive and is essential for the company to achieve its mission and meet its legal requirements.

Note: Confidential is the default classification for all information unless otherwise specified and approved by the designated asset owner.

5002.5.2.1 Potential impact of Unauthorized Disclosure of Information

Public – none, with the exception of public information stored on externally accessible systems. Disclosure would not benefit a competitor, harm Duke Energy, or breach any confidentiality.

Internal - would have an adverse impact on Duke's mission, finances, operations, or public image. The impact would place Duke at a significant competitive disadvantage, expose them to significant financial loss, cause a breach of fiduciary or regulatory obligations, damage Duke's public credibility, or cause other serious damage to Duke's customers or employees.

Confidential – would have a significant impact on Duke's mission, finances, operations or public image. The result would potentially cause irreparable harm and prove difficult to remedy. The results would be a material loss of revenues, profits, or other materially adverse financial impacts, severe public embarrassment, or severe damage to Duke's competitive position.

IT 5002.6 Information Asset Controls

Information assets must be protected at a level commensurate with the security classification. Confidentiality or sensitivity of an information asset must be a consideration when applying controls. Information security consists of physical and logical controls. For more information, see "IT 5004 Physical and Environmental Security" and "IT 5006 Access Controls".

Exhibit IT-4

Duke Energy.

Duke Energy Standard

IT 5003 – Human Resources Security

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 security requirements for managing employees, contractors, and third parties that use, have access to, or have custody of Duke Energy's information or information assets.

IT 5003.1 Prior to Employment

Duke Energy is committed to ensuring that employees, contractors, and third parties have been properly screened prior to performing tasks or being granted access to information assets.

IT 5003.1.1 Roles and Responsibilities

Each member of the Duke Energy workforce is bound by the confidentiality requirements defined in CoBE, for safeguarding company information assets and for compliance with the IT 5000 Series.

IT 5003.1.2 Screening

Screening of individuals will be conducted in accordance with Human Resources (HR) policy "HR 5001 Screening Standard: Prior to Employment". Managers of departments that deal with confidential information assets are responsible for stating in the corresponding job description that the position requires access to confidential assets. Access must not be granted until the company background check process is complete.

IT 5003.1.3 Terms and Conditions of Employment

Terms and Conditions of Employment are defined by HR policies.

IT 5003.2 During Employment

Information security is an ongoing process and requires the workforce to be security focused. Members of the workforce are responsible for understanding the IT 5000 Series and maintaining current knowledge to effectively comply with information security.

IT 5003.2.1 Management Responsibilities

Management must promote information security as a required part of conducting business and must ensure that the workforce implements information security practices as defined in the IT 5000 Series.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

IT 5003.2.2 Disciplinary Process

Security events and company policy violations are subject to investigation, the results of which will be reported to management. Appropriate disciplinary action, up to and including termination, may result. For details see "HR 3000 Corrective Action Policy"

IT 5003.3 Information Security Awareness and Training

Business Unit management is responsible for promoting constant security awareness to all members of the workforce. Corporate IT Strategy and Compliance is responsible for defining the overall security awareness program and supporting the efforts of Business Units.

IT 5003.3.1 Compulsory Training

Business Unit management must ensure that members of the workforce complete the Security Awareness Computer Based Training (CBT) at time of employment and annually thereafter. This training is available on the company portal. Additional training may vary according to needs and can be customized by Corporate IT Strategy and Compliance and/or Business Units.

IT 5003.3.2 Information Technology Employees

Information Technology employees with responsibility for developing, maintaining or administering applications or information systems may receive ongoing training relevant to their area of responsibility through periodic security awareness briefings as deemed necessary by the employee's management or Corporate IT Strategy and Compliance.

IT 5003.3.3 Contractors and Third Parties

Contractors and third parties who access company information systems must complete the Security Awareness Training and provide acknowledgment of completion. In addition they must be provided access and directed to the Corporate IT Strategy and Compliance website: "Policy, Standards, and Procedures" section, or be provided a copy of the applicable IT 5000 Series documents.

IT 5003.4 Termination or Change of Employment

Voluntary and involuntary terminations or change in employment status within Duke Energy will be conducted according to HR policies.

IT 5003.4.1 Return of Assets

Company information assets must be collected by the department manager during the exit process.

IT 5003.4.2 Removal of Access Rights

Access to information assets by individuals will only be granted in support of specific business needs. When an individual no longer needs access, the access rights must be disabled. The following conditions apply:

Transfer - within seven calendar days of the effective date of a user transfer, the manager of the department the individual is transferring out of must ensure information system access that is no longer required is removed.

Exhibit IT-4

IT 5003 – Human Resources Security

Extensions beyond the seven day limit must be approved by the Information Owner or IT Technology Manager. The managers of departments that are effected by regulatory requirements, such as Affiliate Rules, are responsible for ensuring that Affiliate Rules are followed.

Voluntary Termination - within one business day of the effective date of a user termination, the manager of the department in which the individual was a member must ensure that information systems accounts are disabled.

Involuntary Termination - immediately upon termination, the manager of the department in which the individual was a member must ensure that their all information system access rights are disabled.

Exhibit IT-4

Duke Energy.

Duke Energy Standard

IT 5004 – Physical and Environmental Security

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 defines the physical and environmental security requirements for Duke Energy facilities containing information assets, and facilities used in support of information system operations.

IT 5004.1 Secure Areas

Physical access to Duke Energy facilities and their supporting infrastructure (communications, power, and environmental) must be controlled to prevent and detect unauthorized entry into these areas. Physical security controls must be proportionate with the value of the information assets in the facility.

IT 5004.1.1 Physical Security Perimeter

The physical security perimeter defines the physical boundaries of the secure areas protecting Duke Energy information assets. Processing facilities or buildings that house information assets must be protected by physical security controls that prevent unauthorized individuals from gaining access. Processing facilities or buildings that house information assets must have an individual responsible for the physical access and environmental controls. Business Units must ensure that physical perimeters are defined and documented. Facilities affected by regulatory requirements, such as Affiliate Rules, may require additional security perimeters.

IT 5004.1.2 Physical Entry Controls

Corporate Security must be consulted prior to implementing physical security measures.

IT 5004.1.2.1 General Office Buildings

Each general office building is unique in its use and content. Corporate Security must perform a vulnerability assessment to determine mitigation measures.

IT 5004.1.2.2 Processing Facilities

Processing facilities generally require more stringent access controls than office buildings. A processing facility must have an assigned Facility Manager who is responsible for ensuring that:

a) Physical access is limited to authorized personnel.

b) Access authorization to these facilities will only be granted in support of business needs.

c) Access authorization is reviewed annually and revoked immediately if no longer needed.

Exhibit IT-4

The following table defines the minimum levels of access controls, monitoring, and security logs required for different types of processing facilities.

Area to Protect	Access Controls	Monitoring	Security Logging
Data center	Card key access Equipped with doors that automatically and immediately close after they have been opened and an audible alarm must sound in a monitored area when the door has been kept open beyond a reasonable period of time	By at least one of these: Video surveillance of personnel entering the area (monitored 24 x 7) Observation of personnel entering the area by 24 x 7 staff	By at least one of these (time in/time out): Card Key log Personnel logging (recorded log with account validation by staff)
Server room, telecommunication room, telecommunication closets	Locked doors with a key management process Always secured		

Table 5-1: Processing Facility Controls

IT 5004.1.3 Securing Offices, Rooms, and Facilities

Business Units are accountable for securing office space proportional to the value of the information asset. Examples of acceptable physical security methods are cable lock, locked room, or desk.

IT 5004.1.4 Protecting Against External and Environmental Threats

Information assets must be protected from external and environmental threats such as theft, tampering, fire, water, or acts of nature. Appropriate controls must be established to secure information assets to prevent theft during or after external or environmental events.

IT 5004.1.5 Working in Secure Areas

Secure areas are those that require authorization for access. Authorized personnel must not allow unknown or unauthorized individuals into these areas. Authorized personnel are responsible for ensuring they are not tailgated by unauthorized personnel. Company security (security guards at the location) must be notified of unauthorized personnel in a secured area.

IT 5004.2 Equipment Security

Security controls must be applied to prevent the loss, damage, theft, compromise, and interruptions to Duke Energy's activities. The following conditions apply to equipment:

Exhibit IT-4

IT 5004.2.1 Equipment Location and Protection

Measures must be taken to minimize the risks of a physical or environmental event occurring or spreading from adjoining locations. Steps must be taken to ensure that location specific threats (i.e., temperature, fire, explosive, smoke, theft, water, water supply, dust, vibration, chemical effects, electromagnetic interference, electric supply interruption, communications interference, vandalism, seismic activity, and meteorological threats) are properly assessed and accounted for when determining where to locate information assets.

IT 5004.2.1.1 Mobile Equipment

Portable devices 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.

IT 5004.2.2 Secure Disposal or Re-Use of Equipment

Information assets that are to be disposed of or re-used must be cleansed to ensure Duke Energy information and identifying labels are removed. Disposal or re-use cleansing must occur when an information asset:

a) Is sold or surplused

b) Is released as part of a divestiture, unless legal obligations require otherwise.

c) Has reached end of lease

d) Is a removable component, such as disk drive or other media, being retired

e) When an information asset is transferred internally.

IT 5004.2.2.1 Logical Cleansing

Storage media containing information must be cleansed through a media cleansing tool (for re-usable hard drives), degaussing tool (for magnetic media, i.e., floppy disks or tapes), or physical destruction (for other media, i.e., compact disks or NVRAM). Only use Corporate IT Strategy and Compliance approved cleansing tools and procedures.

IT 5004.2.2.2 Physical cleansing

Remove identifiable information, such as the Duke Energy asset tags.

Exhibit IT-4

Duke Energy.

Duke Energy Standard

IT 5005 – Communications and Operations 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 requirements for acceptable and secure operation of information assets.

5005.1 Operational Procedures & Responsibilities

Business Units must maintain operational procedures for secure operations of information assets. These procedures must be in accordance with enterprise standards, must not be in conflict with enterprise procedures, and must include appropriate controls for configuration management, change management, and system backup.

5005.1.1 Configuration Management

The information technologies incorporated at Duke must be configured using a consistent build process. The process must provide for the development, test, approval, and maintenance of a standard configuration for each technology. Corporate IT Strategy and Compliance must review all new or modified security related standard configuration settings prior to implementation to ensure minimum security baselines have been met. Information Technology Managers must establish and maintain the overall standard configuration build documentation, Corporate IT Strategy and Compliance must establish and maintain the baseline security configuration settings. Protocols, services or applications (such as Telnet, FTP, and HTTP) that are not defined in the standard configuration are not allowed.

5005.1.2 Change Management

Changes to Information assets must be managed pursuant to "IT 3010 Technology Change Control". Business Units are responsible for ensuring that change management processes captures the history of all changes and maintain the change history as determined by company retention standards

Changes that impact security settings must be reported to Corporate IT Strategy and Compliance before implementation.

5005.1.3 System Back-up

Each Business Unit must maintain an operational strategy and associated procedures for back-up and recovery of information systems. For more information, see "IT 5009 Business Continuity Management".

Exhibit IT-4

5005.2 Third Party Delivery Management

Controls must be in place to ensure that third party contracts provide for the protection of Duke Energy's information assets and that vendors comply with Duke Energy's security requirements.

IT 5005.2.1 Service Delivery

Corporate IT Strategy and Compliance must be included in the third party contract review process. Third party contracts must contain explicit language addressing security performance expectations, performance metrics, Duke's right to review for compliance, and consequences for failure to perform. Corporate IT Strategy and Compliance must be part of the contract review process prior to signing.

IT 5005.2.1.1 Application Service Providers

Prior to contracting Application Service Provider (ASP) services, the ASP's information security architecture and practices must be evaluated by Corporate IT Strategy and Compliance. Any issues or concerns need to be reviewed by the ASP Review Board. For additional requirements, see "IT 5005.8 Exchange of Information".

5005.2.1.2 Third Party Connections

Third party connections expose the company to risks that cannot be managed through normal controls. Therefore, each connection request must be assessed to determine the level of controls needed for a secure connection. Third party connections must be authorized and registered with Corporate IT Strategy and Compliance and reviewed annually, see "IT 5005-01 Third Party Connection Procedure" for guidance. At a minimum, third party remote connections must have a Duke Energy Sponsor who is responsible for:

a) Coordinating with internal departments on behalf of the third party.

b) Ensuring the following controls are enforced:

   - The access must be disabled when not in use and only select Duke Energy employees can authorize the access to be enabled.
   - Access cannot be authorized and also enabled by the same person. One individual must authorize the access, and another individual must enable it.
   - The control point must always be at the destination resource (Vendor ID on the server).

c) If Non-Duke Equipment is used as the remote device it must:

   - Be part of a configuration management program that ensures active and current virus protection is running on all client. machines and operating systems have up to date patches and/or maintenance levels as determined by the operating system vendor recommendations.
   - Not have concurrent connections to other networks by any means while connected to Duke Network. This includes, but is not limited to, dial-up, wireless, or direct cabling.
   - Not have reconnaissance software used for sniffing, monitoring or other similar activities running while connected to a Duke Energy asset.
   - Not provide broadcast request services, such as DHCP.

Exhibit IT-4

IT 5005 – Communications and Operations Management

5005.2.1.2.1 Third Party VPN

Third party VPN connection requires a signed Network Access Agreement which details the terms and conditions under which the Third party VPN connection is permitted. The connection point must terminate in the perimeter network on a device configured for handling VPN traffic.

5005.2.1.2.2 Third Party Dial-In

Third party dial-in connections to Duke Energy networks are only allowed through the controls established through remote access services and routing controls established at the firewall.

Direct modem connections that allow approved third parties access to an individual information asset for support must only be active during the support session. When the session is complete, the line or modem must be disabled.

5005.3 Protection Against Malicious & Mobile Code

Controls must be established to protect Duke Energy Information assets against loss of availability and unauthorized modification or destruction caused by malicious software. Malicious software refers to any software, which causes destruction, damage, or unauthorized changes to software or information.

5005.3.1 Controls Against Malicious Code

Anti-virus software, i.e., real-time scanning, must be enabled on all Duke Energy servers, workstations, hosts, and computers. The following conditions apply:

a) Virus protection must not to be disabled or removed from Duke Energy information assets.

b) Platform-specific anti-virus software must be maintained at all times.

c) Workstations must be scanned whenever they are accessed and at least once every quarter.

d) Servers must be scanned whenever they are accessed.

e) All anti-virus software must be updated with the most recent version, as it becomes available.

f) Anti-virus software that scans incoming and outgoing e-mail and attachments must be enabled on all e-mail gateways or servers.

5005.4 Network Security Management

Network security management ensures that Duke Energy networks are authorized and effectively managed. For additional information about Network Access Controls, or connecting to the Duke Energy common network, see "IT 7007.4, Network Access Controls".

5005.4.1 Authorization

Networks must have a defined business need and must be authorized by an Information Sponsor.

Exhibit IT-4

5005.4.2 Configuration

All networks (test, development, production, wired, and wireless) must be configured and managed by authorized departments that are on record with Corporate IT Strategy and Compliance. All changes to network configurations must be managed in accordance with Section 5005.1.2 Change Management.

5005.5 Media Handling

Media containing information must be securely managed in order to prevent unauthorized access, modification, or removal.

5005.5.1 Management of Removable Media

Removable media i.e., diskettes, CDs, USB portable storage devices must not be left unattended and must be physically secured at all times. Media containing information with a security classification of confidential must be stored in a locked container, i.e., desk or file cabinet, or stored in a room designated for the secure storage of information not in use. If the information is encrypted, only those encryption technologies approved by Corporate IT Strategy and Compliance are acceptable for use.

5005.5.2 Disposal of Media

Media containing information with a security classification of confidential must be disposed of through degaussing for magnetic media, i.e., floppy disks or tapes, or physical destruction for other media, i.e., compact disks or NVRAM. Media containing information with a security classification of Internal Use Only must be evaluated to determine if degaussing is required. At a minimum all media must be reformatted prior to disposal.

5005.5.3 Information Handling Procedures

Areas that are used for information storage, i.e., datacenters, magnet tape storage faculties, etc. must be restricted to personnel whose job responsibilities require such access.

5005.6 Exchange of Information

Information security controls must be implemented to ensure appropriate use and protection of information exchanged outside of Duke Energy. These controls must take into consideration that the information will be traveling through Non-Duke networks and may be exposed to external sources that may not provide the same level of security as Duke Energy.

5005.6.1 Information Exchange Policies and Procedures

Information exchanged outside of Duke Energy must be evaluated to ensure the appropriate level of security is maintained. Corporate IT Strategy and Compliance can provide assistance in determining the required level of security. Additional guidance regarding information exchange using the Internet and email can be found in "IT 5002 Asset Management".

Exhibit IT-4

IT 5005 – Communications and Operations Management

5005.6.2 Exchange Agreements

Agreements, or contracts, that involve the exchange of information must contain language that specifies the expectations for securing all information. The language must:

a) State that information with a security classification above Public, transmitted to and entrusted in their care, will not be disclosed to unauthorized parties.

b) Provide Duke Energy with rights to examine and test the security architecture, infrastructure, and practices.

c) Include provisions for the return or destruction of information.

d) Define the penalties should a breach in security occur as a result of negligence.

5005.7 Electronic Commerce Services

Information security controls must be implemented that ensure the appropriate use and protection of Duke Energy electronic commerce services. These controls must take into consideration the availability and integrity of information traveling through different internal and external networks.

5005.7.1 DMZ (Demilitarized Zone)

DMZ architectural design must be approved by Corporate IT Strategy and Compliance. Modifications are subject to review and approval. At a minimum, DMZ architecture must consist of network devices (routers and firewalls) that separate network segments or tiers. The following is required for all DMZs:

a) Communications between the DMZ and the internal network must be restricted to the necessary protocols only and must be approved by Corporate IT Strategy and Compliance.
b) A single protocol is not allowed to cross both an external and an internal DMZ network boundary, i.e., a firewall.
c) DMZ-based devices must be vigilantly maintained, i.e., "patched".
d) Intrusion detection and other protocol/content filtering mechanisms (i.e., antivirus, e-mail scanners) must be leveraged to intercept hackers and malicious code before they can penetrate the internal network.
e) FTP will only be used from specified FTP servers in the DMZ and must be called from applications or components in the DMZ. Refer to "IT 5005-02 External FTP Server Configuration" for information.

5005.7.2 Electronic Commerce

Digital signatures must be used to authenticate all material transactions, for example, EDI or other document exchange with external parties communicated over public networks.

5005.7.3 On-Line Transactions

Internet connections must be encrypted prior to and during the transmission of information with a security classification above Public for Duke Energy customer and employee portals. The level of encryption must be at least 128 bits.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

IT 5005 – Communications and Operations Management

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:

Exhibit IT-4

IT 5005 – Communications and Operations Management

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

Exhibit IT-4

Duke Energy.

Duke Energy Standard

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.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

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.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

IT 5006 – Access Control

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.

Exhibit IT-4

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".

Exhibit IT-4

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

Exhibit IT-4

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.

Exhibit IT-4

Duke Energy

Duke Energy Standard

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.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

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.

Exhibit IT-4

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

Exhibit IT-4

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.

Exhibit IT-4

Duke Energy.
Duke Energy Standard

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.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

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

Exhibit IT-4

Duke Energy.

Duke Energy Standard

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.

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

Duke Energy.

Duke Energy Standard

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".

Duke Energy Proprietary and Confidential: Internal Use Only.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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.

Exhibit IT-4

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

Duke Energy SM

SCADA Cyber Security Policy and Standards

IT 6000 SERIES

PROVISIONAL EDITION

March 31, 2006

Exhibit IT-5

Duke Energy Policy Statement

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.)

The IT 6000 Series documents are the property of Duke Energy. Reproduction, distribution, or unauthorized use is strictly prohibited without the expressed written consent of Duke Energy. Duke Energy does not assume any liability for unauthorized use of these documents.

© Copyright 2006 Duke Energy Corporation. All rights reserved.

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

Exhibit IT-5

IT 6000 – SCADA Cyber Security Policy

Table of Contents

© Copyright 2006 Duke Energy Corporation. All rights reserved.

© Copyright 2006 Duke Energy Corporation. All rights reserved.

Exhibit IT-5

Duke Energy.

Duke Energy Policy Statement

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.

Exhibit IT-5

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

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-5

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.

IT 6000 – SCADA Cyber Security Policy

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".

Exhibit IT-5

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.

Exhibit IT-5

Duke Energy.

Duke Energy SCADA Cyber Security Standard

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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

Exhibit IT-5

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.

Exhibit IT-5

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 Proprietary and Confidential: Internal use only.

Exhibit IT-5

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",

Exhibit IT-5

IT 6003 – Compliance, Monitoring, and Response

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

Exhibit IT-5

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.

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.

Exhibit IT-5

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".

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

Exhibit IT-5

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".

Exhibit IT-5

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 Intemet. 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.

Exhibit IT-5

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.

Exhibit IT-5

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.

Duke Energy Proprietary and Confidential: Internal use only.

Exhibit IT-5

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)

Exhibit IT-5

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. <u>Remote Access to SCADA Hosts</u> – 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.

Exhibit IT-5

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.

Exhibit IT-5

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

Exhibit IT-5

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

Exhibit IT-5

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".

Exhibit IT-5

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).

Exhibit IT-5

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. <u>Card Key</u> - 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. <u>Special Locks</u> - These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

Exhibit IT-5

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.

Exhibit IT-5

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

Exhibit IT-5

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

Exhibit IT-5

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".

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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 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

Exhibit IT-5

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

Exhibit IT-5

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;

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".

The following images were scanned as received

Exhibit IT-5

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

Exhibit IT-5

IT 6008 – Incident Reporting

"IT 5002.5.2 Security Classifications".

Exhibit IT-5

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.

Exhibit IT-5

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".

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

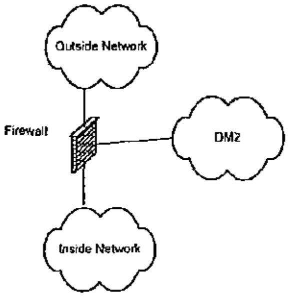


Figure 1

Exhibit IT-5

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.

Exhibit IT-5

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.

Exhibit IT-5

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.)

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.

Exhibit IT-5

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.

Exhibit IT-5

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.

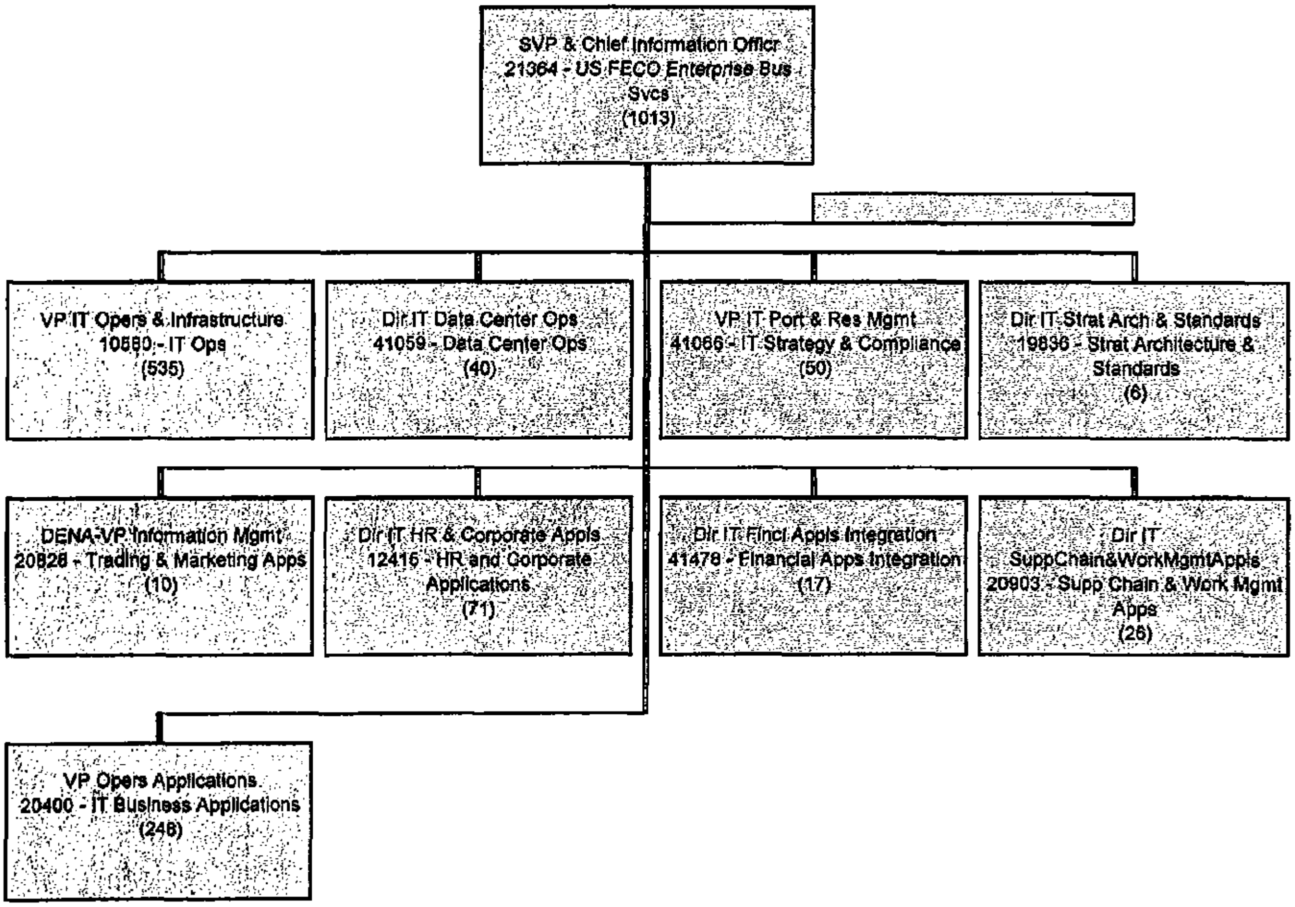
Ǝxhibit IT-5

Glossary of Terms

Exhibit IT-6

DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

Senior Vice President & Chief Information Officer



SVP & Chief Information Officr
21364 - US FECO Enterprise Bus Svcs
(1013)

VP IT Opers & Infrastructure
10580 - IT Ops
(535)

Dir IT Data Center Ops
41059 - Data Center Ops
(40)

VP IT Port & Res Mgmt
41066 - IT Strategy & Compliance
(50)

Dir IT Strat Arch & Standards
19836 - Strat Architecture & Standards
(6)

DENA-VP Information Mgmt
20828 - Trading & Marketing Apps
(10)

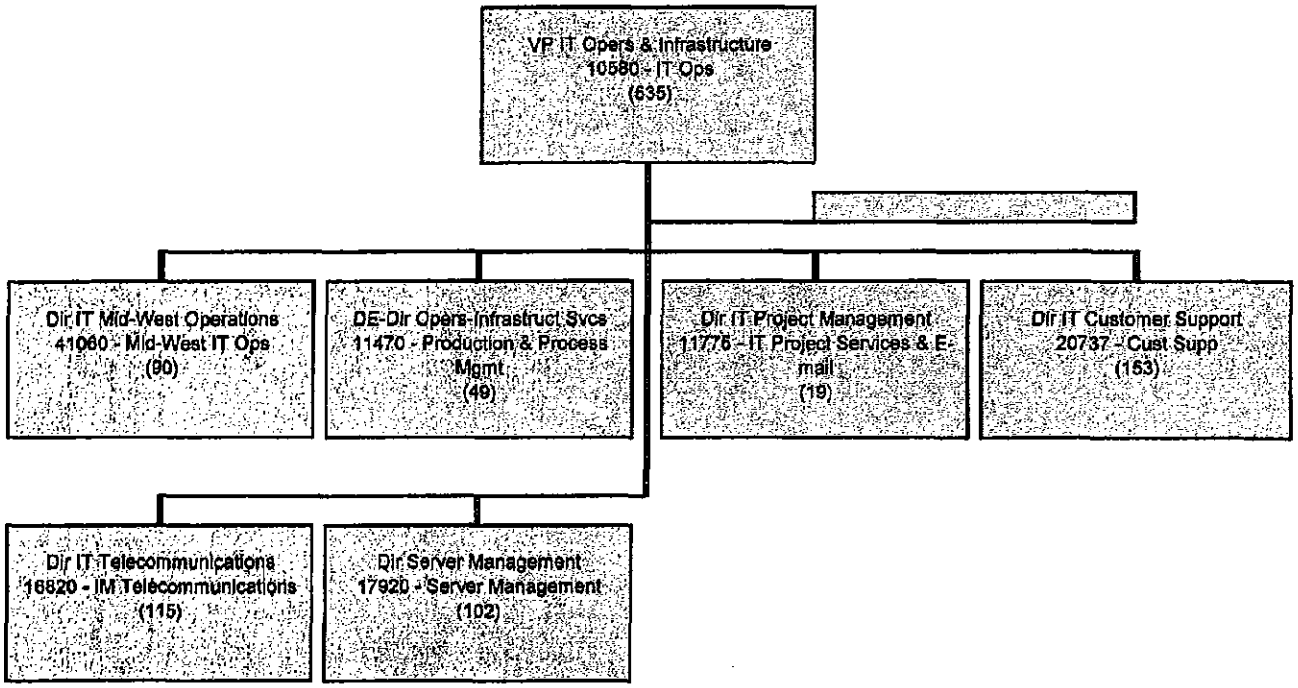
Dir IT HR & Corporate Appls
12416 - HR and Corporate Applications
(71)

Dir IT Fincl Appls Integration
41478 - Financial Apps Integration
(17)

Dir IT SuppChain&WorkMgmtAppls
20903 - Supp Chain & Work Mgmt Apps
(26)

VP Opers Applications
20400 - IT Business Applications
(246)

Vice President IT Operations & Infrastructure



VP IT Opers & Infrastructure
10580 - IT Ops
(635)

Dir IT Mid-West Operations
41060 - Mid-West IT Ops
(90)

DE-Dir Opers-Infrastruct Svcs
11470 - Production & Process Mgmt
(49)

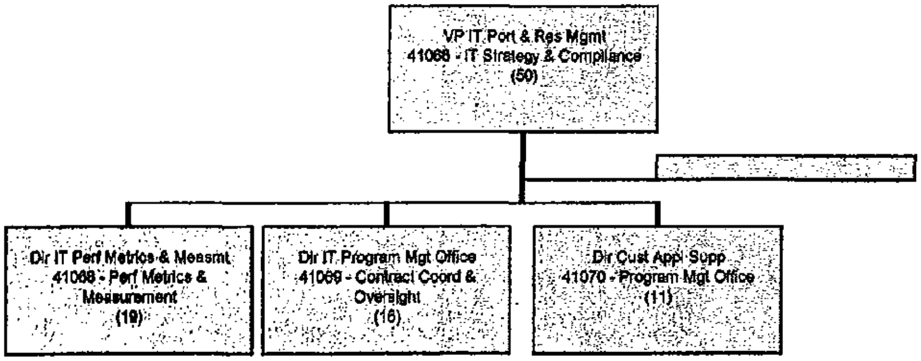
Dir IT Project Management
11776 - IT Project Services & E-mail
(19)

Dir IT Customer Support
20737 - Cust Supp
(153)

Dir IT Telecommunications
16820 - IM Telecommunications
(115)

Dir Server Management
17920 - Server Management
(102)

Vice President IT Portfolio & Resource Management



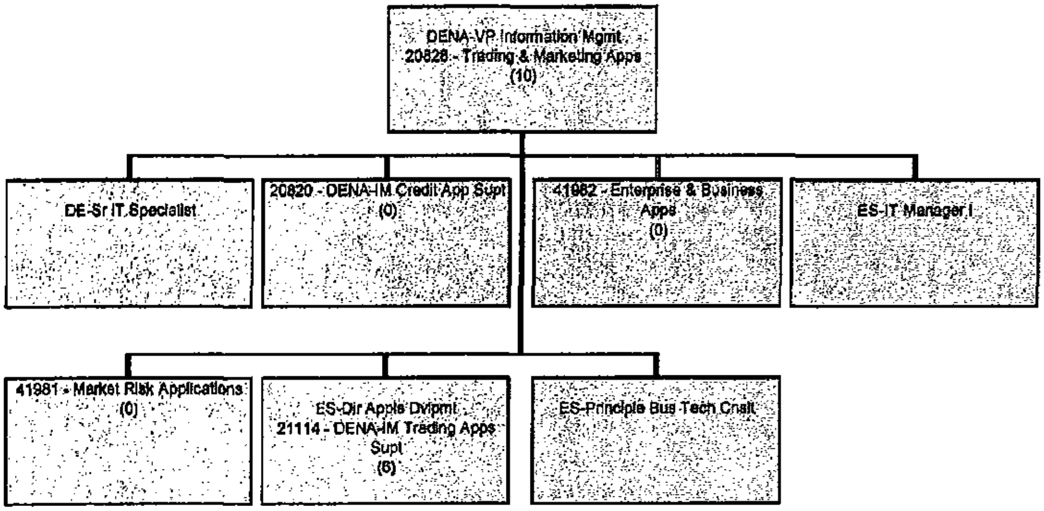
VP IT Port & Res Mgmt
41068 - IT Strategy & Compliance
(50)

Dir IT Perf Metrics & Measmt
41068 - Perf Metrics & Measurement
(19)

Dir IT Program Mgt Office
41069 - Contract Coord & Oversight
(16)

Dir Cust Appl Supp
41070 - Program Mgt Office
(11)

Vice President Information Management- DENA



DENA-VP Information Mgmt
20828 - Trading & Marketing Apps
(10)

DE-Sr IT Specialist

20820 - DENA-IM Credit App Supt
(0)

41982 - Enterprise & Business Apps
(0)

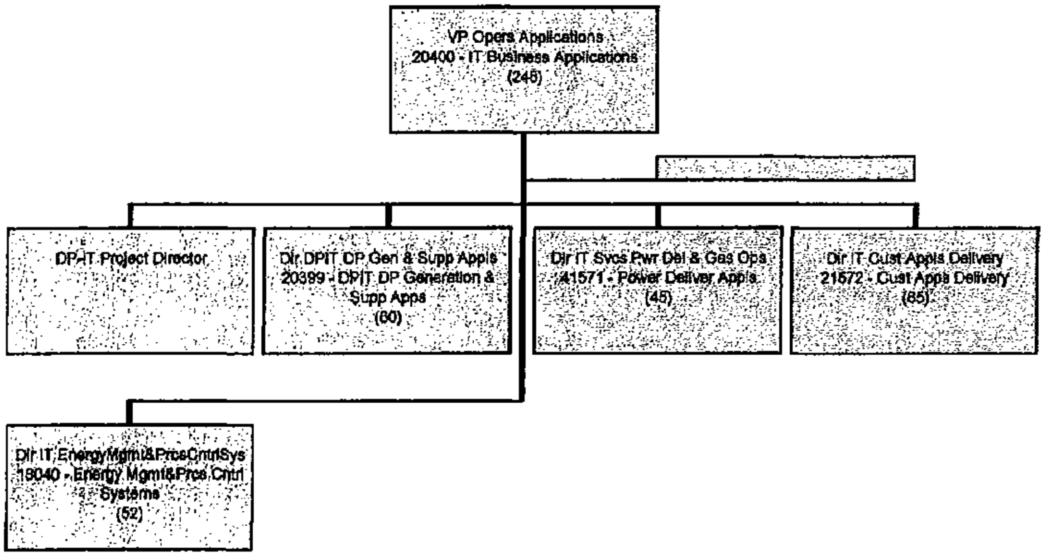
ES-IT Manager I

41981 - Market Risk Applications
(0)

ES-Dir Appls Dvlpmt
21114 - DENA-IM Trading Apps Supt
(6)

ES-Principle Bus Tech Cnslt

Vice President Operations Applications



VP Opers Applications
20400 - IT Business Applications
(246)

DP-IT Project Director

Dir DPIT DP Gen & Supp Appls
20399 - DPIT DP Generation & Supp Apps
(60)

Dir IT Svcs Pwr Del & Gas Ops
41571 - Power Deliver Appls
(45)

Dir IT Cust Appls Delivery
21572 - Cust Apps Delivery
(65)

Dir IT EnergyMgmt&PrcsCntrlSys
18040 - Energy Mgmt&Prcs Cntrl Systems
(52)

Schedule S-4.2

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.

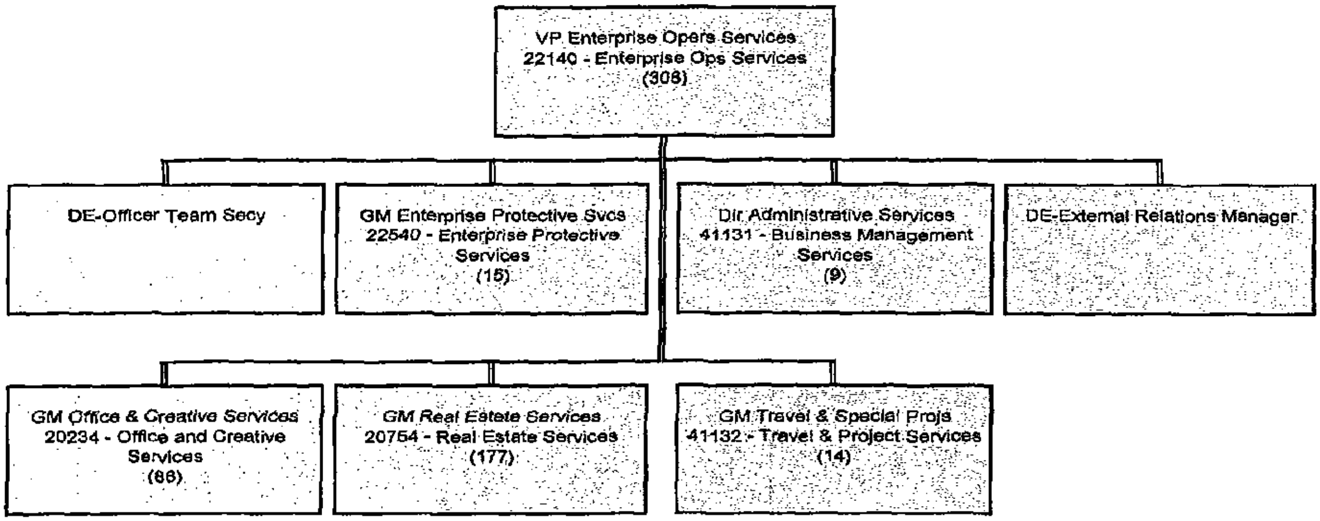
Specific projects or actions that have been identified as additional goals are monitored at functional staff meetings and Leadership Team meetings to assess status and results. Any results that are subjective in nature must be approved by the Vice President of EOS. Additionally customer satisfaction 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.

Exhibit EOS-1

DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

Vice President Enterprise Operations Services



VP Enterprise Opers Services
22140 - Enterprise Ops Services
(308)

DE-Officer Team Secy

GM Enterprise Protective Svcs
22540 - Enterprise Protective Services
(15)

Dir Administrative Services
41131 - Business Management Services
(9)

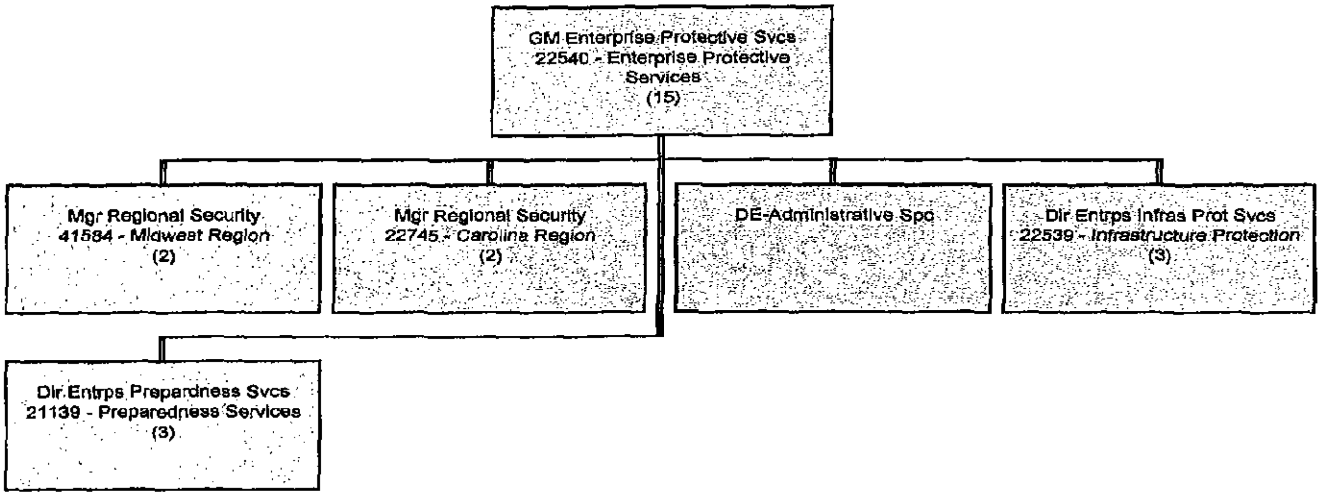
DE-External Relations Manager

GM Office & Creative Services
20234 - Office and Creative Services
(66)

GM Real Estate Services
20754 - Real Estate Services
(177)

GM Travel & Special Projs
41132 - Travel & Project Services
(14)

General Manager Enterprise Protective Services



GM Enterprise Protective Svcs
22540 - Enterprise Protective Services
(15)

Mgr Regional Security
41584 - Midwest Region
(2)

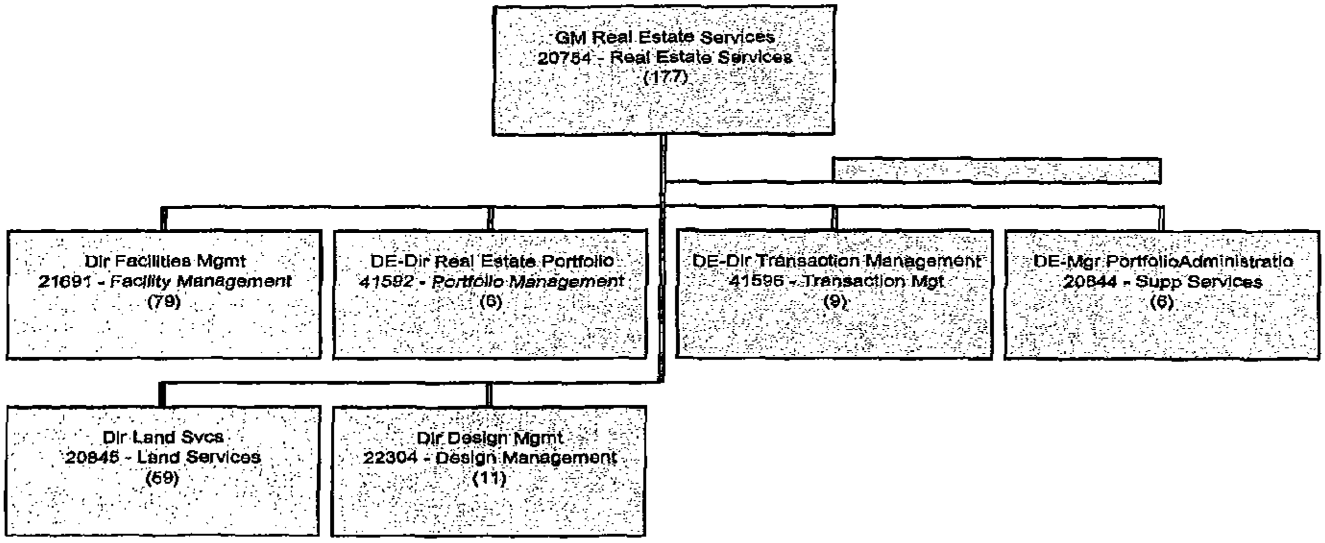
Mgr Regional Security
22745 - Carolina Region
(2)

DE-Administrative Spc

Dir Entrps Infras Prot Svcs
22539 - Infrastructure Protection
(3)

Dir Entrps Prepardness Svcs
21139 - Preparedness Services
(3)

General Manager Real Estate Services



GM Real Estate Services
20754 - Real Estate Services
(177)

Dir Facilities Mgmt
21691 - Facility Management
(79)

DE-Dir Real Estate Portfolio
41592 - Portfolio Management
(6)

DE-Dir Transaction Management
41596 - Transaction Mgt
(9)

DE-Mgr PortfolioAdministratio
20844 - Supp Services
(6)

Dir Land Svcs
20845 - Land Services
(59)

Dir Design Mgmt
22304 - Design Management
(11)

Exhibit EOS-2

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

Exhibit EOS-2

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.

Exhibit EOS-2.1

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.

Exhibit EOS-2.1

Records Management Standard

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

Exhibit EOS-3

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.

Exhibit EOS-3

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.

Schedule S-4.2

DUKE ENERGY
SUMMARY OF MANAGEMENT POLICIES, PRACTICES AND ORGANIZATION
HUMAN RESOURCE DEPARTMENT
SFR Reference: Chapter II(B)(9)(f)(i,ii,iii,iv,v)

I. Policy and Goal Setting

The Human Resources Department (Department) assists the Company in achieving its business goals by facilitating the acquisition, development and maintenance of an efficient and productive workforce.

The Department supports the corporate policies and objectives as described in the Policies section of the Employee Portal through the related Working Environment Policy Manual and Duke Energy procedures and practices.

The Group Executive and Chief Administrative Officer who has overall responsibility for Human Resources with input from the Vice President-Corporate Human Resources and Vice President-HR Business Support participate in strategic planning meetings with corporate senior management. As a result of these meetings, the HR executive team develops goals and objectives for Human Resources in support of the overall business plans of the Corporation and individual business units. The goals are developed in partnership with and reviewed with Company officers.

The Human Resources leadership group then develops goals and objectives that support those developed in partnership with Company senior management. Departmental and individual goals are evaluated and reviewed annually as a part of the performance management process, which is used to determine annual salary adjustments.

The Human Resource Department's sub-departments also engage in policy and goal-setting, as follows:

Staffing and Recruiting - It is the policy of Staffing and Recruiting to select and employ the best qualified available candidate to meet the specific competency requirements of a particular job vacancy and the Company's general qualifications, while operating within a balanced workforce initiative and company compensation guidelines as well as the legal requirements of local, state and federal agencies. Methods for selection and placement of employees (i.e., qualifications and assessment methods) are set by involving line department management. In times of downsizing and restructuring, this division is responsible for the employee transition pool and its activities.

Organizational Development- It is the policy of Organizational Development to consult with executive management and line departments to design and develop non-technical training and organizational interventions which develop the competencies of the individuals and teams within the Company. Additionally, it is the policy of the department to facilitate the implementation of Career Development processes in departments and assist individuals in identifying personal career development plans.

Labor Relations- It is the policy of the Labor Relations Department to foster positive relationships with all unions without eroding the Company's ability to manage. It is the department's goal to promote and improve the relations between the Company and its employees who are represented by unions by honoring the spirit, as well as the terms and conditions, of the individual collective bargaining agreements while supporting management's need to adapt to changes.

Employee Relations and HR Risk Management- It is the policy of the Employee Relations area to provide consultation services to Company management and supervision to facilitate the development, retention, and consistent administration of a quality and engaged workforce for current and future workforce needs of the Company. This includes supporting strategies and processes that ensure a corporate environment that is free of bias, auditing employment practices and associated programs to ensure fair application, and investigating Equal Employment Opportunity complaints. The group coordinates our Affirmative Action Planning activities and compiles and submits information in response to government and regulatory agency requirements and requests.

Compensation & Benefits- It is the policy of this function to maintain an equitable wage and salary administration program which provides payment of fair wages and salaries competitive with those paid for similar positions in other companies and within the industry in order to retain qualified employees and attract competent applicants. The salary structure for management employees is reviewed on an annual basis with the review being guided by economic conditions, wage/salary trends, and market data. Wage rate schedules for classifications represented by collective bargaining units are made the subject of negotiations with such negotiations being guided by these same economic conditions and trends.

It is the policy of this function to design and maintain benefit programs that are competitive with the industry in order to attract and retain the employees necessary to provide safe, reliable energy to our customers.

Diversity, Inclusion and Workforce Strategies- It is the policy of Inclusion Strategies to develop, implement and/or monitor programs, procedures and practices in the area of diversity and work/life to support a respectful, inclusive and bias-free workplace.

A summary of HR policies is attached as Exhibit HR-1.

II. Strategic Planning

The Human Resources group is involved in three categories of planning activities: strategic, operations and budgeting. The Corporate HR business plan is developed by HR executive management, which includes the Group Executive and Chief Administrative Officer, the Vice President-Corporate Human Resources, and the Vice President-HR Business Support. The Vice Presidents and their direct reports develop operational plans that support and enable the HR business plan. Programs which support the HR business plan and departmental plans and goals are translated into resource requirements during the budgeting process conducted annually during the fall.

Functional leaders within HR are responsible for developing long and short range plans that support and facilitate the overall corporate objectives. Daily operational decisions or functional matters are routinely made by functional leaders. Goals and objectives which affect corporate policy or multiple departments are reviewed and discussed with the Group Executive and Chief Administrative Officer, Vice President-Corporate Human Resources and Vice President-HR Business Support, with input from senior corporate management as needed.

The Group Executive and Chief Administrative Officer attends the CEO's staff meetings. Departmental and division staff meetings are also held to communicate with Human Resource employees' progress toward company and department goals and objectives.

III. Organizational Structure

The Group Executive and Chief Administrative Officer reports to the Chairman, President and CEO. The Group Executive and Chief Administrative Officer's organization includes Human Resources, Information Technology, and Enterprise Operations Services (real estate, travel, creative services, etc.) Human Resources, divided into two areas-Corporate HR and HR Business Support, encompasses several departments including: 1) Organizational Development; 2) Compensation & Benefits; 3) Employee Relations and HR Risk Management; 4) Diversity, Inclusion and Workforce Strategies; 5) Labor Relations; 6) Staffing and Recruiting; and 7) Business Partner organizations . Each area is lead by a functional leader who reports to one of the Vice-Presidents of Human Resources.

Organizational charts for the department are attached as Exhibit HR-2.

IV. Responsibilities

The overall goal of Human Resources is to assist the Company in achieving its business goals by facilitating the acquisition, development and maintenance of an efficient and productive workforce, under conditions which foster positive employer- employee and union relations and which conform to the legal requirements imposed by local, state, and federal governments, as further described below:

Staffing and Recruiting - This division is responsible for maintaining a centralized and standardized recruitment, selection, testing and placement process to assure an adequate number of employees with the required competencies and general corporate qualifications. The department is also responsible for administering internship and co-op education programs as well as the internal job posting system. In times of downsizing and restructuring, this division is responsible for the employee transition pool and its activities.

Organizational Development - This division consults with line management to provide supervisory, management, professional and team development activities. It also coordinates the corporate performance management system.

Additionally, the Organizational Development function assists departments in creating climates conducive to career planning and consults with individuals for the purpose of clarifying career aspirations, assessing personal strengths and weaknesses, and establishing career objectives and strategies.

Labor Relations – This division is responsible for planning, organizing and managing the overall relationship between the Company and its unions, collective bargaining negotiations, administering the grievance process, coordinating consistent inter-department administration and interpretation of all labor-management agreements, and representing the Company's position in the final stages of the grievance, arbitration conciliation and/or mediation process. This department also assists line management in policies concerning the coaching, counseling, and disciplining of the union-represented workforce.

Employee Relations and HR Risk Management – This group is responsible for providing consultation services to Company management and supervision to facilitate the development, retention, and consistent administration of a quality and engaged workforce for current and future workforce needs of the Company. This group also audits employment practices and programs to ensure fair application, and investigates Equal Employment Opportunity complaints. The group coordinates our Affirmative Action Planning activities and compiles and submits information in response to government and regulatory agency requirements and requests.

Compensation & Benefits - The Benefits team within the Compensation & Benefits group is responsible for designing and delivering competitive benefits to employees. In addition, this team is responsible for designing and delivering wellness program, disease management programs and other health management program to control health care costs.

The Compensation team within the Compensation & Benefits group is responsible for ensuring a competitive compensation system for all employees. Included in this group's responsibilities is the preparation and analysis of market comparison studies of industry and geographic current practices.

Diversity, Inclusion and Workforce Strategies – This group is responsible for facilitating the creation and support of a culture that is inclusive and diversity-friendly. The guiding principle, which supports Duke's diversity performance initiative, is as follows:

> "Duke will create an organization where no individual or group of individuals is advantaged or disadvantaged because of race, ethnicity, gender, age, religion, sexual orientation, physical ability, tenure or any other cultural or corporate classification. Reaching this goal will assist Duke in maximizing revenues and earnings growth, ensure customer satisfaction by providing excellent service, and align itself to meet and exceed its competitive challenges."

Business Partners – The Business Partners are designated to support functional areas. As HR generalists they are responsible for consulting with management on a broad range of HR issues. Additionally, they facilitate the implementation of HR policies and procedures and serve as a liaison between their functional department and Human Resources.

V. Practices and Procedures

Practices and procedures of Human Resources are organized by department and division. They are described below:

Staffing and Recruiting

- *Developing and conducting recruitment programs for professional employees through* college campus recruiting and coordinating a cooperative education program;
- Developing and maintaining recruitment contacts with state and local employment organizations and area schools to assure an adequate source of nonexempt applications;

- Maintaining applications via an electronic system in order to identify candidates for available positions. Screening and testing applicants and employees in order to determine their suitability and capability for particular positions; and
- Coordinating the internal exempt and nonexempt job posting systems.

Organizational Development

- Administering a Performance Management System for non-union employees in order to assist employees in improving their individual performance, and to provide a means for evaluating job performance and the attainment of corporate goals for salary administration;
- Administering company-wide non-union employee development programs in order to manage and develop the human resources of the Company which are vital to its long-term survival;
- Assisting the operating departments in employee skills training by providing equipment and staff consulting resources;
- Providing coaching and counseling for employees seeking career opportunities.
- Providing consultation to departments in providing the climates and resources conducive to career development;
- Conducting career coaching and counseling training programs; and
- Assisting and coordinating the succession planning efforts for mid-level and executive management positions.

Labor Relations

- Planning, coordinating and supervising the conduct of labor negotiations in order that the management negotiating committee has the necessary information to negotiate a fair and equitable agreement;
- Administering the collective bargaining agreements and advising management on contract interpretation questions to assure fair and uniform application;
- Facilitating the job evaluation committees and administering the job evaluation systems for all job classifications represented by a union;
- Advising management on the grievance procedure and administering the grievance procedure from the third-step through arbitration to assure fair and equitable resolution of employee disputes. Providing labor relations training to supervisors, as required; and
- Providing consistent and defensible counsel to management employees in matters of discipline and labor relations policies.

Employee Relations -

- Designing, and developing procedures to guide management in the implementation of the HR Policies in the areas of affirmative action, work life, fitness for duty, corrective action, diversity, workplace security, preventing and addressing harassment, the development of employees, etc.

- Responding to federal government request for information as well as similar state level and requests (i.e. EEOC charges, OFCCP audits, DHEC complaint, etc.).
- Coordinating the investigation and resolution of EthicsLines issues, Recourses, etc..
- Ensuring an effective HR compliance program by identifying, monitoring, and mitigating risks associated with employment law compliance, internal controls and management effectiveness.
- Administering the Employee Opinion Survey and provide analysis and trending of results with recommendations for actions to address the negative trends.
- Providing Medical and EAP services (medical portion of the overall safety program, FFD program, management referrals) to ensure compliance with various OSHA and NRC programs and to provide assistance to managers and employees in dealing with workplace problems.
- Advising management on the best methods to manage their human resources as an asset (i.e. program development and administration) and on the individual basis) i.e. application of the corrective action procedures to a particular situation).

Compensation & Benefits

- Managing the administration of market pricing and job titling procedures;
- Supervising and administering the application of general wage rate and salary changes for all employees;
- Coordinating and administering the Annual Incentive Programs for all employees;
- Preparing statistical data for negotiations. Administering and preparing wage, salary and fringe benefit surveys and other statistical reports as required for the Company and governmental agencies;
- Designing, implementing and maintaining a comprehensive benefit program and work & family life program that is competitive with comparable utilities and local industries and that provides internal equity in a cost effective manner; and
- Communicating to and educating employees so that they are knowledgeable about the benefits available to them and providing a centralized corporate source for responding to employee questions and problems.

Diversity, Inclusion and Workforce Strategies

- Advising and supporting business partners on recruitment, retention and advancement strategies to ensure equal opportunities for all employees;
- Designing, facilitating and supporting continuing diversity education and awareness.
- Researching and providing information on diversity and work/life best practices and emerging trends;

- Consulting with and providing business partners with solutions to create an inclusive performance-based environment;
- Creating and promoting opportunities for employees to assume individual responsibility for diversity culture change;
- Facilitating, integrating and supporting diversity communications; and
- Developing and maintaining key relationships to promote and support community development and inclusion and identifying opportunities for collaboration with the company's diversity performance initiative.

VI. Decision Making and Control

Daily operational decisions on departmental matters are routinely made by the department functional leads. Decisions affecting corporate policy or multiple departments are reviewed and discussed with the Human Resources Policy Committee of the Board of Directors and the President or involved Officers as required.

The Group Executive and Chief Administrative Officer attends the CEO's staff meeting. Appropriate pending decisions regarding policies and programs on corporate matters are reviewed and discussed. Department and division staff meetings are held after the Officer staff meeting to communicate corporate matters and decisions and to monitor the impact of decisions. In addition, informal discussions routinely take place for decision making with officers and other appropriate internal customers.

VII. Internal and External Communication

Face-to-face internal communications within the individual business units occur frequently during the work day. Communications on topics relevant to other divisions also occur in person daily. External communications with other departments are normally on a personal basis or by phone in order to provide the necessary services to the department. Significant changes occurring within the respective business units are reported at staff meetings. Topics which apply to the entire organization are communicated through various corporate communication vehicles such as the corporate portal, email and targeted direct mailings addressing pertinent human resource issues. Human Resources Communications, in conjunction with Corporate Communications, develops the appropriate materials and distribution methods to communicate pertinent HR information. Decisions on grievances, arbitration proceedings and significant issues affecting employees are communicated to the unions in writing.

External communications also consist of oral communications with counterparts in other utilities, questionnaires, surveys, and participating in and attending professional association meetings, seminars and workshops and industry committee meetings. Other external communications consist of direct contact with human resource counterparts in other companies as well as the governmental agencies.

VIII. Goal Attainment and Qualification

All non-union employees receive an annual performance appraisal review from their reporting manager. During this review meeting, individual division goal achievements are evaluated. Salary adjustments are dependent, in part, on achievement of established goals. The following are examples of performance indicators that provide management of the department with an indication of the quantity and quality of work being completed by the various work units:

Organizational Development

Staffing and Recruiting- Performance is measured by evaluating the number of employees recruited and hired in comparison to the number of job openings, and the time needed to fill the job vacancies as well as customer evaluation of services.

Organizational Development - Performance is evaluated by the actual cost and days of training delivered as compared to the budget plan. Training evaluation questionnaires are used regularly to monitor the value and effectiveness of the programs, as well as customer feedback questionnaires on services, which are administered annually.

Labor Relations - Performance is measured by internal customer feedback questionnaires on services, which are administered throughout the year. The number of hearings and investigations related to third-step grievances, neutral arbitration cases, and the timeliness and persuasiveness of written labor relations' communications are a further gauge of performance.

Employee Relations – Performance is measured in several ways including employee productivity measurements or forced turnover ratios and resulting employee action, the number of complaints, both from an EEO compliance standpoint as well as union, non-union, or potential harassment concerns that are successfully handled to resolution. Other measures used include timely responses to various agency requests for reports, including Affirmative Action Plans and Compliance Reviews. Employee Opinion Survey results and trends as well as internal and external audits of Medical Services.

Compensation & Benefits - General performance indicators of the Compensation and Benefits Group are derived by reviewing wage and benefit surveys among utility companies as well as local, regional and national industry positions to ascertain the Company's position in the wages and benefits area. Benefit program costs such as health care costs are monitored for delivery trends and carrier performance. Performance of programs is also evaluated by the number of employees who use the services and feedback from internal customers and employees.

Diversity, Inclusion and Workforce Strategies - Performance can be measured based on the number and nature of internal and external complaints or grievances relative to hiring, promotional and developmental opportunities and the quality of interpersonal relationships and dealings with others. Training evaluations and other feedback are another means for measuring performance along with any local, regional or national recognition of the company's diversity and work/life practices.

Exhibit HR-1

Duke Energy

Duke Energy

Corporate Compliance/Risk Management Policies, Standards, Procedures, Guidelines.

HR POLICY NAME	RELATED HR STANDARDS	RELATED HR PROCEDURES	RELATED HR GUIDELINES
Approved by HR Governing Body	*Approved by Chief HR Officer Endorsed by HR Governing Body*	*Approved by HR Function Executive Endorsed by HR Governing Body*	*Approved by HR Function Executive Endorsed by HR Governing Body*
HR1000 – Affirmative Action and Equal Employment Opportunity		**HR1001P Affirmative Action, EEO, & Diversity Procedure** **HR1002P Employment and Separation Procedure**	
HR2000 – Alcohol and Drug Free Workplace		**HR2001P Alcohol and Drug Use Procedure**	
HR3000 – Corrective Action		**HR3001P Corrective Action Procedure**	
HR4000 – Diversity and Inclusion			
HR5000 – General Workplace Security	**HR5001S Screening Standard: Prior to Employment** **HR5002S In-Service Screening Standard: Positions of Substantial Authority**	**HR5001P General Workplace Security Procedure** **HR5002P Employee Access to the NRC** **HR5003P Nuclear Safety**	
HR6000 – Harassment		**HR6001P Harassment Procedure**	
HR7000 – Open Door		**HR7001P Employee Recourse Procedure**	
HR8000 – Workforce Development			
HR9000 – Workforce Identification	**HR9001S HR Electronic, Personal Information, Privacy Standard**	**HR9001P Personnel Transaction Entry Procedure**	
HR10000 – WorkLife		**HR10001P FMLA** **HR10002P Non-FMLA** **HR10003P PLOA** **HR10004P Military LOA** **HR10005P Holiday** **HR10006P Vacation** **HR10007P Jury Duty &**	

Exhibit HR-1

Corporate Compliance/Risk Management Policies, Standards, Procedures, Guidelines.

		Court Appearance HR10008P Funeral Absence HR10009P Inclement Weather HR10010P Attendance and Absences HR10011P Service/Retirement Award HR10012P Education Reimbursement HR10013P Sick Time Pay HR10014P Overtime-Callout Pay HR10015P Shift Differential	

Definitions:

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

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

Procedure – The specific actions required to be compliant with the Policies and Standards. They are documented step-by-step instructions and may exist at any level of the organization.

Guideline – *A statement or other indication of policy or procedure by which to determine a course of action.*

Exhibit HR-1

HR1000 Affirmative Action and Equal Employment Opportunity Policy

Applicability:	Applies to United States employees only
Originator:	Corporate Human Resources
Approval:	Group Executive and Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

We meet both the spirit and the letter of the law. We recognize the contributions of every individual. To that end, this policy establishes Duke Energy's commitment to Affirmative Action and Equal Employment Opportunity.

HR1000.1 Policy Expectations

Duke Energy does not discriminate against any employee or applicant for employment because of race, color, sex, religion, national origin, ethnicity, citizenship, sexual orientation, age, marital status, disability, status as a Vietnam Era or disabled veteran. Duke Energy also complies with all applicable state, federal and local laws, regulations and ordinances prohibiting discrimination in places where Duke Energy operates.

Duke Energy will make every good faith effort to ensure that this policy is implemented in all personnel decisions. It will fully comply with local, state and United States federal laws and regulations implementing equal employment opportunity objectives. To achieve this, Duke Energy has implemented an Affirmative Action Program to ensure equal opportunity to obtain employment and to progress without regard to race, sex, disability, or status as a disabled veteran or veteran of the Vietnam Era.

HR1000.2 Accountability: Roles and Responsibilities

The Group Executive & Chief HR Officer will receive and take action on reports regarding Affirmative Action and Equal Employment Opportunity.

Human Resources Compliance & Risk Management is responsible for assuring corporate-wide effectiveness of the Duke Energy Affirmative Action and Equal Employment Opportunity Policy, its Affirmative Action Program, and reporting on progress.

Business and operating units and corporate departments are responsible for managing and evaluating Equal Employment initiatives and Affirmative Action within their areas of responsibility, including:

- developing and implementing Affirmative Action Plans for all locations and employees
- taking strong efforts to include women and minorities in hiring pools
- reporting results at least annually to Corporate Human Resources

Key Terms

Affirmative Action Program: Management tool designed to ensure equal employment opportunity. A central premise underlying affirmative action is that, absent discrimination, over time a contractor's workforce, generally, will reflect the gender, racial and ethnic profile of the labor pools from which the contractor recruits and selects.

Equal Employment Opportunity (EEO): Equal employment opportunity is required by law and mandates that an employer develop a neutral posture ensuring that all people have equal access to employment opportunities. Equal employment opportunity is enforced by the Equal Employment Opportunity Commission (EEOC).

Exhibit HR-1

HR2000 Alcohol and Drug-Free Workplace Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

We operate safely, and rely on one another to achieve superior results. As such, Duke Energy does not tolerate alcohol or drug use and/or abuse connected with business or operations.

HR2000.1 Policy Expectations

Duke Energy employees are expected to report for work and remain at work in a condition free of the effects of alcohol or drugs - prepared to work together safely to operate our business. Alcohol or drug use affecting job performance, corporate reputation, corporation assets, or the safety of employees or the public will not be tolerated.

Employees shall not be involved with the unlawful use, possession, sale, arrange for the sale, manufacture, dispense or transfer illegal drugs, narcotics or alcohol either on or off the job. Any employee using prescription and/or non-prescription drugs must notify supervision or medical staff when job performance may be affected.

Smoking is prohibited in all indoor work areas, unless the Company has designated that area as a smoking area.

Although alcohol may be served at company-sponsored events, any excessive use of alcohol at those events that may jeopardize your safety and/or the safety of your co-workers or the public is prohibited.

Employee Assistance Programs are available for Duke Energy employees (and such use may be required).

Any employee violating this policy will be subject to corrective action up to and including discharge.

HR2000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments are required to develop, communicate, and publish procedures enacting this policy as needed. Where applicable, procedures must address

Exhibit HR-1

Nuclear Regulatory Commission, Department of Transportation, and the Federal Energy Regulatory Commission requirements and applicable state statues.

Unless regulations require otherwise, pre-employment drug screening is required of all applicants offered employment. Where screening shows a confirmed positive drug screen, applicants will not be considered for employment, temporary or otherwise.

Key Terms

Employee Assistance Program : The Employee Assistance Program provides Duke Energy employees and their family members an opportunity to address personal issues privately and effectively before they become overwhelming and impact job performance or quality of life. The program offers a range of services to help you and your family members with a variety of issues including alcohol and drug issues, stress, anger management, and others. You can contact your EAP 24 hours per day, 7 days a week.

Exhibit HR-1

HR3000 Corrective Action Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

All employees are expected to conform to established standards of ethical conduct such as honesty, trustworthiness, dependability and professionalism. Inappropriate conduct will be addressed through corrective actions, up to, and including termination from employment. Corrective action may be imposed regardless of whether the inappropriate behavior is specifically addressed by a written policy.

HR3000.1 Policy Expectations

Corrective action may include, but is not limited to, verbal or written warnings, suspension from work, or other disciplinary action up to and including employment termination. Verbal or written corrective action is intended to eliminate inappropriate workplace conduct of a more minor nature. *Immediate termination without use of progressive discipline may be appropriate for serious incidents.*

HR3000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments may develop, implement, communicate and enforce corrective action procedures as needed. Procedures should:

- explain the corrective action process and conditions for discipline and discharge
- include records retention guidelines
- be consistently enforced

Supervisors are expected to communicate employee conduct expectations, identify inappropriate conduct and take appropriate corrective action.

Employees are expected to:

- cooperate
- promote individual and corporate success
- correct identified inappropriate conduct

Exhibit HR-1

HR4000 Diversity and Inclusion Policy

Applicability:	Applies to Enterprise
Originator:	Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	10/01/2004
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

In keeping with Duke Energy's charter and values, this policy outlines the company's commitment to creating and maintaining a diverse and inclusive workforce, and doing business with diverse suppliers.

Diversity embodies all the differences - life experiences, work experiences, perspectives, cultures, race, gender, sexual orientation, religion, national origin, age or disability. Inclusion entails building an environment where employee differences are valued, employees are empowered and diverse Duke Energy communities are connected across the enterprise.

An inclusive environment encourages all employees to contribute their unique perspectives and capabilities, and fully engages a diverse workforce in achieving superior business results. Inclusion fosters trust, the cornerstone for risking new ideas and fostering *a sense of accomplishment* - powerful motivators that draw out each person's best performance. Inclusion creates the environment where "every employee can start each day with a sense of purpose and end each day with a sense of accomplishment."

Additionally, Duke Energy supports the win-win relationships that a strong supplier diversity program fosters within the communities we serve.

HR4000.1 Policy Expectations

"Respect for the Individual" is fundamental to building a high performance team. All employees share the responsibility for creating a workplace that values and respects diversity and inclusion - enhanced by openness, sharing, trust, teamwork and involvement.

"Win-win relationships" are essential to restoring credibility and earning the trust of employees, customers, suppliers and communities. We demonstrate inclusion in our procurement practices when we provide opportunities for diverse and small businesses to provide goods and services to the company.

HR4000.2 Accountability: Roles and Responsibilities

Exhibit HR-1

The Chief HR Officer is responsible for assuring enterprise-wide implementation of the Duke Energy Diversity and Inclusion Policy and associated initiatives.

Groups which exist to champion and further diversity performance will coordinate and align efforts with the Chief HR Officer

Management at all levels is responsible for ensuring that employee differences are respected and valued in the workplace, the Duke Energy Inclusive Behaviors are personally demonstrated, and that we seek opportunity to do business with diverse companies.

Business and operating units and corporate departments are responsible for:

- *Developing and implementing plans, establishing initiatives and report results that support* diversity and inclusion.

Exhibit HR-1

HR5000 General Workplace Security Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

Duke Energy is committed to operating safely. In so far as practical as possible, it is Duke Energy's intent to maintain a secure work environment free from intimidation, threats, or violent acts.

HR5000.1 Policy Expectations

Violence or threats from employees or others will not be tolerated. Certain actions are prohibited, including the following:

- injuring other persons physically
- causing others reasonable fear of injury
- causing others extreme emotional distress
- possessing or using weapons while on Duke Energy premises or engaged in Duke Energy business, unless authorized
- intentionally damaging property
- threatening others or company property
- committing work-related injurious acts of domestic violence or sexual harassment
- participating in disruptive acts such as sabotage, bomb threats, or other illegal activity

Duke Energy assesses and improves workplace security as necessary. Persons involved in illegal work-related acts may be prosecuted.

Employees:

- are responsible for reporting to local security or their supervisor actual, suspected, or likely acts of theft, violence, harassment, or threats to employees or property
- are required to assist and cooperate in investigations
- must act in a safe and secure manner
- violating this policy are subject to corrective action

HR5000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments establish procedures as needed to enact this policy.

Exhibit HR-1

HR6000 Harassment Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

This policy establishes Duke Energy's commitment to provide a workplace free of harassment, and to take appropriate action if harassment occurs. Duke Energy will maintain a work environment in which employees can perform their assigned duties and responsibilities without being harassed by any other employee, contractor, customer, vendor or visitor. We build relationships based on mutual respect and trust. We support and rely on each other to achieve superior results. Harassment, creating an intimidating, hostile or offensive work environment or interfering with work performance will not be tolerated.

HR6000.1 Policy Expectations

Harassment is defined as any action that singles out an employee, to the employee's objection or detriment, because of race, sex, sexual orientation, religion, national origin, ethnicity, citizenship, age, martial status, disability, status as a Vietnam Era or disabled veteran. Duke Energy also complies with all applicable state, federal and local laws, regulations and ordinances prohibiting discrimination in places where Duke Energy operates. Below are examples of activities that might constitute harassment:

- Verbal or non-verbal threats, insults abuse or ridicule (sexual or otherwise)
- Unnecessary or offensive physical contact
- Possessing, displaying, or distributing pornographic or offensive materials
- Attempted or actual intimate physical contact
- Requesting or demanding favors (sexual or otherwise), explicitly or implicitly, as a condition of employment, promotion, transfer, or any other personnel action
- Physical conduct such as assault or blocking normal movement

Employees should promptly report possible harassment to their immediate supervisor, another manager, or Human Resources. If employees are uncomfortable reporting such matters to these parties, they may also use the external, anonymous EthicsLine at 1-800-525-3783 or the Web site at http://www.dukeenergy-ethicsline.com. EthicsLine is available 24 hours, 365 days per year.

Exhibit HR-1

All harassment claims will be promptly and thoroughly investigated in as confidential a manner as possible. Where investigation confirms harassment occurred, the party committing the harassment will incur discipline up to and including employment termination.

Duke Energy forbids retaliation against employees for their actions in bringing harassment or other concerns to management or regulatory agencies (e.g., the Nuclear Regulatory Commission, Equal Employment Opportunity Commission, Occupational Safety & Health Administration, or other agencies). Retaliation is also forbidden against employees for their participation in harassment investigations or resolutions. Persons found to have committed such retaliation will incur discipline up to and including employment termination.

HR6000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments develop procedures as needed in support of the harassment policy.

Executives, managers, supervisors, and employees having knowledge of possible harassment must promptly inform Human Resources to ensure investigation. Failure to take prompt, immediate and effective reasonable measures to prevent or correct harassment in the workplace may result in corporate or personal legal liability, and may also result in corrective action up to and including employment termination.

HR7000 Open Door Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose

We value clear and open communications, and respect the contributions of all employees. This policy establishes Duke Energy's intent to provide an environment with unrestricted access to management, where employees feel free to raise work-related concerns to their supervisors or others without fear of intimidation or retaliation.

HR7000.1 Policy Expectations

The Open Door policy encourages channels of access and accountability beyond immediate supervision. While employees are encouraged to bring work-related concerns to their supervisor, they may also seek resolution by talking to another member of management or a Human Resources representative.

Employees who wish to discuss an issue without being identified can call the EthicsLine, an external, anonymous reporting system available 24 hours a day, 365 days a year for all employees. The toll-free number is 1-800-525-3783 or use the Web site https://www.dukeenergy-ethicsline.com.

Regardless of how an issue is reported or discussed, retaliation against employees raising concerns or participating in investigations will not be tolerated. This means Duke Energy will not terminate, demote, transfer to an undesirable assignment or otherwise discriminate against an employee who brings work-related concerns to the attention of management, HR, EthicsLine, or any external agency. When an adverse employment action is caused by an employee's protected activity, this policy is violated. Examples of protected activity are: (1) opposing a practice that is prohibited by law in a manner that clearly communicates the employee's opposition; or (2) filing a report, charge, complaint, or testifying, assisting, or participating in any manner in an investigation, proceeding, or hearing under the applicable law or policy.

HR7000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments are required to:

- Create and communicate to employees open door or recourse processes to address personal, business or technical concerns
- Create environments where employees are comfortable elevating issues to their management without fear of retaliation

The Audit Committee reviews concerns regarding questionable accounting, internal financial controls (including internal accounting controls), and auditing matters, and has established a procedure to allow for confidential, anonymous submission by employees. Employees should report these types of concerns to their Corporate Compliance Manager or the Ethics and Compliance Office, or use the EthicsLine, which allows for anonymous reporting. All such concerns will be investigated and the Audit Committee will receive a summary of such reported concerns together with a synopsis of the company's assessment of and resolution of each concern.

HR8000 Workforce Development Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Exhibit HR-1

Statement of Purpose and Philosophy

Duke Energy recognizes the contributions of every individual, and that workforce capabilities and talents are critical to business success. This policy establishes Duke Energy's commitment to employee development, workforce planning, and succession planning.

HR8000.1 Policy Expectations

Duke Energy's goal through workforce development is to ensure that:

- staffing needs are assessed and workforce plans developed
- employee developmental opportunities are available consistent with business needs
- succession planning occurs ensuring business continuity

Duke Energy uses job postings, management referrals, external recruitment, and planned workforce reassignments to fill positions.

Employees are responsible for their career development.

HR8000.2 Accountability: Roles and Responsibilities

TheVice President of Corporate Human Resources establishes processes for workforce planning, management development, and succession planning. This includes:

- regularly scheduled succession planning for key positions
- developmental plans being completed for candidates identified in succession planning

Business and operating units and corporate departments are responsible for:

- workforce planning and employee development within their organizations
- ensuring annual discussions of performance and developmental needs for each employee

HR8000.3 Standards

- Business-related job posting restrictions may occur (e.g., local candidate preference, limited or no relocation expenses paid).
- While employee preferences are considered, meeting business need is the priority in all decisions.
- External candidates are sought when no internal candidates satisfy the position requirements.

HR9000 Workforce Identification Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer

Exhibit HR-1

Effective Date: 04/01/2006
Revision Date: 04/01/2006
Reissue Date: 04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

This policy establishes the Human Resources Management System (HRMS) as Duke Energy's worldwide system of record for establishing and maintaining workforce identity information.

HR9000.1 Policy Expectations

To ensure appropriate workforce authentication and access rights, and to ensure HR processes provide accurate data to support compliance activities, Duke Energy requires that necessary information be entered into the Human Resources Management System, which is the worldwide system of record for workforce identities.

All employees (domestic, international and local nationals, including those on active, inactive, or terminated status), as well as contractors, for whom one or more of the following conditions is true must comply with the policy:

- Identifying information is required for compensation, benefits, training, or other human resources processes.
- Access is required to Duke Energy information technology assets, including, but not limited to, company networks, hardware, and software, including the Duke Energy Employee Portal.

The workforce identification process is intended to protect the company's assets, to help assure compliance with rules regarding data access, and to ensure high integrity data regarding the workforce. This policy and the procedures which support it comply with data privacy laws and policies.

HR9000.2 Accountability: Roles and Responsibilities

HR9000.2.1 Chief Human Resources Officer:

- Ensure enterprise-wide implementation and effectiveness of the Duke Energy Workforce Identification Policy
- Report any compliance failures to the Chief HR Officer and appropriate Business Unit HR Leader.

HR9000.2.2 Director of Human Resources Technology, Systems, and Processes:

- Ensure enterprise-wide processes are in place for system integrity, data integrity, system interfaces, and data entry

- *Produce and distribute HR Data Entry report to support compliance monitoring by business unit*

HR9000.2.3 Business and operating units and corporate departments, Human Resources:

- Ensure accurate entry of workforce data into the Human Resources Management System. Workforce data must be entered prior to granting access to electronic data, certain company facilities, or equipment.
- Ensure timely entry of workforce data.
  - o *Data for employee terminations and employee FERC transfers must be entered according to the following schedule:*

Transaction	**Entry Deadline**
Terminations	Entered by 7 PM EST on or before the last day worked. Exceptions allowed for LOA/LTD/FMLA and unplanned terminations (removals from service). Late entry notification required to Business Unit HR Leader. This notification may be made retroactively (i.e. "after the entry is made") to allow immediate entry of termination record and termination of accesses. Notification may be delegated by the Business Unit HR Leader effective January 2006.
FERC Transfers	Entered by 7 PM EST the day before the effective date of the transfer. No allowance for approvals of late entry for FERC transfers.

- *Entry deadlines for other personnel transactions are as defined in business unit procedures.* (Other personnel transactions include: hires, re-hires, non-FERC impacted transfers, leave of absence, promotion, job title change, pay rate change, job reclassification, off-cycle leadership actions, basic data change, one-time/OCI payment, department reorganization, long term disability (LTD) leave and return from leave)
- Comply with established procedures for HRMS data requirements.
- Report system issues to the Director of Human Resources Optimization (HRO).

HR9000.2.4 Business Unit Manager and Supervisors:

- Ensure timely and accurate notification for entry of workforce data for all terminations and FERC Transfers, in order to comply with the entry deadline timeliness requirement.

HR9000.2.5 HR Administrative Services Provider:

- Ensure timely and accurate entry of workforce data into the Human Resources Management System
- Report system issues to the Director of Human Resources Optimization (HRO).
- Comply with established procedures for HRMS data requirements

Key Terms

Workforce Identification : The process of maintaining a collection of electronic information that describes an individual and provides data which authenticates the individual's identity and can indicate access levels to company information and facilities.

Exhibit HR-1

HR10000 WorkLife Policy

Applicability:	Applies to Enterprise
Originator:	Corporate Human Resources
Approval:	Group Executive & Chief Human Resources Officer
Effective Date:	11/01/1998
Revision Date:	04/01/2006
Reissue Date:	04/01/2006

THIS POLICY DOES NOT CREATE A CONTRACT OF EMPLOYMENT OR ALTER THE AT WILL NATURE OF ANY EMPLOYEE'S EMPLOYMENT IN ANY WAY.

Statement of Purpose and Philosophy

Duke Energy understands that part of being a productive, successful employee is finding the appropriate balance between our priorities at work, home and in our communities. We support and rely on each other as a team and recognize that individual workers may seek flexible work options. This policy sets forth Duke Energy's commitment in addressing WorkLife balance issues to the extent permitted by business needs.

HR10000.1 Policy Expectations

WorkLife balance programs or options can be developed by corporate departments and business units.

In considering WorkLife options, an evaluation of business needs should be performed. This evaluation includes reviewing:

- work requirements
- customer impact
- financial considerations
- employee recruitment or retention
- employee demographics
- rate of employee use
- other relevant needs

All programs must comply with Federal, State, and country specific regulations and be administered in a fair and consistent manner, as applicable.

HR10000.2 Accountability: Roles and Responsibilities

Business and operating units and corporate departments are responsible for considering flexible work arrangement needs, and may implement additional worklife programs.

Managers and employees are encouraged to familiarize themselves with and understand worklife program provisions.

Exhibit HR-1

The Group Executive & Chief Human Resources Officer is responsible for communicating and championing the WorkLife Policy.

Exhibit HR-2

DUKE ENERGY CORPORATION MANAGEMENT STRUCTURE

Vice President Corporate Human Resources

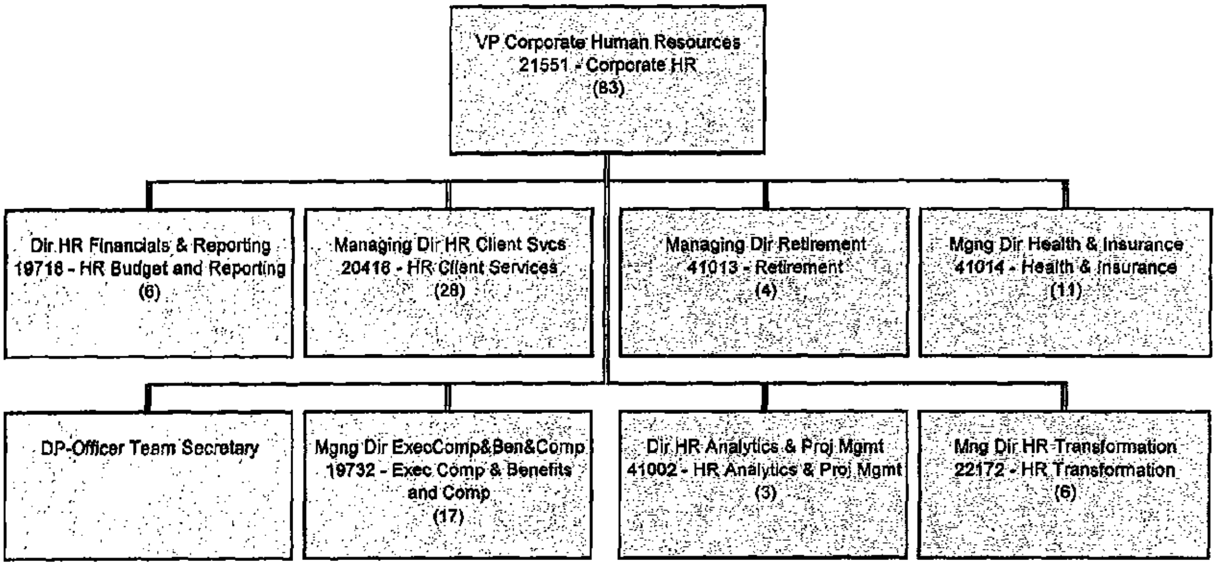
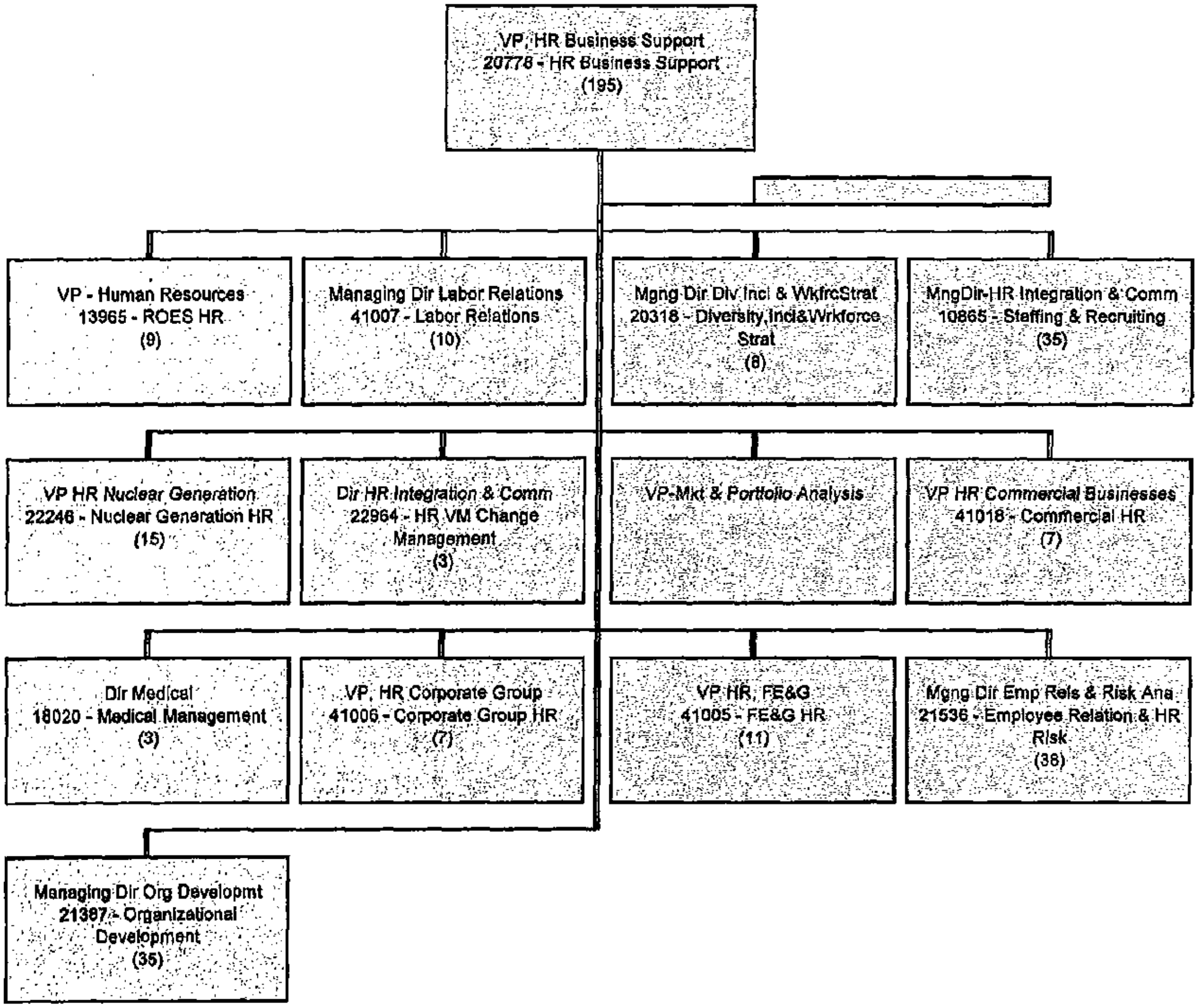

VP Corporate Human Resources 21551 - Corporate HR (83)
Dir HR Financials & Reporting 19716 - HR Budget and Reporting (6)
Managing Dir HR Client Svcs 20416 - HR Client Services (28)
Managing Dir Retirement 41013 - Retirement (4)
Mgng Dir Health & Insurance 41014 - Health & Insurance (11)
DP-Officer Team Secretary
Mgng Dir ExecComp&Ben&Comp 19732 - Exec Comp & Benefits and Comp (17)
Dir HR Analytics & Proj Mgmt 41002 - HR Analytics & Proj Mgmt (3)
Mng Dir HR Transformation 22172 - HR Transformation (6)

Exhibit HR-2

Vice President HR Business Support



VP, HR Business Support
20778 - HR Business Support
(195)

VP - Human Resources
13965 - ROES HR
(9)

Managing Dir Labor Relations
41007 - Labor Relations
(10)

Mgng Dir Div Incl & WkfrcStrat
20318 - Diversity,Incl&Wrkforce Strat
(8)

MngDir-HR Integration & Comm
10865 - Staffing & Recruiting
(35)

VP HR Nuclear Generation
22246 - Nuclear Generation HR
(15)

Dir HR Integration & Comm
22964 - HR VM Change Management
(3)

VP-Mkt & Portfolio Analysis

VP HR Commercial Businesses
41018 - Commercial HR
(7)

Dir Medical
18020 - Medical Management
(3)

VP, HR Corporate Group
41006 - Corporate Group HR
(7)

VP HR, FE&G
41005 - FE&G HR
(11)

Mgng Dir Emp Rels & Risk Ana
21536 - Employee Relation & HR Risk
(38)

Managing Dir Org Developmt
21387 - Organizational Development
(35)

Schedule S-4.2

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:

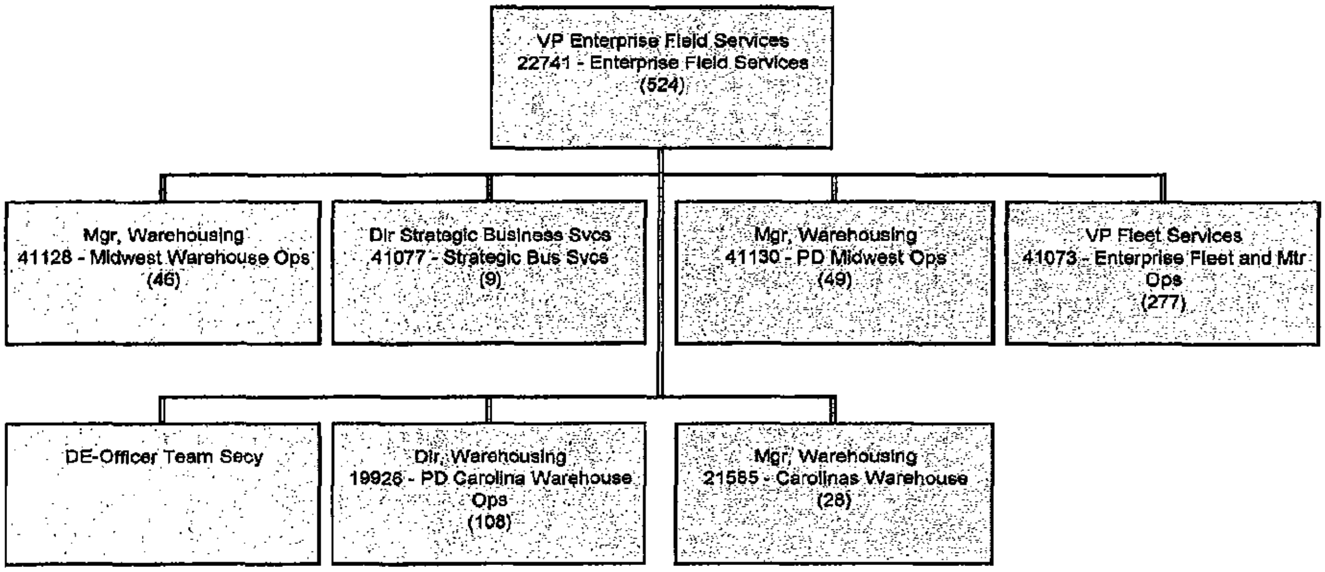
- In 2000 we entered into an alliance for our mounted equipment with ALTEC Industries, Inc. This has helped control costs associated with new and rental line and bucket trucks;
- In 2002 we implemented an automatic progression policy for the union mechanics in the Duke Energy Ohio service territory. 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.

Exhibit TP-1

DUKE ENERGY MANAGEMENT STRUCTURE

Vice President Enterprise Field Services


VP Enterprise Field Services
22741 - Enterprise Field Services
(524)
Mgr, Warehousing
41128 - Midwest Warehouse Ops
(46)
Dir Strategic Business Svcs
41077 - Strategic Bus Svcs
(9)
Mgr, Warehousing
41130 - PD Midwest Ops
(49)
VP Fleet Services
41073 - Enterprise Fleet and Mtr Ops
(277)
DE-Officer Team Secy
Dir, Warehousing
19926 - PD Carolina Warehouse Ops
(108)
Mgr, Warehousing
21585 - Carolinas Warehouse
(28)