. . . a better way

Route To:

_____
_____
_____

NORCON

(NOREX MEMBER CONTRIBUTED DOCUMENT)

NORCON 47-559

Information Security Policy

This policy covers responsibilities of Internet and e-mail use, computer viruses, access codes/passwords, copyright & license agreements, and physical security. *8 Pages*

0308

Information Security Policy

Introduction

Computer information systems and networks are an integral part of business at (company) Corporation. The company has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the company.

Violations

Violations may result in disciplinary action in accordance with company policy. Failure to observe these guidelines may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

(company) is committed to protecting our customers' information and our resources used in the course of doing business. Violations of the Information Security Policies in the may result in disciplinary action up to and including termination of employment. Examples of policy violations include, but are not limited to, exposure of confidential customer or company information resulting from loss of equipment (such as laptops, PDAs, and cell phones), unauthorized use or misuse of company e-mail or other information systems, or failure to adhere to established data handling guidelines. Violations will be dealt with on a case-by-case basis and consequences will mirror the seriousness of the violation. For gross violation, criminal charges may also be pursued.

Administration

The Chief Information Officer (CIO)/IT Manager is responsible for the administration of this policy.

Contents

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Computer viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreements

Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Manager responsibilities

Managers and supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

IT Manager Responsibilities

The IT Manager must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

The Internet and E-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

Policy

Access to the Internet is provided to employees for the benefit of (company) Corporation and its customers. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the company's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable Use

Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed.
- Using e-mail for business contacts.

Unacceptable Use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Conducting a personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Streaming audio such as XM Satellite Radio or Streaming Video. Both take bandwidth away from legitimate business.

Downloads

File downloads from the Internet are not permitted unless specifically authorized in writing by the IT manager.

Employee Responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable (company) policies dealing with security and confidentiality of company records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the company and *may be regarded as public information*. (company) Corporation reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IT Responsibilities

IT shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee Responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Employees shall not load diskettes of unknown origin.
3. Incoming diskettes shall be scanned for viruses before they are read.
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IT manager.

Access Codes and Passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

IT Responsibilities

The Network Administrator shall be responsible for the daily administration of access controls to all company computer systems. The Network Administrator will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request. The Network Administrator will maintain a list of administrative access codes and passwords and keep this list in a secure area.

The Network Administrator is responsible for regulating and monitoring the computer environment. The following security standards and controls have been established:

Password Restrictions:

1. All passwords shall be set to expire every 90 days
2. Passwords must contain at least 8 characters including 3 of the following 4 elements: special characters, numbers, upper case letters and/or lower case letters.
3. Accounts shall be locked out after 3 unsuccessful attempts
4. Account lockout duration shall be set to 120 minutes
5. Password changes shall be allowed once per day
6. Unique passwords shall be required

Audit Policy:

1. Logon and Logoff – any attempt to gain access an NT server shall be logged
2. File and Object Access – any attempt at the introduction of unauthorized scripts or executable programs shall be logged.
3. User and Group Management - any attempt to make changes to Windows NT Users or groups, in particular the membership of the Administrator group, shall be logged
4. System Restart – any attempt to restart or shutdown the servers shall be logged
5. Security Policy Changes - any attempt to make changes to the User Rights, Audit, or Trust Relationships policies, shall be logged.
6. Security logs for all NT servers shall be reviewed at regular intervals

Employee Responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords at least every 90 days.
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period.

Supervisor's Responsibility

Managers and supervisors should notify the IT Manager and Network Administrator promptly via e-mail or telephone whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination. The IT Manager or Network Administrator will immediately forward this information to all system administrators ensuring that all application specific access is also denied.

Human Resources Responsibility

The Personnel Department will notify IT monthly of associate transfers. Terminations, whether voluntary or involuntary must be reported concurrent with the termination to the IT Manager and Network Administrator. The IT Manager or Network Administrator will immediately forward this information to all system administrators ensuring that all application specific access is also denied.

Physical Security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee Responsibilities

The directives below apply to all employees:

1. Diskettes should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IT Manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Employees shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

Copyrights and License Agreements

It is (company)'s policy to comply with all laws regarding intellectual property.

Legal Reference

(company) and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose (company) and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by (company), licensed to (company), or developed using (company) resources by employees or vendors.

IT Responsibilities

The IT Manager will:

1. Maintain records of software licenses owned by (company) Corporation.
2. Periodically (at least annually) scan company computers to verify that only authorized software is installed.

Employee Responsibilities

Employees shall not:

1. Install software unless authorized by IT. Only software that is licensed to or owned by (company) is to be installed on (company)e computers.
2. Copy software unless authorized by IT.
3. Download software unless authorized by IT.

Civil Penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

Criminal Penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain [Title 18 Section 2319(b)]," expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the (company) Corporation Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return **this page only** to the Human Resources Department.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy" and understand the same;

ii. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about (company) Corporation and its customers or its vendors, and that this is and remains the property of the company at all times;

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at (company) Corporation), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree that, if I leave (company) Corporation for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

v. I understand that violations of the Information Security Policies may result in disciplinary action up to and including termination of employment. Examples of policy violations include, but are not limited to, exposure of confidential customer or company information resulting from loss of equipment (such as laptops, PDAs, and cell phones), unauthorized use or misuse of company email or other information systems, or failure to adhere to established data handling guidelines. Violations will be dealt with on a case-by-case basis and consequences will mirror the seriousness of the violation. For gross violation, criminal charges may also be pursued.

Employee signature: _____

Employee name: _____

Date: _____