**Business: [Organization Name]**

**INFORMATION SECURITY POLICIES**

##### Responsible Owner: [Chief Information Security Officer or Equivalent]

##### Version 1.0

**Table of Contents**

1. [Information Security Management Policy 5](#_bookmark0)
2. [Acceptable Use Policy](#_bookmark1) 8
3. [Information Security Incident Management Policy 1](#_bookmark2)7
4. [Password and Authentication Policy 2](#_bookmark3)1
5. [Anti-Virus Policy 27](#_bookmark4)
6. [Information Security Awareness and Training Policy 3](#_bookmark5)0
7. [Information Systems Access Control Policy 3](#_bookmark6)4
8. [Information Systems Asset Management Policy](#_bookmark7) 39
9. [Physical & Environmental Security Management Policy 41](file:///C:\Users\Kurt\Downloads\InfoSecManagementPolicy_Master%20(24).docx#_bookmark8)
10. [Information Systems Operations Management Policy 49](file:///C:\Users\Kurt\Downloads\InfoSecManagementPolicy_Master%20(24).docx#_bookmark9)
11. [Network and Telecommunication Security Management Policy](#_bookmark10) 54
12. [Business Continuity and Disaster Recovery Planning Policy 58](#_bookmark11)

##### Notice/Disclaimer

**Purpose of this Manual**

Information is a critical asset for **[Organization Name]** (“**ORG**” or the “**Organization**”). The daily operations and the associated delivery of customer services rely on the confidentiality, integrity, and availability of information.

Thus, this Manual has the following objective:

To define and establish ORG’s policy surrounding the confidentiality, integrity, and availability of information created, received, stored, or transmitted by the Organization.

The definition of confidentiality, integrity, and availability as used within Information Security Program are:

**Confidentiality** — “data or information is not made available or disclosed to unauthorized persons or processes”.

**Integrity** — “data or information have not been altered or destroyed, except where authorized”.

**Availability** — “data or information is accessible and useable upon demand by an authorized person”.

**Scope**

These policies apply to ORG’s enterprise. Consequently, all employees, contractors, part-time or temporary workers, as well as those employed by others that may perform work or have access to the Organization’s information or information systems, are subject to all policy, procedures, and guidelines contained herein.

**Definitions**

|  |  |
| --- | --- |
| **Policy** | **Standards** |
| Widespread application | Widespread application |
| Changes less frequently | Rarely changes |
| Expressed in broad terms  Statements of “what” and/or “why” | Collection of ***system-specific*** or ***procedural-specific*** requirements that must be met by everyone |
| Answers major operational issue(s) | Must be followed exactly |
| **Procedures** | **Guidelines** |
| Narrow application | Narrow application |
| Subject to change | Subject to change |
| Stated in detail  Statements of “how,” “when” and/or “who” | Typically, a collection of system specific or procedural specific “**suggestions**” for best practice |
| **Describes process** |  |

# Information Security Management Policy

### Assigned Responsibility: Chief Information Security Officer or Equivalent

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Security Management Policy

### Purpose

To specify ORG’s policy for protecting **information** from all threats and to ensure continuity of key processes, minimize disruption and damage, as well as maximize all return on investments and opportunities.

### Applicability/Scope

This policy applies to all information and systems owned or leased by ORG. This policy also applies to all employees, associates, and independent contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

ORG’s Chief Information Security Officer is tasked to establish and maintain the framework necessary to provide assurance that information security strategies are aligned with the Organization’s objectives and consistent with federal and state laws and regulations.

### Enforcement

Failure to comply with information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### ORG Policy

ORG management is committed to protecting its information resources through the implementation and operation of a well-defined information security program. ORG shall manage information security by implementing:

### Information Security Governance Infrastructure

* + Obtain senior management commitment and support for information security throughout the organization.
  + Develop information security strategies in support of the Organization’s business requirements, as well as state and federal regulations.
  + Ensure that definitions of information security roles and responsibilities throughout the organization are adequately defined and enforced.

### Information Security Program Management

* + Develop and maintain plans to implement an information security framework.
  + Develop information security baselines for network and/or application information systems in order to objectively evaluate security gaps.
  + Develop procedures to assist data owners in addressing information security risks.
  + Develop procedures for IT infrastructure change management activities to ensure compliance with information security policies.
  + Promote accountability by business process owners, data owners, and other stakeholders in managing information security risks.
  + Ensure that resources for information security are appropriately identified and managed.

### Incident Response Management

* + Develop and implement processes for detecting, identifying, analyzing, and reporting information security related events.
  + Develop response and recovery plans including organizing, training, and equipping the response and recovery teams.
  + Ensure periodic testing of the response and recovery plans where appropriate.
  + Ensure the execution of response and recovery plans as required.
  + Manage post-event reviews (i.e., “lessons learned”) and coordination of remediation activities to identify event causes and recommend corrective actions.

# Acceptable Use Policy

### Assigned Responsibility: Chief Information Security Officer or Equivalent

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Acceptable Use Policy

### Purpose

This policy is intended to define the appropriate use of ORG’s *Information Resources*. *Information Resources* include data in any form (electronic or paper), computer systems, telephonic systems, or any other system used to convey, interpret, or retain information.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all ORG employees, associates and contractors. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal or state laws or regulatory requirements may preempt this policy.

### Roles and Responsibilities

ORG has the responsibility to ensure that managed/owned networks under his cognizance fully comply with the provisions of this Organization policy.

**System Owners** – are responsible for the implementation and management of this policy.

**Users** – are responsible for reading and complying with the provisions of this policy.

### Enforcement

Sanctions against employees who fail to comply with Organization policies shall be disciplined in accordance with Organization disciplinary procedures. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### ORG Policy

ORG defines acceptable use as using Organization Internet and email resources for **official purposes**. Incidental personal use is permitted so long as it does not violate any of the provisions of this policy and does not inhibit or interfere with official operations. All Users are responsible for discussing personal use issues with his/her local management prior to engaging in non-official activity. In all cases, an employee’s access to and use of this resource is up to the discretion of his/her local management.

### Internet Access

All Internet activity must be transmitted through firewalls to protect the security and integrity of the network infrastructure.

#### Internet Websites

##### Content Management

* + Creating or maintaining personal web pages or non-authorized official web pages using ORG Internet access is strictly prohibited.
  + Internet users may not modify, disable or create hyperlinks, graphics, text or any portion of information that exists on ORG websites.

##### Internet Usage Prohibitions

The following activities are prohibited while using ORG provided Internet and email:

* + Using a non-Organization sponsored email account to conduct Organization business.
  + Conducting any activity that runs contrary to any federal, state or local law or regulation.
  + Soliciting for personal gain or profit or engaging in any official activity that is not in support of sanctioned official activities.
  + Representing personal opinions as those of ORG.
  + Use of personal, free or any other non-Organization email accounts to store or convey ORG proprietary email or data.

##### Security Prohibitions

* + Connecting to systems in an attempt to specifically circumvent security measures that are in place.
  + Auto-opening or auto-executing file attachments.
  + Attempts by any employee or authorized person to gain unauthorized access to any computer, data or communications system.
  + The installation and use of non-Organization authorized encryption software.
  + Conducting any activity that runs contrary to any federal, state or local law or regulation.

#### Guidelines

* All personal postings to public forums shall include the standard disclaimer, “The opinions expressed here are mine and not those of my employer.”
* Publicizing information over the Internet must be approved by the Corporation’s communication group and must comply with ORG’s Data Classification Policy.

#### Data Transmission

Websites that protect data transmission by using SSL or SET encryption *security protocols* are acceptable for exchanging sensitive data via the Internet.

#### Internet File Exchange

* Files that are received or downloaded from the Internet must be decrypted and decompressed before using a virus scan.
* All non-text files (databases, spreadsheets, formatted word processing files, etc.) downloaded from non-Organization sources via the Internet must be screened using virus detection software prior to being installed.
* Internet users are not permitted to download, transmit or install software executables, pirated software, vulnerability scanning tools or inappropriate written/graphic material from the Internet.
* Information that might be considered Proprietary or Restricted by either ORG, one of its customers or an individual must be encrypted by approved methods prior to being transmitted, uploaded or posted to Internet sites.
* ORG’s materials (software, internal memos, policies, etc.) must not be posted on any publicly accessible computer which supports anonymous FTP or similar publicly accessible services.

#### Internet File Transmissions – Prohibitions

* Downloading or introducing any software that could compromise the security of integrity of the Organization’s firewalls, networks or systems (e.g., hacker tools).
* Downloading streaming audio or video files (e.g., MP3 files).
* Downloading any software or electronic files without having current virus protection measures in place and operating.
* Other inappropriate uses not related to the core official of ORG.

#### Internet Communications

* Internet users are prohibited from sending or posting information that is intended to harass, annoy, threaten, attack or alarm another person, group or official.
* Misrepresenting, obscuring, suppressing or replacing an Internet user’s id during an Internet session is prohibited.
* Internet official transactions may be confirmed by use of digital signatures or digital certificates. In cases where these computer identification methods are not available, letters of credit, third party references and telephone confirmations may be used. In any case, the use of digital signatures will not be construed as binding on the Organization.

#### Electronic Mail Usage

ORG’s electronic mail system must be used primarily for official communications. These communications must originate and terminate at the Organization owned, sponsored or managed email server accounts. All email communications must be monitored by network security to support operational, maintenance, auditing, security and investigative activities.

#### Email Accounts

Related email accounts and associated passwords will be provided to users to allow access to the Organization’s electronic mail system.

The accounts will be created and maintained by the individual or group(s) responsible for email management.

#### Personal Email Account Usage

Incidental personal use of the Organization’s email system is permitted provided that it does not inhibit nor interfere with official operations. It is a violation of this policy for users to misrepresent, obscure, suppress or replace any user’s id of the Organization on an *electronic communications system*.

Personally owned email accounts, free Internet email accounts or other non-Organization email accounts may not be accessed from within ORG’s networks.

#### Email Message Content

Profanity, obscenities or derogatory remarks must not be used in email messages. ORG media advertisements, Internet web pages, electronic bulletin board postings, etc., may not be transmitted via email without prior approval from local management.

#### Email Privacy

ORG reserves the unlimited right to access and review all email traffic transmitted through or received by the Organization provided equipment and services.

##### Users should expect no rights to privacy when using Organization computers, networks or associated services.

* Local IT security is authorized to monitor email on Organization information systems as required.

##### No right to privacy for email on Organization resources is implied.

#### Email Security Management

* Virus Protection - Attachments of inbound/outbound email must be scanned for computer viruses. It is a violation of this policy for users to replace, disable or modify anti-virus security software.
* Virus scanning will be performed using a current version of approved virus scanning software.
* Review of Email Communications - User email activity records may be reviewed at any time and without prior notice. The contents of any email message or email attachment may be recorded and/or intercepted for review as requested by senior management.

##### Employees or users of the Organization’s email system should have no expectations to privacy when using or transmitting email or files through the Organization’s network.

* + All email activity will be logged and subject to review on a regular basis.
  + Suspicious activity should be reported to management.

#### Email and Electronic Business Transactions

All contracts must be formed by paper documents prior to purchasing or selling via electronic systems.

#### Electronic Mail Usage – Prohibitions and Guidelines

This list of prohibitions and guidelines is intended to be used as examples and should not be viewed as comprehensive.

#### Prohibitions

* Intentionally receiving, accessing, transmitting or archiving illegal or sexually explicit material or material that promotes hate, violence or discrimination of any kind.
* Automatic forwarding of personal email into an Organization managed email account.
* Forwarding sensitive Organization data to external email accounts.
* Using ORG’s provided equipment and services to access Internet email accounts (Hotmail, Yahoo mail, etc.) to send, receive or store email messages and/or attachments.
* Sending electronic “chain letters” or unsolicited email (SPAM).
* Gambling.
* Auto-opening or auto-executing file attachments.
* Operating a personal mail list service on the Agency email system.
* Distributing non-official related “daily” messages.
* Soliciting for personal gain or profit or engaging in any official activity that is not in support of ORG’s sanctioned official activities.
* Using a non-Organization sponsored email account to conduct Agency official.
* Representing personal opinions as those of ORG.
* Other inappropriate uses not related to the core official of ORG.
* Conducting any activity that runs contrary to any federal, state or local law or regulation.

#### Guidelines

* All personal postings to public forums should include the standard disclaimer “The opinions expressed here are mine and not those of my employer.”
* Publicizing information over the Internet must be approved by ORG’s communication group and must comply with the Organization’s Data Classification Policy.

### Internet Intellectual Property Rights

ORG strongly supports strict adherence to software vendors’ license agreements. Duplicating software inconsistent with the vendor’s license policy is strictly prohibited.

The reproduction, transmission, republication or redistribution of words, graphics, etc., from a website must be approved by the original author/owner prior to use.

### Activity Monitoring

ORG reserves the unlimited right to access and review all traffic transmitted through or received by Organization provided equipment and services. Employees should understand that they have **no expectation of privacy when using Organization computers, networks or associated services.** This includes but is not limited to Internet email messages, web browser cache files, bookmark files, history logs or other information stored on or transmitted through Organization computers.

### Security Issues

Local IT security should be contacted immediately to report the actual or suspected loss, disclosure or theft of information transmitted via the Internet.

# Information Security Incident Management Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Security Incident Management Policy

### Purpose

To define ORG’s processes necessary to enable the rapid identification, reporting, management, mitigation and handling of information security incidents.

### Applicability/Scope

This policy applies to all employees, associates and contractors of ORG. All information systems owned or leased by the Organization are subject to this policy. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal law, state law, or regulatory requirements may preempt this policy.

### Roles and Responsibilities

The primary incident management responsibility is to identify and respond to the incident. In responding, responsibilities are to contain the scope of the incident, to limit additional exposure, and to mitigate damages (to the extent practical).

**ORG Chief Information Security Officer** – ultimately responsible for all information security incident management actions.

**ORG Cyber Emergency Response Team (CERT)** – a cross-functional team comprised of ORG’s Information Security Officer, system administrators, designated attorney, and other support personnel as appropriate.

### Enforcement

Failure to comply with the Organization’s information security policies shall result in sanctions in accordance with the appropriate ORG disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG shall implement an information security incident response capability that will identify and respond to a broad range of security incidents (People, Process, and Technology).

#### Definition:

**Information Security Incident** ―An actual event or the recognition of a potential event which might lead to the unauthorized access, loss, disclosure, modification, or destruction of ORG information or information assets, whether the circumstances are intentional or not.

#### Examples of security incidents are:

* + loss of service, equipment, or facilities
  + system malfunctions or overloads
  + human errors
  + non-compliances with policies or guidelines
  + breaches of physical security arrangements
  + uncontrolled system changes
  + malfunctions of software or hardware
  + access violations

#### ORG Information Security Incident Management Program shall include:

#### Security Training

ORG shall provide its workforce with training on how to identify and report security incidents.

#### Incident Detection

ORG shall establish clear procedures for collecting, analyzing, and reporting security incident data. The integrity of all data relating to an event must be preserved as possible evidence in legal proceedings. Computer forensic procedures must be documented and followed carefully to assist in any investigation.

#### Cyber Emergency Response Team (CERT)

ORG shall develop a cross-functional incident response team to handle a wide variety of incidents. The roles and responsibilities of all team members shall be clearly defined. The CERT shall be adequately staffed and trained to handle a specific range of incidents. Since incidents may be far-reaching, the incident management team may include internal and external entities.

#### Organization Protocols

Security incidents may occur across network boundaries. Protocols will be established and documented for handling of incidents involving cross-boundary issues.

#### Incident Reporting

A communication plan is essential for reporting and managing incidents. ORG shall develop and implement a comprehensive communication plan that details internal communications and escalation procedures that are to be used by the CERT. Security incidents shall be reported to ORG’s Chief Information Security Officer within 30 minutes from the time the incident was discovered.

#### Impact Assessments

ORG defines and documents procedures for evaluating the impact of security incidents. Assessments may be required at various stages of the incident life cycle to assist management in deploying an appropriate risk management strategy.

#### Incident Handling Procedures

Detailed response procedures shall be developed and implemented for incident management. ORG staff assigned to the CERT must be familiar with these procedures.

#### Documentation

All security incidents shall be thoroughly documented. Incident documentation should describe the incident, pertinent times, and affected areas that may be subject to subsequent investigation. The incident report shall indicate who was notified and subsequent actions.

#### Record Retention

ORG shall maintain security incident logs and associated documentation for a minimum of three years following the discovery of an incident or until an investigation is completed.

#### Post-Incident Analysis

Post-incident analysis creates an opportunity for feedback that may improve existing policy, processes, or related procedures. An analysis shall be performed to evaluate the actions taken surrounding each security incident and include suggestions to minimize future incidents.

#### Emergency Planning

Incident management procedures shall include specific criteria for declaring an *Emergency* and corresponding reactions. Normally, if an incident occurs that impacts the safety of ORG personnel or offices or results in a situation where ORG services may be interrupted for an extended period, the incident should be declared an *Emergency*.

### Media Relations

Security incidents are likely to result in media attention when made public. ORG shall develop a crisis management plan to handle such contingencies.

# Password and Authentication Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Password and Authentication Policy

### Purpose

The purpose of this policy is to establish password and account *authentication* requirements for ORG.

### Applicability/Scope

This policy applies to all information systems owned or leased by ORG. This policy also applies to all employees, associates and contractors of the Organization. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

**ORG Chief Information Security Officer** – ORG’s Chief Information Security Officer will implement and manage the policy.

**Users** – responsible for reading and complying with the provisions of this policy.

### Enforcement

Failure to comply with ORG’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG shall implement strong password and access authentication procedures for both internal and external users.

#### Password Generation and User Authentication

Access to ORG’s information stored on desktop and portable computer devices and other network infrastructure devices must be protected by User ID and *strong password* or *strong authentication*. Password administration groups such as Help Desk administrators, etc., are responsible for the creation, maintenance, and implementation of User IDs, passwords and authentication.

#### Passwords – Creating New

All platforms and services permitting access must use *strong passwords*.

User account passwords must contain a minimum of eight (8) characters consisting of a mix of alpha, numeric and/or special characters. Upper and lower case character combination should be used in the password for case sensitive systems.

#### Examples for creating strong passwords

* + Insert a number or special character in the middle of a word, e.g., “Da1%1as”
  + Separate small words with numbers and/or special characters, e.g., “hen#Egg”
  + Alter the ordinary spelling of a phrase by substituting numbers for or alphabxxxxx for entire words, e.g., “You are too envious” becomes “UR2nvus”
  + Create a phrase that can be squeezed into eight (8) characters minimum – similar to a vanity license plate number, e.g., “avp@att”
  + Easily guessed passwords are strongly discouraged. The following are examples:
    - Month and year combinations
    - Account names
    - Names of people
    - Any words found in a dictionary
    - [Organization Name] names or abbreviations
    - Brand names
    - Nicknames
    - College and professional team names and nicknames

#### Password Expiration

Passwords should have a maximum expiration age of ninety (90) days. Automated password expiration prompts should be implemented to remind users when to change their password. New passwords should not be based on any of the last four previously expired passwords.

#### Default Passwords

All operating system default passwords must be replaced with strong passwords.

#### Password Administration / Account and Password Reset

Documented procedures must be established to authenticate users on password reset requests.

Password administration groups, or groups acting on their behalf such as help desks, must have documented procedures in place to authenticate users on password reset requests. **Password administration groups may not ask for the user’s password**. Password administration groups must never retain or document user passwords except to notify the user of a temporary password for an account which requires a password change upon initial logon.

#### Password Sharing

***Users are prohibited from the sharing of passwords***

#### Automated Password Administration

* + Automated password reset must generate a temporary password and the system must require the user to immediately change their password upon next logon.
  + Automated password hints may be provided as long as no two of the following are combined in the same email: username, password, application link.
    - Password hint secret answers must be stored and handled in the same manner a password.
    - If the user provides their secret answer, the password is emailed to a pre- registered address.

#### Private Connection Authentication Methods

If it is not feasible to change internal system passwords every ninety (90) days, IP restriction is acceptable. It is recommended that 90-day password rotation be implemented in addition to IP restriction.

#### Account Management

##### Account Lockout

Failed logon attempts must be limited to three (3) before the system or application initiates a *lockout*. The appropriate password administration group must be contacted to unlock the account and reset the password.

##### User’s Account Storage

Passwords must be stored and transmitted using encryption.

##### Screen Locking

Systems left unattended for twenty (20) minutes or longer must be protected with a screen saver password.

All systems should be configured to automatically start the screen saver feature within a twenty (20) minute period of inactivity.

##### Users are required to use the manual lock feature whenever the system is left unattended.

This immediately invokes the password protected screen saver and overrides the twenty

1. minute automated setting.

For use exclusively by ORG’s employees and approved associates

* + Password protected screen savers should be used on all systems that support this feature.
  + Passwords for the screen lock should be consistent with this policy’s password quality requirement.

#### Disabled and Reassigned Accounts

Accounts assigned to employees who have terminated employment with ORG must be disabled or reassigned (with changed passwords) no later than the last day of employment.

If the terminating employee had administrative accounts and/or accounts with *Superuser*, supervisory, root or system admin privileges, those passwords must be changed immediately.

Accounts of transferred employees must be disabled or reassigned (with changed passwords) no later than thirty (30) days from the effective date of the transfer. This includes administrative accounts and accounts with *Superuser*, supervisory, root or system admin privileges.

#### Account Log Management

All applications, computing platforms and network components, which support account logging, must have account logging enabled.

Review of the *account log files* for security relevant events must be conducted on a regular basis.

Audit trails should be retained as specified in ORG Records Retention Policy. To reduce impact on individual platform storage requirements, archiving processes should be created to automatically transfer account log files to a storage file on a periodic basis.

Any inconsistencies or security relevant events identified in the audit log should be reported to local IT security for review. If there is suspicion that an account, password or system has been compromised, details of the incident must be immediately reported to the system administrator and the local incident response plan shall be implemented.

#### Default Passwords

###### All operating system default passwords must be replaced with strong passwords.

# Anti-Virus Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Anti-Virus Policy

### Purpose

The purpose of this policy is to identify requirements for the protection of all ORG’s information systems from damage from viruses and similar malicious software.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

**ORG’s Chief Information Security Officer** – ORG’s Chief Information Security Officer will implement the policy and manage the policy.

**Users** – responsible for reading and complying with the provisions of this policy.

### Enforcement

Failure to comply with the Organization’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG shall ensure the protection of its information systems by implementing the following protections:

#### Personal Computing Equipment

* + Information Technology (IT) approved anti-virus scanning software must be installed on the system.
  + E-mail attachments must be decompressed and scanned.
  + Users are prohibited from adding, disabling, modifying or removing anti-virus software.
  + Users are prohibited from eradicating *viruses* from their systems without the assistance of the local desktop support department.
  + ORG prohibits the user from installing, configuring, importing or using software that conflicts or inhibits the performance of agency business applications, security software or devices.
  + Local IT management makes the decision of the type of anti-virus software that will be implemented. The software must have the capability of periodic updates, notification of virus alerts, be endorsed by best business practices.

#### Mail Servers

All mail servers, regardless of operating system, must pass all e-mail through an approved anti- virus scanning engine that is capable of analyzing e-mail for viruses prior to delivery. In addition, the anti-virus software must be capable of validating attachment *MIME types* and stripping prohibited or invalid attachments.

#### Anti-Virus Administration

##### Signatures

* Server virus signatures must be updated at least once per business day.
* Desktop virus signatures must be updated at least once per week. The support center is responsible for providing instruction on regularly updating virus software whenever such cannot be provided globally.

##### Emergency Virus Alerts

* Should an endorsed authority issue an emergency virus alert, the desktop support department is responsible for updating anti-virus signatures immediately.
* Users shall not transmit unauthorized virus/security alerts.

##### Virus Response

* Should a virus be suspected or detected, the user must cease using the equipment and escalate to their appropriate support center immediately.
* Should a virus be detected within the network, the support center will immediately notify appropriate management of the issue and assist in preventing further infection.
* Upon detection of a virus, the local incident response plan shall be implemented.
* Upon detection of a virus, the device should be disconnected or isolated from the network immediately.

##### Configuration

* Anti-virus configurations must be set to scan “all files”.
* Logs must be enabled to record all desktop or server virus related activity.
* Logs must be periodically reviewed for virus detected, removed or quarantined situations.

# Information Security Awareness and Training Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Security Awareness and Training Policy

### Purpose

The purpose of this policy is to specify requirements for [Organization Name] information security awareness and training.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

ORG’s Chief Information Security Officer establishes security training and awareness policy and baseline security training standards.

##### Chief Information Security Officer

* + Conduct the initial assessment of workforce members security training.
  + Implement the Organization’s training materials and periodically evaluate information security training needs.
  + Ensure that security awareness presentations are developed to meet specific requirements.
  + Implement the General Security training of users.
  + Provide System-Specific Security training for all users of the Organization’s information systems based on the individual’s roles and responsibilities for that information system.
  + Provide opportunities for Professional Education training for IT security professionals to allow the workforce member to fulfill the security responsibilities of their position.

### Enforcement

Failure to comply with ORG’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG shall develop and implement a training program consisting of information security awareness presentations, general security training, system-specific security training, and professional security education applicable to each workforce member.

#### Information Security Training Requirements:

**ORG shall develop and implement an information security training and awareness program.** This program shall include training plans to develop, implement, and deliver the training to each ORG workforce member. The purpose of the program is to assure that ORG workforce and third parties receiving, processing, or storing ORG information are fully aware of their security responsibilities and know how to fulfill them.

In addition to reflecting all security requirements required by the Organization, as well as state and federal regulations, the security training requirements shall reflect specific information risks of ORG and provide flexibility to accommodate future technologies.

**ORG shall develop Information Security Training Plans** for General Security Training, System-Specific Security Training, and Professional Security Education. Plans shall be reviewed on an annual basis to consider the impact of any new technology or risk management decisions implemented during the previous year. These plans shall include the following elements, as applicable:

* + Goal
  + Scope
  + Training participants; e.g., training, support, business
  + Approach (i.e., train the trainer or train the end users)
  + Methodology (i.e., face-to-face vs. audio vs. self-study)
  + Deliverables (i.e., training plan, reference manual, video track, etc.)
  + Training Objectives
  + Schedule
  + Registration
  + Review and Evaluation

**ORG shall develop and maintain a communications process** for the purpose of describing any new information security program information, routine security information (bulletins), or any other security items of interest.

**ORG shall develop and maintain pertinent materials for use Information Security Awareness presentations.** Source material for security awareness presentations may be obtained from daily news websites, e-mail advisories, self-assessments, internal audits, and/or periodicals. Security awareness presentations or messages may be delivered through e-mail, posters, pop-up messages, web-based sessions, “brown-bag” seminars, or other media depending on the complexity of the message. Security awareness messages may also be delivered through “sign-on warning banners” at logon/access points to computer information systems.

**ORG shall develop material for General Security Training.** All ORG workforce members shall receive General Security Training and regular updates in organizational policies and procedures before being granted access to the Organization’s information resources.

General Security Training shall include acceptable use of information system resources, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, e.g., log-on procedure, procedures for guarding against malicious software, password management, and recognizing and reporting security incidents.

**A summary of the Information Security policies** must be formally delivered to and accepted by all ORG workforce members including employees, contractors, or volunteer staff, either in paper format or electronically, prior to being granted access to the Organization’s information resources.

ORG must ensure workforce members have training and supporting reference materials sufficient to allow them to protect the Organization’s information resources.

For each Information System used, ORG will develop and provide System Specific Security Training that is mapped to job functions with specific performance-based training requirements.

When workforce member job responsibilities change, associated Information Security needs must be re-assessed by the workforce member’s immediate supervisor and associated training provided to reflect the change in job responsibility.

**Provisions for annual training of Security Officials** shall be prioritized in the Training Program to include at a minimum the topics covered by all the Organization’s security policies, i.e., the ISO 17799 standard. Annual training shall also include education on the latest potential information threats and protective measures.

**Provisions for management training** shall be prioritized in the Training Program in order to provide education and training on security management issues including but not limited to risk management, incident response, and compliance management.

**Provisions for Information Technology (IT) staff training** shall include training in Information Security threats and safeguards, with the extent of technical training relative to the jobholder’s individual responsibility. Where IT staff may change jobs, their Information Security needs must be re-assessed, and new training provided as a priority.

**ORG shall monitor training requirements, compliance, and effectiveness**. In order to provide enterprise-wide analysis on education initiatives, key information to be captured shall include courses, dates, audience members, costs, and sources.

**ORG Security Training programs shall provide formal evaluation and feedback mechanisms** to address objectives initially established for the training program. Methods for evaluation and feedback may include but are not limited to evaluation forms/questionnaires, focus groups, selective interviews, independent observations, and formal status reports.

# Information Systems Access Control Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Systems Access Control Policy

### Purpose

The purpose of this policy is to specify security requirements for access to the Organization’s information and information systems.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

The following key roles and responsibilities have been identified for this policy:

**Data****Owner** – person responsible for protecting the information.

**Manager** – person responsible for ensuring operations security.

**System Administrator** – person responsible for configuring and maintaining the information processing systems in the production environment as well as managing user accounts.

**User** – an individual that has been assigned an account and has been granted access to specific information resources.

### Enforcement

Failure to comply with ORG’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG information resources shall be strictly controlled to prevent unauthorized access to the Organization’s information and information systems.

#### Access Control Requirements:

**Access Rights** – The System Owner shall ensure that all access rights or privileges granted are documented and safeguarded as appropriate.

**Access Controls** – Access controls shall be implemented to protect information resources. Only management-approved access control software may be used to restrict access in the production environment. Access to security software shall be limited to security administrators and authorized personnel. Logical access controls shall be implemented on applications, databases, and database management systems (DBMS). These controls will have the effect of limiting access to data based on the *principle of least privilege*.

**Login Attempts** – The number of consecutive attempts to enter an incorrect password shall be limited to prevent password guessing attacks. After three unsuccessful attempts to enter a password, the user attempting entry shall have the account:

* + Suspended until reset by a system administrator.
  + Temporarily disabled.
  + If dial-up or other external network connections are involved - disconnected

**Multiple On-line Sessions** – No ORG user will be allowed to conduct multiple simultaneous on-line sessions without management approval.

**Automatic Log-Off Process** – If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for a significant period of time (typically 20 minutes) the system must automatically either darken the screen or use an acceptable screen saver image and suspend the session. Re-establishment of the session can take place after the user has logged back on to the system.

**Emergency and Temporary Access** – Emergency and temporary access authorization shall be strictly controlled and documented. Emergency access is immediate and is typically granted to correct a problem that if not corrected may result in further damage. Emergency and temporary access authorizations shall be:

* + Documented, approved and maintained on file by the appropriate managers.
  + Communicated to ORG’s Chief Information Security Officer.
  + Automatically terminated after a predetermined period.

**Authentication Methodologies** – ORG shall use only approved technologies to accomplish user and computer-to-computer authentication. These technologies may include tokens, smartcards, digital certificates, or other access control mechanisms selected on the basis of acceptable risk.

**Third-Party Network Connectivity** - All third party (e.g., business associates, vendors, etc.) network connection requests shall be evaluated and approved by management. The connection request will typically contain the following items:

* + List of ORG’s resource(s) that must be accessed and for what purpose.
  + Sensitivity or criticality of the information resource(s) involved.
  + Hours of access start date, and end date for connection requested.
  + Estimated number of users.
  + Detailed description of use.
  + Communication protocol(s) hardware, software, and any special requirements.
  + Request for information resource access forms.
  + Connectivity description.
  + Connectivity risk assessment.
  + Completed business associate access request form.
  + Authorized third-party network service(s) to be used for the connection.
  + Escalation procedures with contact information.
  + Performance requirements.

##### Third party access shall be limited to only those services and/or devices that are needed to perform the required business function.

**Remote Access** – ORG personnel working off-site shall only use management-approved computer software, hardware, and virus protection software when working on ORG business. Remote access to the Organization’s network and resources shall be permitted upon authentication for authorized users. Additionally, the following controls shall be implemented:

* + Limiting the number of Remote Connections - The number of users who can access into the system from remote locations shall be limited, and justification for such access has to be documented and approved by Data Owners. Managers and Data Owners must approve access to the Organization’s resources from remote locations. If a remote access system utilizes dial-up modems, they must be expressly configured to provide secure network access.
  + Monitoring - All dial-in account activity shall be monitored, and if a dial-in account is not used for a period of 30 days, the account will expire.
  + Review of Access Logs - Logs of all inbound access into the Organization’s internal network must be reviewed periodically by the system administrator (at an interval determined by operations management) and any problems reported immediately for subsequent action.

**Access by Unauthorized Personnel** – ORG shall implement controls to ensure that unauthorized personnel do not establish dial-in connections in order to gain access to the Organization’s information resources.

**Use of Virtual Private Networks** – ORG VPN solutions shall utilize approved software and contain an end-to-end security strategy.

**Remote Management** – Management must approve the use of all remote administration, maintenance software, and security controls that are deemed necessary to protect the security of the information resources.

# Information Systems Asset Management Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Systems Asset Management Policy

### Purpose

The purpose of this policy is to identify requirements for the protection of all information resources, including workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, and software.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

**Information Owners** – responsible for inventorying, tracking, and protecting the Organization’s information resources that they own.

**Information Custodians** – responsible for assisting information owners with inventorying, tracking, and protecting the Organization’s information resources in their care.

**Users** – responsible for exercising due diligence in protecting information resources entrusted to them, and immediately reporting the loss, theft or damage of any of the Organization’s information resources.

**Managers** – responsible for ensuring their employees understand their responsibilities regarding protection of information resources.

**[Organization Name] Information Security Officer** – responsible for auditing to ensure that information assets are being tracked and managed in accordance with this policy on an annual basis.

### Enforcement

Failure to comply with the Organization’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

ORG Management will ensure that all information assets are tracked and managed appropriately.

Upon receipt, the Organization’s information assets are to be added to a comprehensive

*Information Asset Inventory* and assigned an asset number.

For each information asset, ORG will track at least the following information:

* + The brand, model, and type of asset.
  + The serial number and ORG Asset Number.
  + The person to whom the asset is assigned.
  + The location of the asset.
  + Any maintenance agreements for the asset.
  + The date of receipt of the item.
  + The date the record was last updated or inventoried.

Upon disposal of an information asset, ORG will track the date of disposal, the method of disposal (e.g., transfer, destruction, donation, etc.), and the name of the new owner (if there is one).

Periodic inventories are to be performed to verify records and account for all information asset. Each asset is to be inventoried at least annually.

# Physical & Environmental Security Management Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Physical and Environmental Security Management Policy

### Purpose

The purpose of this policy is to specify requirements for the minimum level of physical and environmental security of all [Organization Name] facilities housing [Organization Name] information and information assets.

### Applicability/Scope

This policy applies to all information systems owned or leased by [Organization Name]. This policy also applies to all employees, associates and contractors of [Organization Name]. [Organization Name] reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### 

### Roles and Responsibilities

Key roles that affect the implementation of this policy are:

**Facility Managers** – All [Organization Name] facilities shall have a Facility Manager. This function may be outsourced (e.g., with leased buildings) or there may be a [Organization Name] representative assigned to one or more buildings.

**Visitor Control Staff** – All [Organization Name] facilities shall have adequate staff assigned to implement visitor control procedures.

**Safety Officers** – Each [Organization Name] facility shall have designated emergency evacuation personnel that will ensure emergency evacuation routes are clearly posted, emergency response procedures documented and tested, and copies are distributed to all building personnel.

**Network and Computer Operations Management** – All network and computer operations managers shall be responsible for the physical security of the hardware and software asset assigned to them.

**Managers** – All Managers responsible for operations shall ensure that adequate physical security is provided to protect asset.

**Contracts Administration** – Contracts administration shall ensure that all business associates and outsourced entities provide a comparable level of security as defined in [Organization Name] policies. [Organization Name] contracts shall contain the necessary security provisions to require protection of sensitive and critical information by the vendor.

**Employees/Contractors/Volunteers** – All employees / contractors / volunteers have an obligation to protect [Organization Name] assets.

### Enforcement

Failure to comply with [Organization Name] information security policies shall result in sanctions as determined by the appropriate [Organization Name] disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact [Organization Name] Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

[Organization Name] shall implement physical and environmental security controls to protect people, property, and information resources.

#### Physical and Environmental Security Requirements:

##### Physical Access Control (Internal/External)

Facility Managers are responsible for providing adequate physical security in the workplace. [Organization Name] shall implement physical access control procedures at designated points in order to limit access.

##### Visitor Control

[Organization Name] offices shall implement visitor control procedures that include the following:

* + Visitor log maintenance
  + Sign-in/Sign-out procedures with time recorded
  + Temporary badge with tracking number properly displayed
  + Visitor escorted at all times

##### Work Area Security

The employee/contractor work area shall be properly secured to protect both sensitive and critical information and ensure privacy. Workstations shall be placed in a location that protects the confidentiality of data. Documents and media shall be stored in accordance with their classification status.

##### Physical Inventory Control

[Organization Name] shall maintain a formal inventory of all information assets. Information asset inventories shall be performed regularly or as significant changes occur.

##### Power Protection

All sensitive and critical information processing systems shall be protected by an Uninterruptible Power Supply. All critical applications shall be configured to switchover to an alternate power source immediately upon loss of power.

##### Physical Security of Telecommunications Resources

Telecommunications lines and equipment shall be protected to ensure both availability and the confidentiality.

##### Physical and Environmental Security of Off-Site Storage Facilities

All off-site storage facilities shall be afforded the same level of protection as that required within [Organization Name] Offices and those sites will be included in all audit/ compliance reviews.

##### Controls for Environmental Exposures in the Workplace

The [Organization Name] shall protect information asset by implementing controls that to protect from environmental hazards. These controls include but are not limited to temperature and humidity controls, smoke detectors, and fire suppression systems.

##### Mobile Computer Security

Mobile computers and other portable information systems shall be issued only to authorized personnel and those personnel shall be responsible for both the physical security of the device and protection of the information stored on the device. At a minimum, all laptops shall be password protected to limit access to its authorized user; where possible, all portable information system hard-drives will be encrypted.

The use of PDA’s to access and log personally identifiable information within [Organization Name] is generally restricted because of the inherent risk of loss. However, PDA’s

shall be issued only under certain circumstances (i.e., critical need) and the use must subsequently meet the approval of both [Organization Name] Privacy and Information Security Officers.

##### Property Control

Any movement of information, software media, hardware, or physical asset (computers/ servers) shall be strictly controlled. Only authorized personnel shall be permitted to take [Organization Name] property off the premises and they shall be responsible for protecting the property and controlling its use while in their possession.

##### Removable Storage Devices

The use of removable storage devices (e.g., USB Flash Drives, CD R/W drives, Zip Drives) shall be permitted at [Organization Name] facilities, but strictly controlled.

##### Safety and Emergency Procedures

The [Organization Name] shall regard personnel safety as a high priority and take the necessary steps to ensure a safe workplace. Emergency procedures shall be written, maintained, and tested periodically at each facility.

##### Emergency Equipment

The [Organization Name] facilities shall contain emergency equipment (e.g., emergency lighting, fire extinguishers) to establish an adequate level of safety for those working within a facility. This equipment shall be inspected annually to ensure its operational capabilities.

##### Incident Management

[Organization Name] shall implement a process that addresses all physical security incidents. Refer to the Information Security Incident Management Policy for details.

##### Disposal of Sensitive Documents, Media, and Equipment

Sensitive documents, media, and equipment must be disposed of in an approved manner that protects the confidentiality of the information printed or stored. [Organization Name] Information Security Officer shall develop procedures for the following:

* + Disposal of sensitive documents
  + Destruction of computer equipment that may contain sensitive information
  + Sanitization (i.e., Object Reuse) of equipment that might be sold or transferred to other organizations
  + Destruction of all types of magnetic media

##### Physical Site Inspections

A physical security inspection shall be performed periodically by [Organization Name] Information Security Officer to ensure policy compliance.

#### Potentially Related Procedures (Not included with this document)

Building Records Management Procedure Facility Perimeter Protection Procedure Perimeter Security Controls Testing Procedure

Perimeter Security Controls Update – Change Management Notification Parking Area Security Protection Procedure

Parking Area Security Controls Testing Procedure Physical Access Control Procedures (External) Access Point Control Procedure

Facility Physical Access Review Procedure Physical Access Provisioning Procedure Physical Access Termination Procedure Visitor Access Control Procedure

Visitor Log Review and Approval Procedure Missing Visitor Badge Tracking Procedure

Data Center Control Procedures

Technical Infrastructure Physical Security Controls Procedure Environmental Security Procedure

Environmental Controls Test Procedure Environmental Controls Monitoring Procedure Power Protection Controls Test Procedure

Power Protection Controls Monitoring Procedure Protection of Supporting Utilities Procedure Supporting Utilities and Redundancy Test Procedure Off-Site Storage Facility Physical Security Procedure Off-Site Physical Security Controls Testing Procedure Off-Site Environmental Controls Testing Procedure Physical Security of Mobile Devices Procedure Removable Storage Device Procedures

Emergency Equipment Procedures

Disposal of Sensitive Information Procedures

#### Potentially Related Forms & Logs (Not included with this document):

Vendor Contract Requirements Review and Approval Form Vendor Contact Number List

Facility Security Management Report Form Perimeter Security Controls Inventory

Perimeter Security Controls Testing Review and Approval Form Perimeter Monitoring Log

Perimeter Monitoring Security Incident Reporting Form Perimeter Monitoring Log Review and Approval Form Access Control Point Authorization List

Access Controls Monitoring Checklist

Access Controls Monitoring Review and Approval Form Physical Security Incident Notification Form

Physical Access Change Management Notification Form Visitors Log

Visitor Badge Inventory

Asset Inventory Physical Safeguards

Network and Power Cable Security Standards

Network and Power Cabling Review and Approval Form Physical Internal Segregation Controls

Internal Security Boundary Diagram Internal Segregation Controls Inventory Physical Privacy Safeguards Inventory Environmental Controls Inventory

Environmental Controls Testing and Monitoring Review and Approval Form Power Protection Controls Inventory

Power Protection Controls Testing and Monitoring Review and Approval Form

Critical Asset Physical Security Controls Critical Asset Inventory

Supporting Utilities and Redundancy Inventory Property Removal Authorization Form Property Inventory Review and Approval Form Removable Storage Device Inventory

Storage Device Removal Authorization Form

# Information Systems Operations Management Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Information Systems Operations Management Policy

### Purpose

The purpose of this policy is to identify security requirements for [Organization Name] information systems operating environment.

### Applicability/Scope

This policy applies to all information systems owned or leased by [Organization Name]. This policy also applies to all employees, associates and contractors of [Organization Name]. [Organization Name] reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

The following key roles and responsibilities have been identified for this policy:

**Data Owner** – person responsible for protecting the information

**[Organization Name] Information Security Officer** – person responsible for ensuring operations security

**System Administrator** – person responsible for configuring and maintaining [Organization Name] information production environment, as well as managing user accounts

**IT Operations Personnel** – individuals responsible for supporting [Organization Name] Information Systems Operations

**Users** – individuals authorized to access specific [Organization Name] information resources

### Enforcement

Failure to comply with [Organization Name] information security policies shall result in sanctions as determined by the appropriate [Organization Name] disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact

[Organization Name] Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

[Organization Name] Office of Information Technology shall establish administrative, physical, and technical controls intended to create a basic level of information security for the production environment.

#### Information Systems Operational Security Requirements:

**Information Systems Governance** – Operations Management shall adopt and follow an approved Information Systems Governance methodology. A formal Information Systems Governance approach ensures there is top-down management along with auditable control objectives for compliance checking.

**Information Systems Operations Staff** – Information Systems Operations shall be adequately staffed to ensure the availability of applications and systems, as well as protect the confidentiality and integrity of the data being processed. Staffing requirements include

* + Skill level – the skill level of each technician working in the production environment shall be such that basic tasks may be performed efficiently and effectively, with minimal disruption in service.
  + Cross-Training Staff – Cross-training is necessary to ensure availability. In designing workflow, management must ensure that duties are assigned so as to not lead to conflict s of interest (e.g., an individual implementing a task having final review or approval of that work effort).
  + Job Descriptions – Each member of the information systems operational staff must have clearly documented job descriptions that explain their exact role and the required level of systems and applications access.

**Information Systems Technology** – All information systems and applications in the production environment shall be supported and maintained, at a minimum, in accordance with manufacturer’s guidelines. All systems and applications shall be evaluated, prior to acquisition and again prior to implementation, to ensure an

appropriate level of security is provided according to the classification of information being processed or stored by those systems and applications. Some legacy platforms may require additional controls beyond those initially provided by the manufacturer or developer in order to achieve an acceptable risk level. Systems and applications that are not capable of providing a minimal level of security according to the classification of data being processed or stored must be replaced.

**Information Systems Processes and Procedures** – All processes and procedures associated with managing, maintaining, and operating [Organization Name] information systems shall be documented and updated annually using a formal document control system. Such processes and procedures shall include but not be limited to the following:

* + Configuration Management
  + Inventory Control
  + Change Control
  + Patch Management
  + Backup and Restoration
  + Viruses and Malicious Code Protection
  + Object Reuse
  + System and Application Access

**Operations Documentation and Escalation** –Documentation and operations procedures of supporting vendors or other organizations shall be available to [Organization Name] information systems support personnel as appropriate. Escalation procedures and contact lists for supporting vendors or other organizations shall be posted in the operations area and properly updated. Helpdesk operations shall be implemented wherever possible to minimize downtime.

**Data Classification** – All data in transit or storage within [Organization Name] shall be reviewed to determine its level of sensitivity and criticality. Upon review, all data shall be properly labeled, and controls implemented to protect the data against unauthorized access or disclosure.

**Physical and Environmental Security** – Physical and environmental security controls shall be implemented to protect the operations environment.

**User Access and Auditing** – Access to information resources should be based upon a “need to know’ or a “need to use,” according to [Organization Name] Access Control Policy.

**Assigning User Privileges** – A formal authorization process shall be established to assign privileges for each [Organization Name] user and to determine what specific information resources may be accessed. This process will be strictly controlled and require the approval of management for any changes.

**Establishing User Accountability** – Each information processing system shall be configured to provide individual user accountability, no general or group access machines.

**Information Systems Auditing** – All sensitive and critical information systems shall be audited on a regular basis. Information systems auditing priorities shall be based on incident history, application criticality, and sensitivity of information.

**Information Security Risk Management** – [Organization Name] Information Security Officer shall develop and maintain a documented Information Risk Management program that will include:

* + Risk assessment
  + Risk treatment
  + Management decision making
  + Risk re-assessment
  + Monitoring and reviewing of risk profile
  + Information security risk in the context of Organization governance
  + Compliance with other risk-based standards and regulations

**Controls** – Administrative processes and procedures, physical access controls and technical controls shall be implemented to ensure the confidentiality, availability, and integrity of all information in the production environment.

**Incident Management, Alerts, and Notifications** – Security alerts and notification mechanisms shall be implemented.

**Contingency Planning** – Contingency plans shall be written and maintained to ensure the availability of business-critical information systems and operations in the event of loss of service. Alternative site operations shall be developed as part of a formal disaster recovery plan.

#### Potentially Related Procedures (Not included with this template)

Equipment Start-up and Shutdown Procedure Information Systems Equipment Maintenance Procedure Data Center Operating Procedures

System Administration Procedures

Data Handling / Backup Procedures Security Administration Procedures Error Handling Procedures

System and Audit Logging Procedure

#### Potentially Related Forms & Logs (Not included with this template)

Information Systems Equipment Inventory Equipment Maintenance Approval Form Support Contacts Documentation

System Event Log

Master Asset and Equipment Testing and Maintenance Schedule Application Audit Log

Application Audit Log Review and Approval Form

System Event Log Review and Approval Form

# Network and Telecommunication Security Management Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  |  |
|  |  |  |
|  |  |  |

## Network and Telecommunication Security Management Policy

### Purpose

The purpose of this policy is to specify the Organization’s security requirements for data and telecommunications networks, as well as the information transiting or stored in such systems.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

Responsibility for providing an adequate level of network and telecommunications security within ORG lies with ORG’s Chief Information Security Officer.

#### The following key roles and responsibilities have been identified for this policy:

**ORG Chief Information Security Officer** – provides security oversight and guidance to management. Involved in Security Incident reporting and responsible for security policy compliance.

**Data Owners/Custodians** – responsible for maintaining the data in accordance with its data classification.

### Enforcement

Failure to comply with the Organization’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### The ORG Policy

ORG shall implement network security controls necessary to protect network asset and information owned by the Organization.

#### Network and Telecommunications Security Requirements:

**Network Architecture** – ORG shall design, implement, and maintain all network architecture with preventative, detective, and corrective security controls. At a minimum, a layered architecture will be employed with the intent to isolate attacks and limit damage to the network environment.

**Network Addressing** – All network names and addresses shall be managed and approved by a central addressing authority within the Organization. Internal network addresses shall be considered sensitive data and not be distributed to unauthorized personnel.

**Network Services and Protocols** – Only management-approved network services and protocols will be implemented. All non-authorized protocols and services will be removed and/or disabled.

**Network Perimeter** – A clearly defined boundary shall be established to control traffic between the Organization’s information resources and external entities. All inbound and outbound network traffic shall pass through appropriate access control devices prior to reaching the Organization’s information resources. ORG’s network shall monitor for and disconnect any traffic not passing through the appropriate access control points.

**Network Availability and Redundancy** – The Organization’s network design shall provide adequate redundancies to reduce the likelihood of a single point of failure.

**Network Integrity** – The Organization’s network shall establish a system of controls to safeguard the data, detect and correct transmission line errors, and ensure message integrity throughout the system.

**Network Security Management** – All ORG networks shall implement a security management function that includes network configuration management, continuity of operations, and manages network audit capabilities.

**Network Security Incidents** – All network incidents shall be reported immediately using the Organization’s security incident reporting procedures. All network malfunctions are to be considered potential security incidents and reported.

**Physical Security** – The Organization shall protect all network equipment from unauthorized access.

**Network Technology** – The Organization shall implement and properly configure network security technology to protect sensitive information flowing across the network.

**Network Switching Devices** – Network management shall be responsible for approving the selection and configuration of all network devices such as routers, hubs, and switches deployed.

**Network Servers** – The Organization’s servers shall be protected commensurate with the level of sensitivity and criticality of the information and function that they perform.

**Network Firewall** – Only ORG approved traffic and services shall be permitted through the Organization’s firewall(s).

**Virtual Private Network (VPN)** – All VPN solutions shall be designed to provide authentication, authorization, encryption, and auditing capabilities. ORG’s VPN solutions shall utilize approved software and maintain an end-to-end security strategy.

**Intrusion Detection Systems (IDS)** – Due to the significant risk of internal and external intrusion from unauthorized persons, intrusion detection systems shall be implemented. ORG’s Chief Information Security Officer shall be responsible for the IDS design and implementation.

**Content Filtering** – The Organization’s Network shall provide content filtering to minimize SPAM, the risk of damage occurring from receiving malicious email attachments or downloading viruses, worms, spyware or other malicious code.

**Email Security** – Electronic mail is critical to performing the Organization’s Operations and delivering needed services to its constituent base. ORG shall implement security processes and solutions that protect:

* + Mail Servers – hosts that deliver, forward and store mail.
  + Mail Clients – software that allows users to read, compose, send and store email messages.

NOTE: In general, all sensitive ORG information transmitted over the external network must be securely encrypted. Email shall be retained in accordance with the Organization’s guidelines.

**Third Party Network Connection Security** – All third-party connections shall be evaluated by considering access, administration, confidentiality, and monitoring requirements. Network services provided over third-party connections shall be limited to those services necessary to perform the required function. Third-party access shall be limited to those services and/or devices that are needed to perform the required business function.

**Telecommunications Security** – All ORG telecommunications lines shall be secured in a manner that ensures availability and prevents tampering. The Organization shall provide the following:

* + Intrusion Detection – ORG shall implement a method to detect intrusion activity on its telecommunications lines.
  + Line security – The Organization’s telecommunications lines shall be secured in a manner that ensures availability and prevents tampering.
  + Telecommunications Equipment Security – The Organization’s telecommunications equipment, terminal boxes, and access points shall reside in secure, controlled areas. Only authorized personnel shall be permitted access to such equipment.
  + Configuration Records – ORG shall maintain current configuration records on all telephone systems, including outside and inside wiring, cabling, telephone, wiring closets, and associated equipment.
  + Wireless Security - ORG shall implement only approved wireless solutions designed to protect the confidentiality of information.

# Business Continuity and Disaster Recovery Planning Policy

### Assigned Responsibility: [Chief Information Security Officer or Equivalent]

## History

|  |  |  |
| --- | --- | --- |
| **Revision: Approved By Date** | | |
|  |  | J |
|  |  |  |
|  |  |  |

## Business Continuity and Disaster Recovery Planning Policy

### Purpose

The purpose of this policy is to establish that Information Technology Business Continuity Plans are developed, implemented, and tested in support of continuity of operations for ORG’s functions.

### Applicability/Scope

This policy applies to all information systems owned or leased by the Organization. This policy also applies to all employees, associates and contractors of ORG. ORG reserves the right to change, modify, add, or remove portions of this policy at any time. Federal laws, state laws, or other regulatory requirements may preempt this policy.

### Roles and Responsibilities

The following key roles and responsibilities have been identified for this policy:

**ORG’s Chief Information Security Officer** – responsible for the oversight of the business continuity and disaster recovery plans, as well as establishing and managing the Business Continuity / Disaster Recovery Team.

**Business Continuity / Disaster Recovery Team** – shall develop, revise, administer, and implement the Business Continuity Plan and the Disaster Recovery Plan.

**ORG Information Systems Owners** – Ensure that responsible individuals are trained and familiar with their particular information systems business continuity requirements.

### Enforcement

Failure to comply with the Organization’s information security policies shall result in sanctions as determined by the appropriate disciplinary procedure. For enforcement questions or clarification on any of the information contained in this policy, please contact ORG’s Chief Information Security Officer or the individual with responsibility for this policy as indicated on the policy cover page.

### Policy

In order to ensure timely and reliable access to critical automated services and information, ORG shall develop, review, and update information technology business continuity plans (BCP) and disaster recovery (DR) plans as part of an Information Availability Program.

The Organization’s Business Continuity Plan should achieve an overall business continuity strategy that includes the development, maintenance, and testing of contingency plans, including work around procedures, for the purpose of sustaining operational continuity of mission critical information technology systems and resources.

The Organization’s Business Continuity Plan shall include periodic review and analysis practices that ensure compliance with applicable federal or state legislation, rules, or conditions of funding specific to business continuity or disaster recovery.

##### ORG Business Continuity Plan shall include:

* + Establishment and identification of a Business Recovery Organization with identifying roles and responsibilities, allocated resources and a defining scope of the business continuity management program.
  + Identification of mission critical information technology business systems and business functions.
  + A business impact analysis that identifies time sensitive business functions, financial exposures, operational impacts that estimates total information technology resources necessary for successful business resumption.
  + A risk assessment to determine risk priorities and probability of identified risk.
  + Development and maintenance of current information technology business continuity and recovery plans, policies, and procedures.
  + Plan activation and notification procedures.
  + A Communication Plan including crisis communication procedures and coordination with other public authorities.
  + Emergency response procedures based upon type of emergency(s) and identify command and control procedures for the recovery operation.
  + Back up and replacement of information, equipment, and staff resources, including work around procedures in the event of a disruption.
  + Identification of alternate locations, facilities, and off-site storage facilities.
  + Identification of critical resources and inventories for plan implementation.
  + Development of recovery/restoration procedures for time critical systems/applications/ functions and business functions.
  + Development of appropriate testing schedules to validate the information technology recovery plans and business operations recovery plans.
  + Development of training and awareness of the Business Continuity Program and plan.
  + Development of procedures to maintain and update at least annually the BCP/DR plan(s).