**COMPANY Logo**

**Information Security Policies:** Computer & Network Operations Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO Approved on: 00/00/20

Approved by: COO Approved on: 00/00/20

Approved by: Board of Directors Approved on: 00/00/20

# Purpose

The purpose of the Computer and Network Operations Management Policy is to implement the correct and secure operation of information processing facilities within COMPANY (“COMPANY”). This policy:

* Defines requirements for secure computer operations including: system planning and acceptance; protection against malicious code; monitoring and logging; and backups
* Defines requirements for security network management including: network and infrastructure oversight; network and system integrity; patches and updates to network and infrastructure devices and software; non-standard software; change management; and security controls

# Scope

This policy applies to Users (employees, contractors, vendors, consultants, or other persons) having access to COMPANY computing assets or information. It applies to all systems and network devices used to conduct COMPANY business and sets forth security policy for computer and network operations management. It covers all computers and network and communications systems provided by COMPANY including those systems that must be validated and other systems that contain or access sensitive information.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer (or equivalent) | Information Security Organization | IT Organization | Users |
| --- | --- | --- | --- | --- | --- |
| Operational Procedures | C | A | I | R | I |
| System Planning and Acceptance | C | A | I | R | I |
| Computer and Network Security | C | A | R | R | I |
| Protection Against Malicious Software | C | A | R | R | I |
| Backups and Recovery | C | A | R | R | I |
| Patches and Updates | C | A | R | R | I |

# Policy Statements

# The Computer and Network Operations Management Policy is implemented for the management and operation of all information processing facilities. Secure Computer and Network Operations Management processes ensure the protection of information in computers and networks and the protection of the supporting infrastructure.

This is accomplished via the following:

## Operational Procedures

* + 1. IT must document and maintain computer and network operating procedures.
    2. IT must control changes to COMPANY information processing systems.
    3. IT must ensure formal management responsibilities and procedures are in place to assure satisfactory control of all changes to COMPANY equipment, software, or procedures.
    4. IT must ensure strict change management controls are applied to computer and network operational systems and application software.
    5. IT must establish roles, responsibilities and permissions associated with users accessing COMPANY information that ensures a clear separation of duties.
    6. IT must enforce separation of duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of COMPANY’s assets.
    7. IT must segregate development, test, and operational networks to reduce the risks of unauthorized access or changes to the operational systems.
    8. IT must protect system documentation against unauthorized access.
    9. IT must establish responsibilities and procedures for the management and operation of all COMPANY information processing facilities.
    10. IT must develop and maintain documentation that completely describes the COMPANY network and infrastructure including the security architecture.
    11. IT must consider hardware as well as software security requirements in future design, development, and acquisitions for the COMPANY network and infrastructure.

## System Planning and Acceptance

* + 1. IT must ensure the availability of adequate capacity and resources to deliver required system performance.
    2. IT must monitor, tune, and project future capacity requirements to avoid potential bottlenecks that might present a threat to COMPANY system security or user services.
    3. IT must establish acceptance criteria for new information systems, upgrades, and new versions and ensure suitable security tests of the system are carried out prior to acceptance.

## Computer and Network Security

* + 1. The Information Security Organization must provide configuration management guidelines for all COMPANY networking and infrastructure hardware and software.
    2. The Information Security Organization must ensure appropriate safeguards are implemented to protect against compromise, subversion, or unauthorized manipulation of system software.
    3. The Information Security Organization must adequately manage and control computers and networks in order to protect them from threats, and to maintain security for the systems and applications using the network, including information in transit.
    4. The Information Security Organization must identify and include in any network services agreement (whether these services are provided in-house or outsourced) security features, service levels, and management requirements of all network services.
    5. The Information Security Organization must ensure safeguards are implemented to prohibit application programs from modifying system software.
    6. The Information Security Organization must ensure controls are implemented that prohibit users of applications residing on LANs from making any changes to the system software. Where possible, vendor supplied security controls must be utilized.
    7. The Information Security Organization must ensure software security packages are used only with a valid justification for using these products. The evaluation of these software security packages must be included in the risk assessment of COMPANY information systems to be aware of their advantages and disadvantages.
    8. The Information Security Organization must ensure the use of diagnostic tools such as network and systems scanning are limited on the COMPANY network and infrastructure to trained support personnel, consistent with their job responsibilities.
    9. The Information Security Organization must ensure probing the security of the COMPANY network or infrastructure is restricted to specifically authorized staff with engagement rules specified and agreed to in advance. The use of "sniffing" software or hardware, or probing tools by users is expressly prohibited.
    10. The Information Security Organization must ensure attempts to interfere with service to any user, host, or network ("denial of service attacks") is prohibited. This includes, but is not limited to; "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
    11. The Information Security Organization must ensure the use of programs that infiltrate or attempt to infiltrate a computer or computing system and/or damage or alter the software components of a local or remote computer or computing system are prohibited; even if such action is "harmless" to the targeted system.
    12. The Information Security Organization must implement tools for detecting intrusion of COMPANY network and infrastructure.
    13. IT must maintain a list of approved hardware devices authorized to connect to the COMPANY network.
    14. IT must regularly monitor the COMPANY network to validate that only the approved hardware devices are attached to the network.
    15. IT must maintain a list of approved software authorized for use in the COMPANY infrastructure. This software must be protected from unauthorized modification to the maximum extent possible by the hardware and software mechanisms within the COMPANY infrastructure.
    16. IT must ensure valid documentation that supports the COMPANY software used by programming, operations, and user personnel exists. Only personnel performing official duties should be allowed access to this documentation.
    17. IT must keep software authorized for use in the COMPANY network and infrastructure under close and continuous configuration management controls so that unauthorized changes are not made.
    18. IT must configure routers and switches to prevent disclosure of the configuration of the internal network to external entities.

## Protection Against Malicious Software

* + 1. The Information Security Organization must provide appropriate user awareness materials for protection against malicious software.
    2. IT must implement precautions to prevent and detect the introduction of malicious and unauthorized mobile software.
    3. IT must implement detection, prevention, and recovery controls to protect against malicious software.
    4. IT must ensure that authorized mobile software operates according to a clearly defined security policy, and unauthorized mobile software is prevented from executing.
    5. IT must ensure that all Windows computers (desktop, laptop, and server) connected to the COMPANY network are protected with anti-malware software. This includes personal/home machines that are used for remote access to the COMPANY network.
    6. IT must implement controls to ensure that system hard drives are scanned each time the system is initialized.
    7. IT must implement controls to ensure that each floppy disk, CD, DVD, or USB storage device placed into a computer is scanned automatically.
    8. IT must implement controls to ensure that files downloaded from the Internet via the firewall are scanned for viruses.
    9. IT must implement controls to ensure incoming email attachments are scanned for viruses.
    10. IT must implement controls to ensure anti-malware software is updated on a regular basis to include current virus signatures. Where technically possible, automated anti-malware software updates must be employed to maintain current virus signatures. Where automated virus signature updates are not technically feasible, COMPANY users and/or system administrators are responsible for maintaining current versions of their anti-malware software.
    11. IT must manage malware in accordance with documented COMPANY incident response processes and procedures.
    12. IT must ensure that due care is taken with portable devices such as Blackberry’s, Treos, PDAs and Cell Phones that are targets for malicious software.

## Backups and Recovery

* + 1. IT must establish routine procedures to implement the agreed backup policy and strategy for taking back-up copies of data and testing their timely restoration.
    2. IT must routinely backup, store, manage, and recover all COMPANY critical information using the documented preferred backup solution.
    3. IT must backup mission critical or financially significant information on a regular basis.
    4. IT must backup audit log information daily and store it for at least 12 months
    5. IT must document and test procedures to restore a complete system, or any specific file, from its backup.
    6. IT must make backup copies of information and software and regularly test recover in accordance with the agreed backup policy.
    7. IT must test backup and recovery to ensure completeness and integrity on a regular basis.
    8. IT must ensure all backups have externally visible labels.
    9. IT must regularly check and test restoration procedures to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
    10. IT must retain data and other company records according to guidelines established in the Records Retention Policy.

## Patches and Updates

* + 1. IT must install upgrades and patches.
    2. IT must ensure network and infrastructure devices and software are kept current and patched.
    3. IT must test the installation of upgrades and patches to software to ensure that it is malware-free.
    4. IT must test the installation of upgrades and patches to software to ensure that it is compatible with existing software.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate content
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an Information Security Policy Acknowledgement form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Authorization / Access Control:** The granting of access rights to a user, program, or process.
* **Availability**: The state when data and/or system resources are in the place needed by the user, at the time the user needs them, and in the form needed by the user.
* **Change Control:** Change Control is the process used to review and approve network and infrastructure changes before they are made. This process should be formal, to ensure that the right persons review and approve proposed changes for budget, schedule, performance, and security impact before making changes.
* **Configuration**: The documented physical and functional characteristics of a particular item or system.
* **Configuration Management**: The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items.
* **Information Processing Facility**: Any information processing system, service, or infrastructure – or the physical locations housing them.
* **Information System Security**: The protection given to an information system in order to preserve the availability, integrity, and confidentiality of the system and the information it contains.
* **Intrusion:** The successful act of bypassing the security mechanisms of a network.
* **Malicious Code**: Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose. A self-propagating program that infects and may damage another program.
* **Network:** Interconnection of three or more communicating entities and (usually) one or more nodes. Combination of passive or active electronic components that serves a given purpose.
* **Network Security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.
* **Security Controls:** Hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing it.
* **System Integrity:** The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
* **Third Party**: A person or organization that is recognized as being independent to the corporation.