**COMPANY Logo**

**Information Security Policies:** Information Asset Management

Effective Date:

**COMPANY Logo**

Revised:

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

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

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

# Purpose

The purpose of the Information Asset Management Policy is to achieve and maintain appropriate protection of COMPANY (“COMPANY”) information assets. This policy sets forth requirements for securely creating, collecting, processing, managing, controlling, storing, and using information. In addition, the most critical information (including Non-Public Information) must be identified and given sufficient protection controls and processes. COMPANY considers information to be a business asset of the corporation that must be valued and protected as any other business asset.

# 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 used to conduct COMPANY business, and applies to internal COMPANY information and information shared with and received from third parties.

# 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 | Information Security Organization / IT | Information Owners | Users |
| --- | --- | --- | --- | --- | --- |
| Information Ownership | C | C | R | A | I |
| Information Classification | C | C | R | R | I |
| Information Labeling | C | C | R | A | I |
| Information Protection | C | A | R | R | R |
| Cryptographic Controls | C | A | R | I | I |
| Information Disposal | C | A | R | R | R |
| Inventory of Information Assets | C | C | R | A | I |

# Policy Statements

The Information Asset Management Policy is implemented in order to safeguard information from unauthorized disclosure, modification, or use. COMPANY requires that specific security measures be taken to protect sensitive assets.

This is accomplished via the following:

## Information Ownership

* + 1. Information Owners must be designated for information and assets associated with information processing resources.
    2. Information Owners must be responsible for ensuring that information and assets associated with information processing resources are appropriately classified.
    3. Information Owners must be responsible for defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies as defined in the *Access Controls Management Policy*.
    4. Information Owners must be responsible for determining the value associated with potential loss or damage to business information assets.
    5. Information Owners must determine and review access to business information assets. This access will be based upon User responsibilities.
    6. Information Owners must assign a classification designation to the information asset and ensure the security controls are equal to the level of classification assigned.
    7. Information Owners must ensure a risk assessment is completed on the information asset.

## Information Classification

* + 1. Information Owners must classify information in terms of value, legal requirements, sensitivity, and criticality to COMPANY.
    2. The Information Security Organization must develop guidelines for classifying information, identifying ownership, and ensuring appropriate protection controls.
    3. The Information Security Organization must ensure that information is classified according to its potential impact on COMPANY.
    4. The Information Security Organization must ensure that information in all forms (electronic, printed, media, fax, voice) is protected commensurate with its classification level.
    5. The Information Security Organization must ensure that information is protected during use, storage, transmission, and disposal commensurate to the classification level of the information.

## Information Labeling

* + 1. The Information Security Organization must develop an appropriate set of procedures for information labeling and implementation in accordance with the classification scheme adopted by COMPANY. This classification scheme and procedures for information labeling will be documented in the *Information Classification and Protection Guidelines* and *Information* *Labeling Standards* documents.
    2. The Information Security Organization must ensure that labeling procedures for information labeling cover information assets in physical and electronic formats.
    3. The Information Security Organization must ensure that information assets or information processes are labeled (marked) using the defined classification scheme, from the time of creation until they are destroyed.
    4. The Information Security Organization must ensure that for sensitive information, the information label must identify the Information Owner and the most restrictive classification of information contained. Labels are to be applied uniformly, leaving no doubt about the classification status and the level of protection required.
    5. The Information Security Organization must ensure that document labels appear on the cover page and at the top of each interior page, indicating the level of classification and Information Owner. For very sensitive information, specifically indicate individuals for distribution.

## Information Protection - Information Security Organization

* + 1. The Information Security Organization must ensure that for Non-Public Information, access controls (i.e., password protected) are implemented.
    2. The Information Security Organization must ensure the security of information in electronic media is maintained while in storage.
    3. The Information Security Organization must implement procedures to record the receipt, storage, access requests, issuance, and destruction of media.
    4. The Information Security Organization must implement procedures to cover the retention, logging, usage, maintenance and the disposal of stored media.
    5. The Information Security Organization must implement procedures to monitor the status and location of the stored media.
    6. The Information Security Organization must ensure access to Non-Public Information is allowed by addressee, or as a function of access privileges.
    7. The Information Security Organization must ensure control and distribution of information and that users observe "Need-to-Know" and "Least Privilege" principles.
    8. The Information Security Organization must ensure confidentiality protection controls to ensure that information in storage or transit is protected from unauthorized disclosure are implemented. Information confidentiality requires the use of electronic and procedural methods to ensure the protection of the information.
    9. The Information Security Organization must ensure integrity protection controls to ensure that information in storage or transit is protected from unauthorized modification are implemented. Information integrity requires the use of electronic and logical methods to ensure the consistency of information.
    10. The Information Security Organization must ensure non-repudiation controls using electronic and logical methods that prove formally and legally the fulfillment of a given commitment and/or transaction are implemented.
    11. The Information Security Organization must ensure the availability of information by means of periodic back-ups and recovery mechanisms are maintained.
    12. The Information Security Organization must ensure back-ups of all essential business information are maintained.
    13. The Information Security Organization must ensure back-up information is physically protected to the same standards as the information on the system.
    14. The Information Security Organization must ensure backup information is stored in containers that are suitable to handle the information’s sensitivity.
    15. The Information Security Organization must ensure back-up information is environmentally protected to the same standards as the information on the system.
    16. The Information Security Organization must ensure at least one copy of the backup is stored in a different location so that both the backup and the original could not be affected by the same incident.
    17. The Information Security Organization must ensure that more than one generation of backups are kept.
    18. The Information Security Organization must regularly test back-up media to ensure that they can be relied upon for emergency use when necessary.
    19. The Information Security Organization 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.

## Information Protection - Users

* + 1. Users must evaluate their protection of information resources and act in the best interests of COMPANY.
    2. Users must only access information for authorized purposes (i.e., clear business need).
    3. Users must require advance permission from the Information Owner to access sensitive information.
    4. Users must handle information in all forms (electronic, printed, fax, voice, and media) commensurate with the classification level.
    5. Users must prevent the unauthorized disclosure / dissemination of Non-Public Information.
    6. Users must be responsible for ensuring that locally held information is properly backed up and recoverable.

## Cryptographic Controls - Information Security Organization

* + 1. The Information Security Organization must develop and implement a policy on the use of cryptographic controls for protection of information.
    2. The Information Security Organization must ensure sensitive information is encrypted when included in audit logs (i.e.; captured XML streams).
    3. The Information Security Organization must ensure passwords are treated as sensitive information and encrypted when stored, transmitted, and contained in audit logs.
    4. The Information Security Organization must approve all encryption processes and algorithms. Only certified encryption algorithms that come from trusted sources will be used to encrypt information. When possible, algorithms that support backup keys must be used.
    5. The Information Security Organization must ensure a cryptographic checksum is implemented to protect the integrity of stored information.
    6. The Information Security Organization must approve and ensure cryptographic mechanisms are implemented to support non-repudiation measures.

## Cryptographic Controls - Users

* + 1. Users must use encryption to ensure confidentiality of sensitive information.
    2. Users must encrypt sensitive information when transmitted outside of physically secured areas.
    3. Users must encrypt sensitive information when the information resides in physically unsecured areas.
    4. Users must encrypt sensitive information when transported in computer-readable storage media, such as magnetic tape, floppy disk, CD-ROM, or any other removable media.
    5. Users must encrypt sensitive information when not actively in use.
    6. Users must encrypt sensitive information when stored on hard disks.
    7. Users must use digital signatures on messages for non-repudiation of origin.
    8. Users must use digital signatures on delivery confirmations for non-repudiation of delivery.

## Information Disposal - Information Security Organization

* + 1. The Information Security Organization must develop and disseminate information disposal procedures for the appropriate disposal of Non-Public Information (this includes all media hardcopy, floppy disks, etc.).
    2. The Information Security Organization must put procedures in place to ensure that when electronic media is to be disposed of (e.g., scrapped or sold); no confidential or restrictive information or software can be recovered from that media after disposal.
    3. The Information Security Organization must ensure electronic storage media being returned to a vendor for trade-in, servicing, or disposal offers no opportunity for unauthorized access to confidential or restrictive information or software held on that media.
    4. The Information Security Organization must carry out or oversee the destruction of sensitive information.
    5. The Information Security Organization must erase or overwrite information using the standard operating system facilities (i.e., format) before reusing or disposing of media containing Non-Public Information.
    6. The Information Security Organization must overwrite the media several times (wiping) with changing patterns, using an approved security utility before reusing or disposing of media containing sensitive information.
    7. The Information Security Organization must approve any disposal mechanism/method.
    8. The Information Security Organization must destroy media that cannot be overwritten or is damaged.

## Information Disposal - Users

* + 1. Users must ensure that all sensitive information must be completely deleted from media.
    2. Users must take reasonable precautions for Non-Public Information on hardcopy, to prevent unauthorized access of disposed materials.
    3. Users must shred sensitive hardcopy to prevent unauthorized access.

## Inventory of Information Assets

* + 1. The Information Security Organization must ensure that all information assets are clearly identified and an inventory of all important assets are created and maintained.
    2. The Information Security Organization must ensure the importance of all information assets is identified and documented.

# 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:

* **Access Control**: The application of technical controls and procedures as preventive measures or countermeasures against the threat of unauthorized access to data.
* **Authorization**: The granting of access rights to a user, program, or process.
* **Authentication**: To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. To verify the integrity of information that has been stored, transmitted, or otherwise exposed to possible unauthorized modification. Security measures designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.
* **Data Protection**: The concepts, techniques, technical, administrative, and managerial measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, manipulation, modification, loss, or use.
* **Digital Signature**: A method for signing documents, data, or code and authenticating the sender, data file, or code in a way that is unique to the individual and to the document, data, or code and simultaneously guarantee its integrity. Recipients and systems can verify the identity of the sender, creator, or approver using their public key. Creating a message digest and comparing it to the one in the digital signature provides a means of verifying that the message, data file, or program has not been changed in any way.
* **Electronic Signature**: A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's hand-written signature.
* **Encryption**: The protection of data during storage or transmission by cryptographic means.
* **Identification**: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
* **Information Availability**: The state when data is in the place needed by the user, at the time the user needs it, and in the form needed by the user.
* **Information Classification**: The determination that data is sensitive and requires a specific degree of protection against unauthorized disclosure.
* **Information Compromise**: Disclosure of data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of data, may have occurred.
* **Information Confidentiality**: The concept of holding data in confidence, limited to an appropriate set of individuals or organizations.
* **Information Integrity**: The property that data meet an a priori expectation of quality.
* **Integrity Check**: A mechanism for ensuring that data has not been tampered with by adding to, removing from, or otherwise modifying its contents. Often achieved through digital signatures and one-way hash functions.
* **Least Privilege**: The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks
* **Non-Repudiation**: The concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.
* **Privilege**: Authorization to perform a specific function; usually restricted to a limited set of individuals or elements.
* **Security Controls**: Hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of data and the means of processing it.