Information Classification and Management Policy Template, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Olumuyiwa Agubiade
Last Review Date: November 2023

Information Classification and Management Policy Template

Purpose

The purpose of the (Company Name) Information Classification and Management Policy Template is to provide a system for classifying and managing Information Resources according to the risks associated with its storage, processing, transmission, and destruction.

Audience

The (Company Name) Information Classification and Management Policy Template applies to any individual, entity, or process that interacts with any (Company Name) Information Resource.

Contents

Responsibilities

Information User

- The person, organization or entity that interacts with Information for the purpose of performing an authorized task.
- Have a responsibility to use Information in a manner that is consistent with the purpose intended and in compliance with policy.

Information Owner

- The person responsible for, or dependent upon, the business process associated with an information resource.
- Is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- Determines the appropriate value and classification of information generated by the owner or department.
- Must communicate the information classification when the information is released outside of the department and/or (Company Name) .
- Controls access to their information and must be consulted when access is extended or modified.

- Must communicate the information classification to the Information Custodian so that the Information Custodian may provide the appropriate levels of protection.
- Must periodically review their information to ensure the proper classification is applied.

Information Custodian

- Maintains the protection of Information according to the information classification associated to it by the Information Owner.
- Delegated by the Information Owner and is usually Information Technology personnel.

Policy

Information Classification

- Information owned, used, created or maintained by (Company Name) should be classified into one of the following three categories:
    - Public
    - Internal
    - Confidential
- Public Information:
    - Is information that may or must be open to the general public.
    - has no existing local, national, or international legal restrictions on access or usage.
    - While subject to (Company Name) disclosure rules, is available to all (Company Name) employees and all individuals or entities external to the corporation.

  Examples of Public Information include:
    - Publicly posted press releases,
    - Publicly available marketing materials,
    - Publicly posted job announcements.
- Internal Information:
    - Is information that must be guarded due to proprietary, ethical, or privacy considerations.
    - Must be protected from unauthorized access, modification, transmission, storage or other use and applies even though there may not be a civil statute requiring this protection.
    - Is restricted to personnel designated by (Company Name) , who have a legitimate business purpose for accessing such Information.

  Examples of Internal Information include:
    - Employment Information,
    - Business partner information where no more restrictive confidentiality agreement exists,
    - Internal directories and organization charts,
    - Planning documents,
    - Contracts.
- Confidential Information:
    - Is information protected by statutes, regulations, (Company Name) policies or contractual language. Information Owners may also designate Information as Confidential.
    - Is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a “need-to-know” basis only.

- Disclosure to parties outside of (Company Name) must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:

- Customer data shared and/or collected during the course of a consulting engagement,
- Financial information, including credit card and account numbers,
- Social Security Numbers,
- Personnel and/or payroll records,
- Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction,
- Any Information belonging to an (Company Name) customer that may contain personally identifiable information,
- Patent information.

Information Handling

- All Information should be labelled according to the (Company Name) Labelling Standard.
- Public:
  - Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.
- Internal:
  - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
  - Must be protected by a confidentiality agreement before access is allowed.
  - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
  - Is the “default” classification level if one has not been explicitly defined.
- Confidential:
  - When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
  - When stored on mobile devices and media, must be encrypted.
  - Must be encrypted at rest.
  - Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
  - Must not be transferred via unsecure communication channels, including, but not limited to:
    - Unencrypted email
    - Text messaging
    - Instant Messaging
    - Unencrypted FTP
    - Mobile devices without encryption
  - When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
  - When transmitted via USPS or other mail service, must be enclosed in a sealed security envelope.

- Must not be posted on any public website.
- (Company Name) Management must be notified in a timely manner if Information classified as Confidential has been or is suspected of being lost or disclosed to unauthorized parties.

Information Retention & Destruction

- All information stored by (Company Name) must be stored in accordance with the (Company Name) Data Retention Schedule.
- All information maintained by (Company Name) must include a documented timestamp or include a timestamp as part of metadata.
- Information that is no longer required to be maintained by (Company Name) is classified as "Expired" and must be destroyed in accordance with the(Company Name) Media Reuse and Destruction Standard.
- Information owners should be consulted prior to information destruction and may have the opportunity to extend Information expiration, given business needs and/or requirements for the extended retention.
- (Company Name) customers may have their own information retention requirements that supersede (Company Name) 's requirements. Such customer requirements should be documented in contractual language.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP
- Authentication Standard
- Data Retention Schedule
- Labelling Standard
- Media Reuse and Destruction Standard

Waivers

Waivers from certain policy provisions may be sought following the (Company Name) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments

1.0.0	November 2023		Olumuyiwa Agunbiade	Document Origination

Question & Answer?