Data Classification Policy

Effective date: mm/dd/yyy
Revision: #123

Purpose and Scope

This Data Classification Policy provides the basis for protecting the confidentiality of data at Organization Name by establishing a data classification system. From time to time, Organization Name may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to Organization Name including applicable laws and regulations.

This policy applies to all Organization Name data assets utilized by personnel acting on behalf of Organization Name or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all Organization Name policies and plans.

Classification Management

All Organization Name data should be classified into one of the following four classifications:

- Restricted Data,
- Confidential Data,
- Internal Data, and
- Public Data.

All data that is not explicitly classified should be treated as Internal data and a classification should be determined and requested.

The examples below are not exhaustive. Data owners and senior management are responsible for assigning the types of ways certain data can be used as well as assigning the appropriate classification to Organization Name data.

If you are unable to determine the appropriate data owner or a classification for the data or believe certain data should be reclassified, please contact Security Email .

Changes to the classification of data must be approved by the senior management of Organization Name .

Classification Levels

Public Data

Public data is information that may be disclosed to any person regardless of their affiliation with Organization Name. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside Organization Name and no steps need be taken to prevent its distribution.

Examples of Public data include:

- published press releases;
- published documentation
- published blog posts
- anything on the Organization Name public website
- anything on Organization Name social media profiles

Internal Data

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in moderate risk to Organization Name, its customers, or its partners. Internal data generally should not be disclosed outside of Organization Name without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your manager or send an email to Security Email .

Examples of Internal data include:

- unpublished Organization Name memos
- unpublished marketing materials
- non-public Organization Name customer and partner names
- procedural documentation that should remain private

Confidential Data

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or Organization Name. This classification also includes data that Organization Name may be required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Any unauthorized disclosure or loss of Confidential data must be reported to Policy Owner and an email should be sent to Security Email .

Examples of Confidential data include:

- individual employment information, including salary, benefits and performance evaluations for current, former, and prospective employees
- legal documents
- customer data
- contractual agreements
- compliance reports such as SOC 2
- data that is subject to an NDA or other confidentiality clause
- information shared by partners or investors

Restricted Data

Restricted data includes any information that Organization Name has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to Organization Name , its customers, or its partners. The highest level of security controls should be applied to Restricted Data.

Examples of Restricted data include:

- Organization Name codebase
- intellectual property
- passwords, private keys and other credentials
- bank information
- tax ids
- information related to pending litigation or investigations
- data required to be protected by regulatory obligations
- additional employment information such as background checks, health and medical information, social security numbers.

Restricted data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted data must be immediately reported to your manager and Security Email .

Handling Information

All persons accessing classified information must follow the rules listed above. Each incident related to handling classified information must be reported in accordance with the Security Incident Response Plan.

The method for secure erasure and destruction of media is prescribed in the Configuration and Asset Management Policy.

Exceptions

Organization Name business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Organization Name policy. If an exception is needed, Organization Name management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other Organization Name policy or procedure may result in disciplinary action, up to and including termination of employment. Organization Name reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Organization Name does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Organization Name as soon as possible.

Responsibility, Review, and Audit

Organization Name reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Policy Owner .

This document was last updated on mm/dd/yyy .