**Data Classification Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.8q3in51gc09r)[**4**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.8q3in51gc09r)

[**Scope**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.2vn6fxkvscet)[**4**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.2vn6fxkvscet)

[**Objectives**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.vs7rvoak6l42)[**4**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.vs7rvoak6l42)

[**Policy**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.8wm42y65xfsj)[**4**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.8wm42y65xfsj)

[**Change Request**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.vioz2zn27mka)[**4**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.vioz2zn27mka)

[**Change Review**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.uxxng66elqpo)[**5**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.uxxng66elqpo)

[**Change Approval**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.dpdxy0s5prqt)[**5**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.dpdxy0s5prqt)

[**Change Implementation**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.45p1bjae0n6l)[**5**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.45p1bjae0n6l)

[**Change Testing**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.i8fybfmqimy3)[**5**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.i8fybfmqimy3)

[**Version Control**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.e4ac8kyo1w7u)[**5**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.e4ac8kyo1w7u)

[**Change, Review, and Update**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.5gvei5yt6zoy)[**6**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.5gvei5yt6zoy)

[**Disciplinary Action**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.cmhctdr2g6ok)[**6**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.cmhctdr2g6ok)

[**Responsibility**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.z0lmne9fwh3i)[**6**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.z0lmne9fwh3i)

[**Related Documents**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.v6z7e8uoe1xk)[**6**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.v6z7e8uoe1xk)

[**Risk Management Policy**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.bl1oyyesf030)[**6**](https://docs.google.com/document/d/1PU45Zh-swVSfJxyFIN3d2v6Cg56GN2mlUVisVtIqHnI/edit#heading=h.bl1oyyesf030)

# 

# **Purpose**

This policy establishes our framework for data classification based on its sensitivity, value, and criticality to the company to ensure the appropriate level of data protection. Also, it defines the types of data and specifies roles for data classification.

# **Scope**

This policy applies to all corporate and customer data created, collected, stored, or processed by the company. In addition, it applies to all of the company’s employees and third-party agents authorized to access the data.

# **Policy**

* The classification of data across the information systems in *[Company]* is approved by the management.
* Whenever possible, clearly labeling of information with its data classification should be in place.
* All staff should be guided by the information category in their handling of all company information.

Based on the **FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems** levels of the potential impact on *[Company]* or individuals should there be a breach of security:

* **Low impact** - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
* **Moderate impact** - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that do not involve loss of life or serious life-threatening injuries.
* **High impact** - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

## **Data classification standards**

We classify all data residing in our systems into the following categories.

### **Public**

Public information poses no risk to the company if it is made generally available. Distribution of this information does not require specific approval from the information owner. But, the decision to make a piece of information public should be approved by the adequate authority. Public information can be viewed or copied without restriction.

While it might be necessary to protect source documents from unauthorized modification, public data may be shared with a broad audience both within and outside the company.

The examples include but are not limited to released marketing material, commonly known information, press releases, information held on the website, etc.

### **Internal**

Internal data is information that is potentially sensitive and should not be shared with the public. Internal data generally should not be disclosed outside of our company without the permission of the management. It is the responsibility of the data owner to designate information as internal.

Unauthorized access has the potential to influence our operational effectiveness, cause a crucial financial loss, provide a significant gain to a competitor, or cause a significant drop in customer confidence.

Examples include but are not limited to internal memos, design documents, product specifications, correspondences, internal documentation, etc.

### **Confidential**

Confidential data is any information that, if made available to unauthorized parties, might adversely affect our company. It refers to any company and customer data, processed by us. This classification also includes data required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. Confidential data should be used only by pre-authorized parties and should be protected both when it is in use and when it is being stored, processed, or transmitted.

Examples include but are not limited to legal documents, company agreements, employee PII, employee salary information, customer PII, customer operating data, confidentiality agreements.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by Legal Counsel.

# **Disciplinary actions**

*[Company]* employees who purposely violate this policy are subject to disciplinary action, including denial of access, legal penalties, and dismissal. In addition, any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

# **Responsibility**

The Legal Counsel is responsible for communicating and upholding the Data Classification Policy. All staff is responsible for following the Data Classification Policy.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related documents**

* Data Protection Policy