|  |
| --- |
|  Classification policyFree to use example |
| Let’s boost up your securityVersion 1.0 Created by: securitybooster.net |



Version 1.0

Created by: securitybooster.net

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Rationale** |
| 0.1 | 01-06-2022 | J. Smith, security team | First draft |
| 1.0 | 15-06-2022 | J. Doe, board of directors | Approved version release |
| 1.1 | 04-10-2022 | F. Jacobs, security team | Updated scope to include all of the organization |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Purpose

All employees of <name of organization> have the responsibility to protect our data from unauthorized access, modification or disclosure. All employees are expected to understand and comply with this policy. Data classification is a framework for classifying our data based on its level of sensitivity, value and criticality to our organization. The classification of data will aid in determining the baseline security controls for the protection of the data.

# Scope

This policy applies to all data which is owned or at the responsibility of the organization, both physical and electronic. No data item is too small to be classified.

# Roles and Responsibilities

The following roles and responsibilities are most important for this policy:

The Data Owner is the main person who determines the correct and up-to-date classification of the data under its responsibility.

The Data User is the employee or contractor who is authorized to access the data, and adheres to this and other policies, guidelines and procedures pertaining to the protection of the data.

# Data Classification

Data that is created, processed, collected or maintained by the organization is classified into the following categories:

1. Public data
2. Internal data
3. Sensitive data

**Public data**

Data are considered public when their unauthorized disclosure, alteration or destruction would cause little to no risk to the organization or its affiliates.

Examples of public data include data that may or must be freely available to the general public. It is defined as information with no existing local, national, international or contractual restrictions or access or usage:

* Articles published on the corporate website
* Press releases
* Corporate messages published on social media platforms

Public data must be protected to prevent unauthorized modification, unintended use, or distribution.

**Internal data**

Data is considered as internal data when its potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of the organization without the permission of the person or group that is responsible for that data.

Examples of internal data include:

* Articles published on the internal intranet website
* Memo’s, meeting minutes, etc
* Internal documentation, like manuals, procedural documents, etc

Internal data should be minimal protected by:

* Strong passwords
* Transported using encryption
* Using the corporate identity access management system
* Using corporate provided devices

**Sensitive data**

Data is considered sensitive when unauthorized disclosure, alteration, or destruction would cause significant level of risk to the organization. Sensitive data should only be disclosed to individuals and business partners on a strict-to-know bases.

Examples of sensitive data include:

* Corporate financial data
* Personal Identifiable Information
* Passwords

Sensitive data should be minimal protected by:

* The minimal protection as stated for internal data
* Using Multi Factor authentication methods
* Transmitted outside the organization by using secure connections (like VPN)
* Stored on encrypted disks
* Must be physically stored in locked cabinets

# Conflicts

Some data may be subject to specific protection requirements under contract or according to a law or regulation not described here. In those circumstances, the most restrictive protection requirements should apply. If you have questions, please contact Information Security.