Data Classification Policy

Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Purpose

Explain why data classification should be done and what benefits it should bring.

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organisation, so sensitive corporate and customer data can be secured appropriately.

## Scope

Define the types of data that must be classified and specify who is responsible for proper data classification, protection and handling.

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of the organization’s employees, as well as to third-party agents authorized to access the data.

## Data Classification Procedure

Describe each data classification procedure step by step. Detail who performs each step, how data is assessed for sensitivity, what to do when data doesn’t fit an established category and so on.

Example of a detailed procedure:

<Role> reviews each piece of data they are responsible for and determines its overall impact level, as follows:

1. If it matches any of the predefined types of restricted information listed in Appendix A, the <Role> assigns it an overall impact level of ‘High’.
2. If it does not match any of the predefined types in Appendix A**,** the <Role> should determine its information type and impact levels based on the guidance provided in this document. The highest of the three impact levels is the overall impact level.
3. If the information type and overall impact level still cannot be determined, the <Role>must work with the <Role> to resolve the question

The <Role> assigns each piece of data a classification label based on the overall impact level:

| **Overall impact level** | **Classification label** |
| --- | --- |
| High | Restricted |
| Moderate | Confidential |
| Low | Public |

The <Role> records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.

<Role> apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.

Example of a basic procedure:

*<*Role*>* review and assign each piece of data they own an information type based on the categories.

<Role> assign each piece of data a potential impact level for each of the security objectives (confidentiality, integrity, availability), using the guide in this document. The highest of the three is the overall impact level.

*<*Role*>* assign each piece of data a classification label based on the overall impact level:

| **Overall impact level** | **Classification label** |
| --- | --- |
| High | Restricted |
| Moderate | Confidential |
| Low | Public |

*<*Role*>* record the impact level and classification label for each piece of data in the data classification table.

<Role> apply information security controls to each piece of data according to its classification label and overall impact level.

## Data Classification Guideline

Create a table that describes each type of information asset stored, detail the impact of each of the three security objectives and specify the impact levels and classification to be assigned to each type of asset.

Use this table to determine the overall impact level and classification label for many information assets commonly used in the organization.

|  |  |  |  |
| --- | --- | --- | --- |
| **Budget Planning Documents** | | | |
| Budget planning documents state the potential expenses for the following year. They include data about partners and suppliers, as well as analytical and research data. | | | |
| **Information Types** | | | |
| Funds Control | Funds Control documents include information about the management of the budget process, including the development of plans and use programs, budgets, and performance outputs. | | |
| Security Objectives | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| Impact Description | Unauthorized disclosure of funds control information (particularly budget allocations for specific programs or program elements) can be seriously detrimental to your interests in procurement processes. | Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements. | Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on operations, assets or individuals. |
| Impact Level | Moderate | Moderate | Low |
| Overall Impact Level | Moderate | | |
| Data Classification Label | Confidential | | |

## Impact Level Determination

Provide a table that will help *<*Role*>* determine the impact level for each piece of data by describing the security objectives you want to achieve and how failure to attain each objective would impact the organization.

Use this table to assess the potential impact to the company of a loss of the confidentiality, integrity or availability of a data asset that does not fall into any of the information types described in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Objective** | **Potential Impact** | | |
| **Low** | **Moderate** | **High** |
| **Confidentiality.**  Restrict access to and disclosure of data to authorized users in order to protect personal privacy and secure proprietary information. | Unauthorised disclosure of the information is expected to have **limited** adverse effects on operations, organizational assets, or individuals. | Unauthorised disclosure of the information is expected to have a **serious** adverse effect on operations, organizational assets, or individuals. | Unauthorised disclosure of the information is expected to have a **severe or catastrophic** adverse effect on operations, organizational assets, or individuals. |
| **Integrity**.  Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity. | Unauthorised modification or destruction of the information is expected to have a **limited** adverse effect on operations, assets, or individuals. | Unauthorised modification or destruction of the information is expected to have a **serious** adverse effect on operations, assets, or individuals. | Unauthorised modification or destruction of the information is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals. |
| **Availability**.  Ensure timely and reliable access to and use of information. | Disruption of access to or use of the information or information system is expected to have a **limited** adverse effect on operations, assets, or individuals. | Disruption of access to or use of the information or information system is expected to have a **serious** adverse effect on operations, assets, or individuals. | Disruption of access to or use of the information or information system is expected to have **a severe or catastrophic** adverse effect on operations, assets, or individuals. |

## Appendix A

Describe the types of information that should automatically be classified as “Restricted” and assigned an impact level of “High.” Having this list will make the data classification process easier for *<Role>*.

## ***Types of Information that Must be Classified as “Restricted*”**

***Authentication information***

*Authentication information is data used to prove the identity of an individual, system or service. Examples include:*

* *Passwords*
* *Shared secrets*
* *Cryptographic private keys*
* *Hash tables*

***Payment Card Information (PCI)***

*Payment card information is defined as a credit card number in combination with one or more of the following data elements:*

* *Cardholder name*
* *Service code*
* *Expiration date*
* *CVC2, CVV2 or CID value*
* *PIN or PIN block*
* *Contents of a credit card’s magnetic stripe*

***Personally Identifiable Information (PII)***

*PII is defined as a person’s first name or first initial and last name in combination with one or more of the following data elements:*

* *Driver’s license number*
* *Financial account number in combination with a security code, access code or password that would permit access to the account*

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <ROLE> and the <ORGANISATION>. Policy exceptions must describe:

* The nature of the exception
* A reasonable explanation for why the policy exception is required
* Any risks created by the policy exception
* Evidence of approval by all appropriate parties

Review of this document: this will be reviewed annually by the <Role>.

Next review date: <DATE>