Data Classification Policy

Last updated: November 2023

1. Overview

Data classification is important because it allows organizations to understand the types of information they are processing and storing. The knowledge gained through data classification allows a company to take the necessary measures to protect the data based on its importance or sensitivity

2. Purpose

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.

3. Scope

This policy defines 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.

4. Policy

Data Classification Procedure

The Data Owner 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 data owner assigns it an overall impact level of ‘High’.

2. If it does not match any of the predefined types in Appendix A, the Data Owner 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 Data Owner must work with the Data Protection Officer to resolve the question

The Data Owner 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 Data Owner 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.

The Data Protection Officer applies 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.

Data Classification Guideline

The following table is the template to describe 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.

<information asset name>			
<information asset description>			
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

This table aims to help the Data Owner determine the impact level for each piece of data by describing the security objectives they want to achieve and how failure to attain each objective would impact the organization.

This table is used 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.	Disruption of access to or use of the information or	Disruption of access to or use of the information or	Disruption of access to or use of the information or information system is

Ensure timely and reliable access to and use of information.	information system is expected to have a **limited** adverse effect on operations, assets, or individuals.	information system is expected to have a **serious** adverse effect on operations, assets, or individuals.	expected to have **a severe or catastrophic** adverse effect on operations, assets, or individuals.

Appendix A

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

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

The following definition and terms can be found in the Cloudoko Glossary.

- Data Owner
- Data Protection Officer

8. Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version

www.cloudoko.com