Information Classification and Handling Policy

NOTE: *Please review and edit, or replace, this content as appropriate to meet the needs of your business. Note any places with content in square brackets [ ], are fill-in-the-blank sections. Please provide appropriate content before you save the template. Check to ensure the content of your saved policy is consistent with the* ***in-scope controls*** *you have associated with this policy.*

Policy reviewer and updates: Ashish Mahendru
Policy owner and approver: Sachin Smotra
Last reviewed and updated: 05-MAR-2024
Last approval date: 06-MAR-2024

Introduction

This policy establishes rules for information classification based on confidentiality, integrity, availability and relevant interested party requirements.

Objective

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

Responsibilities and Scope

This policy applies to all employees who manage, oversee or carry out any of the defined policy requirements within this policy.

To meet information classification and handling requirements, the following controls must be followed:

1. Classification of Information

Policy Requirements

Classification of Information

Information must be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements to ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

Owners of information must be accountable for its classification.

The classification scheme must include conventions for classification and criteria for review of the classification over time. Results of classification must be updated in accordance with changes of the value, sensitivity and criticality of information through their life cycle.

The classification can be determined by the level of impact that the information's compromise would have for the organization. Each level defined in the scheme must be given a name that makes sense in the context of the classification scheme's application.

Information Classification Table

Data Sensitivity	Description	Example
Public Data	Information intended or required for public release	• Published website content • Press releases
Sensitive Data	Requires additional levels of protection	• Operational information • Personnel records • Information security procedures • Research • Internal communications • Log records (firewall logs, audit trails, etc.)
Confidential Data	Information that must be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements	• Personal Information (PI) • Personally Identifiable Information (PII) • Social Security Number (SSN) • Cardholder data (e.g. primary account number (PAN), card service code (3-4 digit code) • Electronic Protected Health Information (ePHI) • Individually Identifiable Health Information (IIHI) • Employment records • Intellectual property (e.g. copyrights, patents and trade secrets) • Client/Customer Data

Document Control

Enforcement

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

Distribution

This policy is to be distributed to all Dataworkz employees who manage, oversee or carry out any of the defined policy requirements within this Information Classification and Handling Policy.

Version History

If you are reading a printed version of this document you must check Security Policies to ensure that you have the most up to date version.

Supporting Procedures, Standards, Baselines and Guidelines

Please see the below link for further information on how this topic-specific policy has been operationalized: Confluence-Security