Data Classification Policy

Doorway

SOC 2 Criteria: C1.1, PI1.1
ISO 27001 Requirements: 7.5.2, 7.5.3
ISO 27001 Annex A: A.5.1.1, A.7.1.2, A.7.2.1, A.8.1.1, A.8.2.1, A.8.2.2, A.16.1.4, A.18.1.3

Keywords: Confidential Data, Internal Data, Public Information, Restricted Data, Classification

---

Purpose

This policy will assist employees and other third-parties with understanding the Company's information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect sensitive or confidential information (e.g., Company Confidential information should not be left unattended in conference rooms).

Scope

Information covered in this policy includes, but is not limited to, information that is received, stored, processed, or transmitted via any means. This includes electronic, hardcopy, and any other form of information regardless of the media on which it resides.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

Definitions

- **Confidential/Restricted Data**:

Generalised terms that typically represent data classified as *Sensitive or Private*, according to the data classification scheme defined in this policy.

- **Internal Data**:

All data owned or licensed by Doorway, including non-sensitive data that's imported via a human resource integration.

- **Public Information**:

Any information that is available within the public domain.

Data Classification Scheme

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to Doorway should that data be disclosed, altered, or destroyed without authorisation. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data should be classified into one of the three following classifications.

Confidential/Restricted Data

Data should be classified as Restricted or Confidential when the unauthorised disclosure, alteration, or destruction of that data could cause a serious or significant level of risk to Doorway or its customers. Examples of Sensitive data include data protected by state or federal privacy regulations (e.g. PHI & PII) and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted and Confidential Data:

- Disclosure or access to Restricted and Confidential data is limited to specific use by individuals with a legitimate need-to-know. Explicit authorisation by the Security Officer is required for access to because of legal, contractual, privacy, or other constraints.
- Must be protected to prevent loss, theft, unauthorised access, and/or unauthorised disclosure.
- Must be destroyed when no longer needed. Destruction must be in accordance with Company policies and procedures.
- Will require specific methodologies, procedures, and reporting requirements for the response and handling of incidents.

Internal Use Data

Data should be classified as Internal Use when the unauthorised disclosure, alteration, or destruction of that data could result in a moderate level of risk to Doorway or its customers. This includes proprietary, ethical, or privacy considerations. Data must be protected from unauthorised access, modification, transmission, storage or other use. This applies even though there may not be a civil statute requiring this protection. Internal Use Data is restricted to personnel who have a legitimate reason to access it. By default, all data that is not explicitly classified as Restricted/Confidential or Public data should be treated as Internal Use data. A reasonable level of security controls should be applied to Internal Use Data.

Public Data

Data should be classified as Public when the unauthorised disclosure, alteration or destruction of that data would result in little or no risk to Doorway and its customers. It is further defined as information with no existing local, national, or international legal restrictions on access or usage. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorised alteration or destruction of Public Data.

Assessing Classification Level and Labelling

The goal of information security, as stated in the Information Security Policy, is to protect the confidentiality, integrity, and availability of Corporate and Customer Data. Data classification reflects the level of impact to Doorway if confidentiality, integrity, or availability is compromised. If a classification is not inherently obvious, consider each security objective using the following table as a guide. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorised employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorised parties either internal or external to Doorway. Impact could include negatively affecting Doorway's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by Doorway.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Confidential information were to become available to unauthorised parties either internal or external to Doorway. Impact could include negatively affecting Doorway's competitive position, damaging the company's reputation, violating contractual requirements, and exposing geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originating within or owned by Doorway, or entrusted to it by others. Internal Use information may be shared with authorised employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Internal Use information were to become available to unauthorised parties either internal or external to Doorway. Impact could include damaging the company's reputation and violating contractual requirements.

PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	**NO DAMAGE** would occur if Public information were to become available to parties either internal or external to Doorway. Impact would not be damaging or a risk to business operations.

HANDLING CONTROLS PER DATA CLASSIFICATION

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement	NDA is required prior to access by non-Doorway employees.	- NDA is recommended prior to access by non-	- No NDA requirements	- No NDA requirements

(NDA)		Doorway employees.		

Labeling

Internal Network Transmission (wired & wireless)	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited	- Encryption is recommended - Instant Messaging is prohibited - FTP is prohibited	- No special requirements	- No special requirements

Labeling

External Network Transmission (wired & wireless)	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited - Remote access should be used only when necessary and only with VPN and two-factor authorisation when possible	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited	- Encryption is recommended - Instant Messaging is prohibited - FTP is prohibited	- No special requirements

Labeling

Data at Rest (file servers, databases, archives, etc.)	- Encryption is required - Logical access controls are required to limit unauthorised use - Physical access restricted to specific individuals	- Encryption is recommended - Logical access controls are required to limit unauthorised use - Physical access restricted to specific groups	- Encryption is recommended - Logical access controls are required to limit unauthorised use - Physical access restricted to specific groups	- Logical access controls are required to limit unauthorised use - Physical access restricted to specific groups

Labeling

Mobile Devices (iPhone, iPad, USB Drive, etc.)	- Encryption is required - Remote wipe must be enabled, if possible	- Encryption is required - Remote wipe must	- Encryption is recommended - Remote wipe	- No special requirements

		be enabled, if possible	should be enabled, if possible	

Labeling

Email (with and without attachments)	- Encryption is required - Do not forward	- Encryption is recommended - Do not forward	- Encryption is recommended - Do not forward	- No special requirements

Labeling

Physical Mail	- Mark "Open by Addressee Only" - Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings	- Mark "Open by Addressee Only" - Use "Certified Mail" and sealed, tamper-resistant envelopes for external mailings	- Mail with company interoffice mail - US Mail or other public delivery systems	- No special requirements

Revision History

Version	Date	Editor	Description of Changes
1.0	24.02.2022	Henry Sinclair	Initial Creation
2.0	13.10.2022	Hugh Fraser	Inclusion of HR platform integration specifications