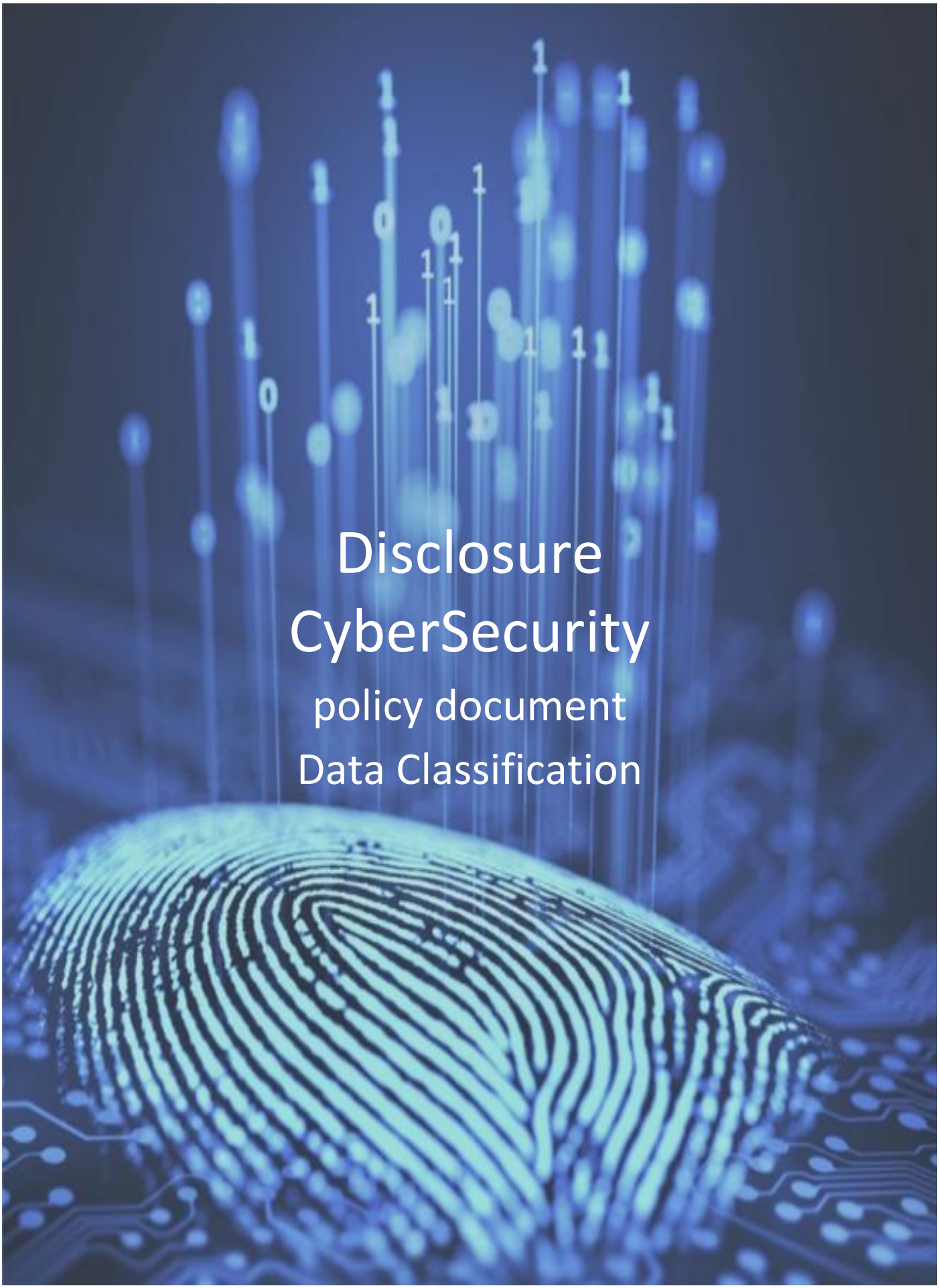

Disclosure CyberSecurity

policy document

Data Classification

Document Control

Document Name:	Disclosure CyberSecurity - policy document - Data Classification		
Version Number:	1.0		
Revision History:	Date:	Change:	Version:
	17.03.2026	Initial draft	0.1
	18.03.2026	Release	1.0
Author:	Peter White, Chief Technology Officer		

Table of Contents

Table of Tables

Table of Figures

No table of figures entries found.

ISMS document reference

ISMS Control	Reference
Document name	Data classification
Document version	1.0
Document file name	Disclosure CS – policy – data classification
Author	Peter White; CTO, CISO
ISMS number	00032
Classification	Confidential
Document owner	Risk and Compliance
Document type	Policy
Administration	Senior Leadership Team
Location	SharePoint; Operations; Compliance
Last issue date	18.03.2026
Date of last review	18.03.2026

Table 1 ISMS document reference

1. Introduction

1.1 Background

Disclosure CyberSecurity are maturing their security posture and cyber resilience to protect the Confidentiality, Integrity and Availability of assets from vulnerabilities and associated threats. As part of this improvement, an Information Security Management System (ISMS) has been defined and to ensure policies, procedures, and objectives can be created, controlled, standardised, implemented and published across the organisation.

implemented and published across the organisation.

The ISMS requires a data classification policy to proactively define, guide and maintain standards-based compliance such as ISO 27000 and Cyber Essentials; as part of the Disclosure CyberSecurity continuous life-cycle management, protection and improvement initiatives.

The use of data classification is growing within Disclosure CyberSecurity, and guidelines for use are required to protect Disclosure CyberSecurity.

1.2 Objectives

The objectives of a data classification policy include the following:

- Ensure the organisation, individuals, contracted staff and auditors understand the methods, approach and intent of data classification.
- Reduce the probability of data misclassification.
- Enhanced data security targeting classifications with data protection solutions; including security measures like data segmentation (application, storage, system), encryption or data loss prevention (DLP).
- Adapt security controls for data access, processing, storage and backup.
- Maintain General Data Protection Regulation (GDPR) regulatory compliance.
- Reduce data storage costs by identifying duplicate, redundant or outdated (by regulation) information.

1.3 Definitions

Table 2 details the policy definitions:

Definition ID	Description
DEF-001	Data classification is the process and governance of organising data into categories based on its sensitivity, value, and risk to an organisation, allowing for appropriate security controls and compliance management.

Table 2 definitions

1.4 Applicability

This policy applies to all employees, consultants, vendors and partners consuming, processing, sorting or controlling Disclosure CyberSecurity data; including standard data and artificial intelligence generated or processed data.

Adherence to these requirements is mandatory; and wilful or negligent infringement of the policy will result in disciplinary, employment, and/or legal sanctions.

1.5 Scope

A data classification policy consists of many components. This document defines the Disclosure CyberSecurity policy and strategy for data classification.

Table 2 summarises the data classification categories considered in scope of this data classification policy:

Category	Components
Data classification approach	Content-based data classification, context-based data classification, user-based data classification.
Data classification labels / use	Public, internal, confidential, restricted, sovereignty.

Table 3 data classification categories

1.6 Out of scope

This data classification policy does not include the following:

- Defined data classification procedures.
- Defined data classification solutions.

1.7 Transferred scope

This policy has no transferred scope.

2. Data classification policy

2.1 Principles

Table 4 details the policy principles:

Principle ID	Description
PCP-001	All data classification will be performed on ingest of new data, acquisition of organisations, data reliance application migrations or transformation, periodic classification assessments.
PCP-002	This policy will be reviewed and continuously updated to include category and component changes to ensure all future data classification requirements are enclosed.

Table 4 data classification principles

2.2 Assumptions

Table 5 summaries the data classification policy assumptions:

Assumption ID	Description
ASS-001	This policy will encompass all data classification components.
ASS-002	All new data introduced into the environment will be assessed for compliance; and this policy will be updated for new data classification components where the current scope is not sufficient.

Table 5 data classification assumptions

2.3 Data classification preparation

To maintain an effective data classification process, the organisation will be required to maintain the following items:

- Data classification policy (this document).
- Data classification process (this document).
- Data classification owner; this is typically the Data Protection Officer (DPO).
- Data classification procedures; for all data ingests, processing, storage and control.
- Data managers and consumers must be adequately educated for data classification.

2.4 Data classification review board

The data classification review board consists of key business stakeholders with the executive team. The main role of the board is to establish and maintain control and order of data classification within the organisation:

- Management: of the data classification review board and business function heads.
- Governance: of data classification decisions and regulatory or insurance compliance.
- Impact Analysis: risk assessment and planning of potential data classification breaches.
- Authority: of brand and commercial impact.
- Data owner: of the data classification and the business data.
- Technical and Security: assurance of software and services.
- Validation: of board decisions and risks.
- Support: of board activities and delegate of authority for board member absence.

Table 6 details the business community board members and roles:

Role	Data classification review board member(s)	Contact details
Chairperson	Chief Executive Officer	*Refer to the Information Security Management System document for contact details.*
Management		
Governance	Chief Operating Officer	*Refer to the Information Security Management System document for contact details.*
Impact Analysis		
Authority		
Data Owner	Data Protection Officer	*Refer to the Information Security Management System document for contact details.*
Technical	Chief Technology Officer	*Refer to the Information Security Management System document for contact details.*
Security	Chief Information Security	*Refer to the Information Security Management System document for contact details.*
Validation	Head of Risk and Compliance	*Refer to the Information Security Management System document for contact details.*
Support		

Table 6 data classification categories

2.5 Data classification approach

Table 7 summarises the data classification approach:

Category	Component(s)	Item(s)
Content-based data classification	Real-time file scanning	- Identifies data and provides classification recommendations / assignment during real-time access, processing and ingest; based on defined key word matches.
	Periodic file scanning	- Identifies data and provides classification recommendations / assignment on a periodic based for legacy data or data missing by the real-time process; based on defined key word matches.
Context-based data classification	Meta-data	- Identifies data and provides classification recommendations / assignment from data attributes; such as creator, application, creation date, modification date, processor.
	Source	- Identifies data and provides classification recommendations / assignment from data attributes; such as storage location, storage type, supplier.
User-based data classification	User	- Provides manual data classification assignment and can be used to validate automated data classification, especially for protected and sensitive data.
	Data owner	- Provides manual data classification assignment for data sources, applications and storage areas.

Table 7 data classification approach

All data classification in Table 7 are included in this policy:

- Data classification must be assigned to all data.
- All data ingress points must be covered by the data classification process; including email, filesharing, messaging, electronic data interchange.

- All data egress point must be covered by the data classification process; including (the data ingress points), backup, archiving, system replication.
- All data application processing must be covered by the data classification process; including the ability to tag / label data within the application manually and automated.
- Any data that cannot pass through a data classification point must be stored in a protected area until it can be classified.

2.6 Data classification labels

Table 8 summarises the data classification labels:

Category	Component(s)	Item(s)
Data classification labels	Public	- Data is available to the public and provides zero business risk if disclosed. - Minimal protection is required; integrity is more important than confidentiality.
	Internal	- Data is Intended for internal use only and available within the organisation for general use with; medium business risk if exposed but not meant for public consumption. - Basic security controls and internal access.
	Confidential	- Sensitive data requiring restricted access within the organisation; high risk where unauthorised disclosure may cause financial loss or reputational damage. - Advanced security is required to limited to access to authorised personnel, requiring encryption, privilege access and full access auditing.
	Restricted	- Highest level of sensitivity within the organisation; high-catastrophic risk where a leak can cause legal, financial, regulatory, personal or system harm, including trade secrets, intellectual property, specialised compliance data, stock manipulation, protection / encryption keys, board-level meeting minutes, and high-security legal documents. - Enhanced security, granular access control, encryption in transit and at rest, and audit logs with continuous checking and validation and zero trust.
	Sovereignty	- Data sovereignty is an additional parallel label used alongside another label, where data consumption is either: o limited to a specific region, or; o the accompanying classification label is impacted within or outside of a region. ***Note**: requires that data is managed according to the laws of the country where it is stored.*

Table 8 data classification labels

All Data classification type in Table 8 are included in this policy:

- Data classification labels must be used for all data; initial unlabelled data must be treated as the most secure until labelled.

2.7 Data classification use

Table 9 summarises the data classification use guide:

Category	Component(s)	Item(s)
Data classification use	Public	- Website content. - Publicly accessible policies. - Publicly accessible financial records - Job adverts.
	Internal	- Operational policies. - Job descriptions. - Organisation chart.
	Confidential	- Business strategy. - Insurance documentation. - Risk register. - Job references. - Client personally identifiable information. - Client case information. - Supplier contract information. - Employee personally identifiable information. - Human resources. - Payroll information. - Health information. - Authentication information. - Technology used information.
	Restricted	- Organisation financial records. - Acquisitions and mergers.
	Sovereignty	- Offshore client personally identifiable information. - Offshore client case information.

Table 9 data classification use

***Note**: Table 9 provides examples of data classification assignments.*

2.8 Auditing

Table 10 summarises the data classification auditing:

Category	Component(s)	Item(s)
Data classification use	Data classification approach	- As defined in section 2.5.
	Data classification labels	- As defined in section 2.6.

Table 10 auditing

All data classification auditing in Table 10 are included in this policy:

- Data classification must be audited by the data classification review board; the data classification review board's audit activities must also be audited by the Risk and Compliance team.

2.9 Reporting

Data classification reporting is important to ensure that all key stakeholders are continuously informed of the following:

- Data classification compliance.

- Data classification deviations.

Table 11 summarises the reporting schedule of this data classification policy:

Deliverable	Frequency (every)
Data classification compliance report.	26 week(s).
Data classification deviation report.	52 week(s).

Table 11 reporting

2.10 Roles

Table 12 details the roles and responsibilities to support the data classification policy:

Role	Responsibility	Description
Service stakeholder + **delegated authority**	Govern Data Protection Officer	- Owns the data classification service. - Owns the data classification plan. - Liaises with organisations executives. - Promotes the data classification service. - Audits and validates the success of the data classification service.
Service owner + **delegated authority**		- Owns the data classification process. - Defines and maintains the data classification process. - Maintains the data classification plan. - Ensures compliance by data classification teams, users, suppliers and partnerships. - Contributes to the data classification User Guide. - Promotes the data classification plan and provides guidance within the organisation. - Manages the continuous risk assessment. - Audits and validates the management execution of the data classification plan.
Manager + **delegated authority**		- Manages the continuous improvement plan for the data classification plan. - Defines and maintains the data classification procedures aligned to the data classification process. - Reports on the data classification service. - Communicates changes with the organisation. - Audits and validates the execution of the data classification process and procedures.
Users	Comply	- Comply with all data classification policies. - Comply with all data Classification procedures. - Notify management and compliance any accidental or intentional infringement.

Table 12 roles and responsibilities

2.11 Key performance indicators

Table 13 summarises the key performance indicators and success criteria for the implementation and management of this data classification policy:

Deliverable	Review frequency (every)	Objective

Improvement of data classification.	52 week(s).	Complete.
Reduction of miss-classification deviations	52 week(s).	Complete.

Table 13 key performance indicators