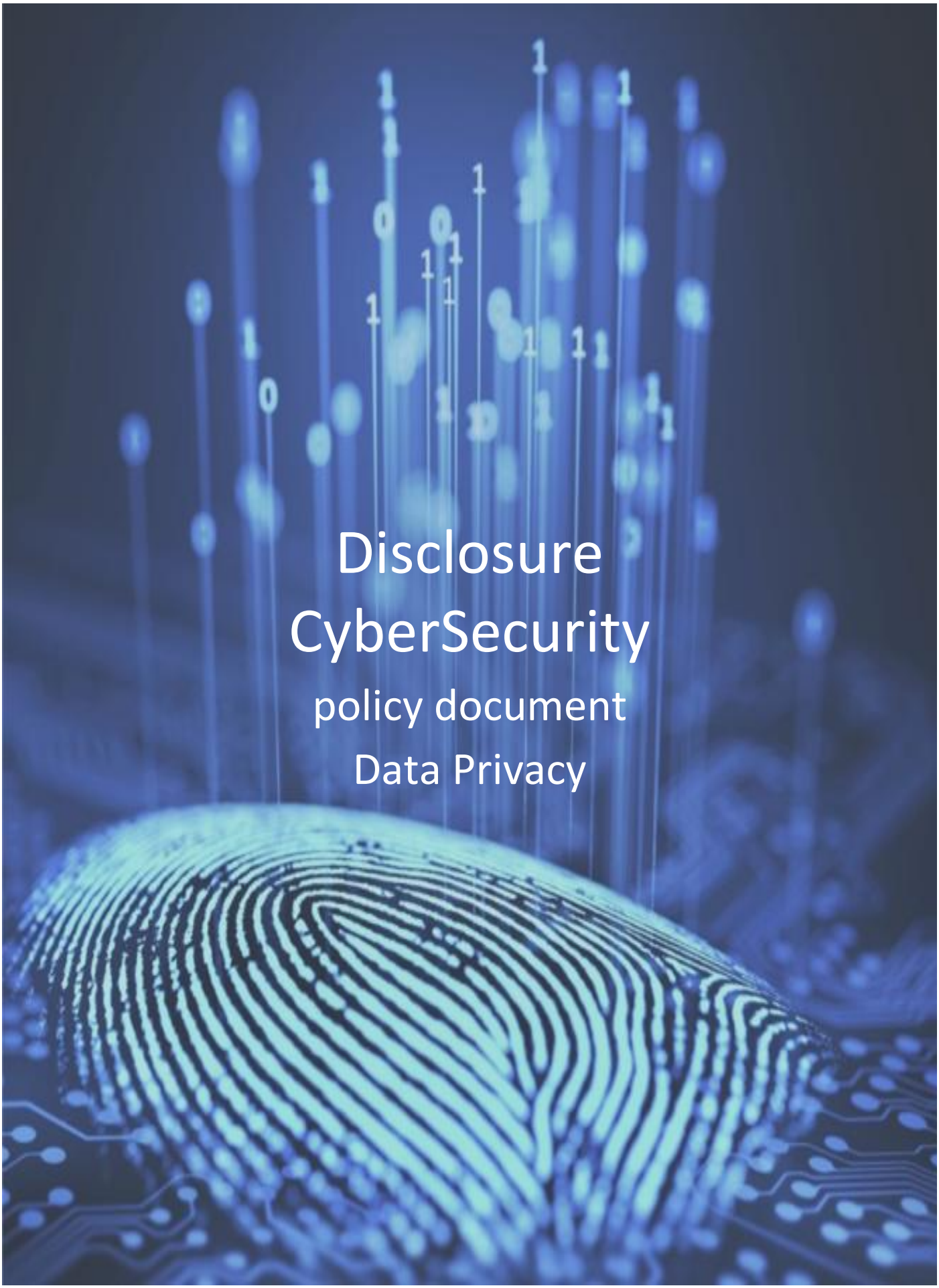

Disclosure CyberSecurity

policy document

Data Privacy

Document Control

Document Name:	Disclosure CyberSecurity - policy document - Data Privacy		
Version Number:	1.0		
Revision History:	Date:	Change:	Version:
	18.03.2026	Initial draft	0.1
	22.03.2026	Release	1.0
	23.03.2026	User rights updates	1.1
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 privacy
Document version	1.1
Document file name	Disclosure CS – policy – data privacy
Author	Peter White; CTO, CISO
ISMS number	00033
Classification	Confidential
Document owner	Risk and Compliance
Document type	Policy
Administration	Senior Leadership Team
Location	SharePoint; Operations; Compliance
Last issue date	24.03.2026
Date of last review	24.03.2026

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 privacy 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.

1.2 Objectives

The objectives of a data privacy policy include the following:

- Ensure the organisation, individuals, contracted staff, auditors and the public understand the methods, approach and intent of data privacy.
- Reduce the probability of data privacy breaches.
- Enhanced data security targeting privacy 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.
- Meet legal requirements for data privacy.

1.3 Definitions

Table 2 details the policy definitions:

Definition ID	Description
DEF-001	Data privacy policy is a mandatory, transparent document explaining how an organisation collects, uses, stores, and protects personal data, ensuring compliance with regulations like UK GDPR. It must detail data retention, security measures, and user rights (e.g., access, deletion).
DEF-002	The right of individuals defines how their personal information (names, health records, IP addresses and financial details) is collected, used, and shared by organisations. It focuses on compliance with legal regulations like GDPR, ensuring data is handled lawfully, transparently, and securely to prevent misuse.
DEF-003	Personal Data is any information that 'relates to' an identified or identifiable individual, including information that can identify an individual directly or indirectly in combination with other information.

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

Table 3 summarises the data privacy categories considered in scope of this data privacy policy:

Category	Components
Data collection	Data classification, employees, employee special circumstances, suppliers / partners, clients, services.
Data used	Employees, employee special circumstances, suppliers / partners, clients, services.
Data sharing	Employees, employee special circumstances, suppliers / partners, clients, services.
Data retention	Employees, employee special circumstances, suppliers / partners, clients, services. Active data, archived data, backup data (immutable).
Data destruction	Digital, physical.
User rights	Right to be Informed, Right of Access, Right to Rectification, Right to Erasure, Right to Restrict Processing, Right to Data Portability, Right to Object, Rights Related to Automated Decision-Making & Profiling, Right to Withdraw Consent, Right to Complain.

Table 3 data privacy categories

1.6 Out of scope

This data privacy policy does not include the following:

- Defined data privacy procedures.
- Defined data privacy solutions.

1.7 Transferred scope

This policy has no transferred scope.

2. Data privacy policy

2.1 Principles

Table 4 details the policy principles:

Principle ID	Description
PCP-001	Data privacy applies to all internal and external data.
PCP-002	This policy will be reviewed and continuously updated to include category and component changes to ensure all future data privacy requirements are enclosed.

Table 4 data privacy principles

2.2 Assumptions

Table 5 summaries the data privacy policy assumptions:

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

Table 5 data privacy assumptions

2.3 Data privacy preparation

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

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

2.4 Data privacy review board

The data privacy 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 privacy within the organisation:

- Management: of the data privacy review board and business function heads.
- Governance: of data privacy decisions and regulatory or insurance compliance.
- Impact Analysis: risk assessment and planning of potential data privacy breaches.
- Authority: of brand and commercial impact.
- Data owner: of the data privacy 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 privacy 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 privacy categories

2.5 Data collection

Table 7 summarises the data collection:

Category	Component(s)	Item(s)
Data collection	Data classification	- see the Data Classification policy.
	Employees	- Recruitment process. - Job role updates and transfers to new role. - Legal identification. - Company benefit (in kind) application form. - Employee leaver process.
	Employee special circumstances	- Specialist role application form. - Vetting application form. - Legal activities / actions.
	Suppliers / partners	- Supplier onboarding form. - Partner onboarding form. - Partner services agreement. - Continuous contact introduction.
	Clients	- Project engagement form. - Project proposals. - Project statement of works. - Continuous contact introduction.
	Services	- Online service registration form. - Services agreements. - Service contracts. - Continuous contact introduction.

Table 7 data collection

All data collected in Table 7Table 10 are included in this policy:

- Data must be collected in the defined data collection methods.
- Data collected must be validated by the source data provider.
- All data collection variations must be recorded and the collection process updated if required.

2.6 Data used

Table 8 summarises the data used:

Category	Component(s)	Item(s)
Data used	Employees	- Personnel records; full name, date of birth, sex and gender, address, telephone / mobile number, relationship status. - Financial information; employee identification, renumeration, benefits in kind, bank account, pension plans, health plans, tax and national insurance information. - Professional information; qualifications, memberships, performance and appraisal records, leave and sickness records, disciplinary and grievance information. - Digital information; photographs, browsing history, cookie history, use-policy deviations. - Accident, injury or death information. - Personnel emergency contacts; full name, email address, telephone / mobile number. - GP surgery / doctor's emergency contacts (for acute illness); name, address, telephone / mobile number (OPTIONAL). - Legal identification (right to work); driving license, passport, identity cards. - Insurances (driving); previous 5-year insurance history, all refused insurances. - Pre-employment; personal contact details (recruitment), references. - Post-employment contact details (follow-on communications); pension, payslips.
	Employee special circumstances	- Clearance and vetting information (DBS, SC, DV); full previous names, full previous address, criminal allegations, current and spent convictions, full financial disclosure.
	Suppliers / partners	- Company information; registration, address(s). - Contact information; name, registered office, email address, telephone / mobile number. - Insurances; public liability, cyber. - Payment information; Bankers' Automated Clearing Services (BACS), bank account.
	Clients	- Company information; registration, address(s). - Contact information; name, registered office, email address, telephone / mobile number. - IPv4 and IPv6 address ranges; used when remote access to client is required, connectivity services used, security services provided. - Financial information; credits, debts, payment history. - Project information; designs, implementations, configurations, assets, licenses, other project collateral.
	Services	- Credentials; username, password (unreversible encrypted), multi-factor authentication device.

	- IPv4 and IPv6 address(s); used when consuming a service and working remotely. - Access behaviours: login date and time, process date and time, logout / termination date and time. - Data manipulation; additions, changes, deletions. - Service information; assets (names, IP addresses), configurations, software, software versions, hardware, hardware versions. - Cookies; persistent filtering, sorting and grouping.

Table 8 data used

All data used in Table 8Table 10 are included in this policy:

- Data must be stored in the correct repositories to ensure adequate security controls restrict access.
- Data must be classified as per the Data Classification policy.

Table 9 confirms the data that Disclosure CyberSecurity do not collect, store or process:

Category	Component(s)	Item(s)
Data not used	Employees	- Credit or debit card information. - Legal documentation. - Race or ethnic origin. - Political opinions. - Religious or philosophical beliefs. - Trade union membership. - Genetic and biometric data (used for identification). - Health Data. - Sexual orientation.
	Employee special circumstances	
	Suppliers / partners	
	Clients	

Table 9 data not used

2.7 Data sharing

Table 10 summarises the data sharing:

Category	Component(s)	Item(s)
Data sharing	Employees	- Employment reference. - Legal requirements. - Government departments and agencies; HMRC - Crime prevention or detection agencies; police, serious fraud office, courts or tribunals. - Outsourced business functions; payroll, cloud-based systems, archiving facilities, pensions and insurance providers.
	Employee special circumstances	- Transfer of vetting. - Transfer of Undertakings (Protection of Employment).
	Suppliers / partners	- Legal requirements.
	Clients	- Client reference. - Client case study. - Legal requirements. - Supplier, partner or vendor introduction.
	Services	- Legal hold (or litigation hold).

Table 10 data sharing

All data sharing in Table 10 are included in this policy:

- Data sharing must be communicated to all affected parties.
- Data sharing must be recorded in a data sharing register.

2.8 Data retention

Table 11 and Table 12 summarises the data retention:

Category	Component(s)	Item(s)	Retention
Data retention	Employees	- Pre and post-employment information. - Active employment information. - Accident, injury or death information.	- 2 years. - 7 years. - 3 years.
	Employee special circumstances	- Clearance and vetting information.	- 2 years.
	Suppliers / partners	- Company information. - Contact information. - Financial information.	- 7 years. - 5 years. - 7 years.
	Clients	- Company information. - Contact information. - Financial information. - Project information (not secret). - Project information (secret).	- 7 years. - 5 years. - 7 years. - 7 years. - 0 years.
	Services	- Credentials. - IPv4 and IPv6 address(s) (audit log). - Access behaviours (audit log). - Data manipulation. - Service information. - Cookies.	- 0 years. - 10 years. - 10 years. - 1 year. - 10 years. - 0 years.

Table 11 data retention

Category	Component(s)	Item(s)	Retention
Data retention	Active data	- Multiple copies for resilience, with real-time access. - Continuous retention whilst active.	- Continuous.
	Archived data	- Single copy for near-time retrieval.	- 2 years, - Unless backed-up or deleted.
	Backup data (immutable)	- Multiple copies for resilience, with offline retrieval.	- 3 to 10 years, - Unless there are special retention circumstances.

Table 12 data retention

All data retention in Table 12 are included in this policy:

- Data may be retained in both an archive state and backup state, using separate data repositories.
- Data can be deleted from the active and archived data repositories.

- Backup data can not be deleted from an immutable backup data store.
- backup data can be retained for longer than the retention period for special circumstances.

2.9 Data destruction

All data destruction included in this policy:

- Data destruction must be performed in accordance with the retention lifecycle.
- Appropriate data destruction must be performed in accordance with the data media; digital, physical.
- Where backups contain combined data streams, it may be necessary to restore the combined data instance, delete the necessary data, and recreate the backup data instance.

2.10 User rights

Table 13Table 14 summarises the data privacy user rights:

Category	Component(s)	Item(s)
Data privacy user rights	Right to be Informed (Articles 13 & 14)	- Organisations must provide clear information about how they use, store, and share personal data via privacy notices.
	Right of Access (Article 15)	- Individuals can request a copy of their personal data (a Data Subject Access Request or DSAR) to know what is held, why, and to whom it is disclosed.
	Right to Rectification (Article 16)	- Individuals can ask to correct inaccurate or incomplete data.
	Right to Erasure (Article 17)	- Individuals can request the deletion of their personal data, often used when data is no longer necessary, consent is withdrawn, or there is an objection.
	Right to Restrict Processing (Article 18)	- Instead of erasure, individuals can ask to limit how their data is used, keeping it stored but not actively processed.
	Right to Data Portability (Article 20)	- Individuals can request to receive their data in a structured, commonly used, machine-readable format to transfer it to another controller.
	Right to Object (Article 21)	- Individuals can object to processing based on legitimate interests, public interest, or for direct marketing, which must be honoured.
	Rights Related to Automated Decision-Making & Profiling (Article 22)	- The right not to be subject to a decision based solely on automated processing, including profiling, that has legal or significant effects.
Additional user rights	Right to Withdraw Consent	- Where processing is based on consent, individuals can withdraw it at any time.
	Right to Complain	- Individuals have the right to lodge a complaint with a supervisory authority.

Table 13 user rights

All data privacy user rights in Table 13 are included in this policy:

- User rights a mandatory.

- User rights must be understood by the Data Privacy Board.
- User rights must be actioned within a reasonable timeframe:
    - Data Subject Access Requests (DSARs) must be processed with 30 days from the date the request was received; but not including authorisation time.
    - Complex Data Access Requests must be processed with 90 days from the date the request was received; but not including authorisation time.

2.11 Auditing

Table 14 summarises the data privacy auditing:

Category	Component(s)	Item(s)
Data privacy auditing	Data collection	- As defined in section 2.5.
	Data used	- As defined in section 2.6.
	Data not used	
	Data sharing	- As defined in section 2.7.

Table 14 auditing

All data privacy auditing in Table 14 are included in this policy:

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

2.12 Reporting

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

- Data privacy compliance.
- Data privacy deviations.

Table 15 summarises the reporting schedule of this data privacy policy:

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

Table 15 reporting

2.13 Roles

Table 16 details the roles and responsibilities to support the data privacy policy:

Role	Responsibility	Description

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

Table 16 roles and responsibilities

2.14 Key performance indicators

Table 17 summarises the key performance indicators and success criteria for the implementation and management of this data privacy policy:

Deliverable	Review frequency (every)	Objective
Improvement of data privacy.	52 week(s).	Complete.
Reduction of privacy breaches.	52 week(s).	Complete.

Table 17 key performance indicators