CYBER STANDARD DOCUMENT

INFORMATION MANAGEMENT

ABSTRACT:

This Standard defines the requirements to implement Information Management as mandated in the National Community Security Policy. It encompasses the management of policing information within the OFFICAL tier of the Government Security Classification model.

ISSUED	December 2023
PLANNED REVIEW DATE	October 2024
DISTRIBUTION	Community Security Policy Framework Members
STANDARD VALIDITY STATEMENT This document is due for review on the date shown above. After this date, the document may become invalid. Members should ensure that they are consulting the currently valid version of the documentation.	

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Sanjay Gurung	Updated Requirements, Abstract	05/05/23
0.2	Sanjay Gurung	Updated Purpose and Scope, Terms and Abbreviation	21/09/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for Cyber standards	30/11/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
https://www.ncsc.gov.uk/collection/10-steps	Web Page	05/2021
College of Policing Information Management Authorised Professional Practice	See College of Policing website	09/2023

Terms and Abbreviations

Terms	Name
ACL	Access Control List
CIS	Centre for Internet Security
CSF	Cloud Security Forum
CSP	Community Security Policy
DLP	Data Leakage Prevention
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
GSCP	Government Security Classification Policy
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ISF	Information Security Forum
ISO	International Organisation for Standardisation
JML	Joiners Movers Leavers
MV	Management Vetting
MFA	Multi Factor Authentication
NCPSB	National Cyber Policy and Standards Board
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NMC	National Management Centre
NPCC	National Police Chiefs' Council
PAM	Privileged Access Management
PDS	Police Digital Service
PIAB	Police Information Assurance Board
PII	Personally Identifiable Information
RBAC	Role Based Access Control
RV	Recruitment Vetting
SAL	Security Aspects Letter
SbD	Secure by Design
SFTP	Secure File Transfer Protocol
SIRO	Senior Information Responsible Owner
SoGP	Standard of Good Practice
SWG	Security Working Group
SyAP	Security Assessment for Policing
TLS	Transport Layer Security
TPAP	Third Party Assurance Process
UK DPA 18	UK Data Protection Act 18
VPN	Virtual Private Network

Contents

Community Security Policy Commitment

National policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy (NCSP) Framework and associated documents sets out national policing requirements for handling policing information at the OFFICIAL classification tier as stated in the Government Security Classification Framework.

Introduction

This Information Management standard specifies requirements for secure management of policing information throughout the complete information lifecycle. It aims to provide members of the community of trust with clear direction to protect confidentiality, integrity and availability of policing information, and compliance with legal, regulatory, and contractual requirements.

Policing processes and stores a vast amount of sensitive information thus it is critical to have robust Information Management practices in place to prevent risks of data breaches, data loss, loss of public confidence, reputational damage, financial penalties etc.

Owner

National Chief Information Security Officer (NCISO)

Purpose

This standard helps organisations demonstrate compliance with the following NCSP policy statements:

Information Management

- To establish Information Management practices and responsibilities to protect policing information against corruption, loss, and unauthorised disclosure.
- To securely manage policing information throughout all stages of the information lifecycle – create, process, transmit, store and dispose.
- To align policing to the Government Security Classification Policy (GSCP) and protect policing information accordingly to its classification tier.

Audience

This standard is aimed at:

- Any member of the policing Community of Trust who has access to policing information or national policing systems.
- Member Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs), Information Security Officers (ISOs), Data Protection Officers (DPO), information security practitioners
- Information & Cyber risk practitioners and managers.
- Suppliers acting as service providers or developing products or services for members of the policing community of trust who may have access to policing information assets.
- Auditors providing assurance services to PDS or policing.

Scope

1. This standard applies to all policing information classified at the OFFICIAL tier. The requirements described in this standard are the minimum baseline for all levels of classification under the GSCP.
2. OFFICIAL information marked SENSITIVE is information that is not intended for public release and that is of at least some interest to threat actors (internal or external), activists or the media. OFFICIAL information that uses the SENSITIVE marking is likely to be of interest to threat actors due to its sensitivity or topical significance. A compromise could cause moderate, short-term damage. Such information should be identified using the SENSITIVE marking and additional handling controls apply.
3. The requirement for SECRET assets is described separately to this standard as the controls are in addition to those needed for OFFICIAL. For SECRET and TOP SECRET systems and information guidance should be sought from the assurer or IAO.
4. This standard will be supported by the policing security classifications guideline.
5. Policing information can include in the form of digital, physical, and unrepresented such as ideas, knowledge and thoughts that are intangible.
6. This standard applies to any member of the policing Community of Trust and applicable third parties to the policing community.

Requirements

This section details the minimum requirements to implement effective Information Management to securely protect policing information.

Ref.	Minimum requirement	Control reference	Compliance Metric
1	**Information Security Governance**		
1.1	Identify and document all legal, regulatory, contractual requirements relevant to information security and the organisation's approach to meet these requirements. **Examples of relevant requirements:** • UK DPA 18 • GDPR • NPCC PDS standards • HMG Security Policy Framework • Contracts with suppliers	ISF IM 2.1 ISF IM 2.2 ISF IM 1.3 ISO 27002:2013 18.1.1 ISO 27002:2022 5.31 NIST CSF ID.GV-3 Security Governance Standard	Review of information security policies, procedures, and contracts to determine relevant requirements are addressed and managed
1.2	Define Information security roles and responsibilities for the entire workforce including third party stakeholders to securely protect organisation's information assets. **Examples of roles and responsibilities:** • SIRO – accountable for protecting Police force's data and owner of information security risks • IAO – responsible for management of information asset • ISO – responsible for information assurance of Police force's data • DPO – responsible for ensuring compliance with data protection laws	ISO 27002:2013 6.1.1 ISO 27002:2013 7.2.1 ISO 27002:2022 5.2 ISO 27002:2022 5.4 ISO 27002:2022 5.9 NIST CSF ID.GV-2 NIST CSF ID.AM-6 NIST CSF PR.AT-1 NIST CSF PR.AT-2 NIST CSF PR.AT-3 NIST CSF PR.AT-4 NIST CSF PR.AT-5 Security Governance Standard	Review organisation chart, roles and responsibilities documents, user attributes, contracts with suppliers Interview staffs, practitioners, third party stakeholders and senior managers
1.3	Establish and maintain segregation of duties and principle of least privilege to reduce the risk of fraud, error and bypassing of information security controls that arises from conflicting duties and areas of responsibility. Lack of segregation of duties can present opportunities for unauthorised modification or	ISO 27002:2013 6.1.2 ISO 27002:2013 9.1.2 ISO 27002:2013 9.2.3 ISO 27002:2013 9.4.1 ISO 27002:2013 9.4.4 ISO 27002:2013 9.4.5 ISO 27002:2022 5.3	Review and audit roles and responsibilities, user access privileges, user attributes

Ref.	Minimum requirement	Control reference	Compliance Metric
	misuse of the organisation's information assets and other assets. **The following are examples of activities that require segregation:** • Initiating, approving, and executing a change • Requesting, approving, and implementing access rights • Designing, implementing, and reviewing code • Using and administering applications • Using applications and administering databases • Designing, auditing, and assuring information security controls	ISO 27002:2022 5.15 ISO 27002:2022 8.2 ISO 27002:2022 8.3 ISO 27002:2022 8.18 ISO 27002:2022 8.4 NIST CSF PR.AC-4	Interview staff, practitioners, third party stakeholders and senior managers
2	**Collecting and Handling information**		
2.1	Collection of information in policing should have regard for these key principles from the College of Policing Information Management Authorised Professional Practice (APP): • A record must have been created for a policing purpose or corporate information including other organisational information, such as human resources (HR) or finance records, minutes of meetings, policies and procedures. • All records must comply with the data quality principles. Such as POLE standards and Data Protection requirements. • A record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose. • Before recording information, checks should be made in other business areas to see whether the information is already held, thereby avoiding unnecessary duplication. • If information is recorded on an individual who is the subject of an existing record, the record should reflect this.	College of Policing Information Management Authorised Professional Practice (APP) DPA 18	Review information management policy and collection processes Records to evidence requirements being made Interview staff, senior managers

Ref.	Minimum requirement	Control reference	Compliance Metric
	- If it becomes apparent that the information being recorded is connected to other information, it must be appropriately linked. - Police information must be recorded as soon as is practicable, in accordance with the standards relating to the business area in which the information is held. - Apply the appropriate government security classification. - Treat unmarked information as OFFICIAL. Liaise with authors if in doubt as to the classification or handling instructions. - Where appropriate, the source of the information should be recorded to ensure accuracy and to assist in requesting further information.		
2.2	Establish an information classification policy based on the Government Security Classification Policy (GSCP) which applies to all forms of information including digital, physical, and unrepresented. Classification provides people who deal with information with a concise indication of how to handle and protect it. **GSCP classifications:** - Official/Official-sensitive - Secret - Top Secret **GSCP classification is based on:** - Sensitivity of the information and its importance to National security or if the public interest would be severely damaged if the information were to be disclosed - The harm that could be caused by the mismanagement of information - The need to restrict access to those with a legitimate requirement for information based on their role and responsibilities	CIS 3.8 ISF IM1.2 NIST CSF ID.AM-5 NIST CSF ID.GV-1 ISO 27002:2013 8.2.1 ISO 27002:2022 5.12 Government Security Classification Policy	Review information classification policy and audit of documents to determine effective classification activities

Ref.	Minimum requirement	Control reference	Compliance Metric
2.3	Establish an information labelling procedure in accordance with classification policy to indicate the level of sensitivity of information and the required level of protection. **Examples of labelling:** • Physical labels • Headers • Metadata • Watermarks	ISO 27002:2022 5.13 ISO 27002:2013 8.2.2 NIST CSF ID.AM-5 NIST CSF ID.GV-1 NIST CSF PR.DS-5	Review labelling policy and processes, and audit of documents to determine effective labelling activities
2.4	Establish and maintain an inventory of information assets (Information Asset Register - IAR) to identify and manage organisation's information assets and risks to them throughout its lifecycle. An information asset should be recorded in the IAR if it would cause severe organisational consequences if it was unavailable or corrupted. A role shall be assigned to be responsible as Information Asset Owner (IAO) who will be responsible for the proper management of information assets for their area of operations / business.. The IAR supports identifying and protecting information assets, risk management, compliance, incident response, upgrade, and disposal. The IAR shall be maintained and updated to ensure that it is current and accurate for it to be effective. **Employ following attributes but not limited to:** • Owner • Location • Access control requirements • Impact of loss of availability, confidentiality, and integrity • Regulatory requirements • Sensitivity (classification)	CIS 3.2 ISO 27002:2013 8.1.1 ISO 27002:2013 8.1.2 ISO 27002:2022 5.9 NIST CSF ID.AM-1 NIST CSF ID.AM-2	Review and audit information asset inventories Interview IAOs and practitioners

Ref.	Minimum requirement	Control reference	Compliance Metric
	• Whether Personally Identifiable Information (PII) • Risk appetite • Asset end of life / disposal / decommissioning		
2.5	Establish and maintain an inventory of data flows within organisation’s systems and networks. **Data flow diagrams can support security in several ways:** • Identify when information is at rest and in transit • Identify when information is shared externally • Identify which users and systems have access to which data • Ensure that the Information Asset Register reflects assets and data flows • Identify critical information processes • Enable the notification of affected users, systems, and vendors in the event of a security breach or incident • Establish baseline and thresholds to detect anomalies or malicious actions	CIS 3.8 ISO 27002:2013 13.2.1 ISO 27002:2022 5.14 NIST CSF ID.AM-3 NIST CSF DE.AE-1	Review and examine data flow diagrams
2.6	Identify and meet the requirements regarding the preservation of privacy and protection of Personally Identifiable Information (PII) data according to applicable laws and regulations and contractual requirements. **Examples of relevant best practices:** • Apply appropriate technical and organisational measures such as encryption, access control, data masking • Notify data breach to regulators, authorities, and data subjects appropriately and in a timely manner • Secure handling of PII	ISO 27002:2022 5.34 ISO 27002:2013 18.1.4 NIST CSF DE.DP-2 NIST CSF ID.GV-3	Review information asset inventory, contracts with third parties, data protection practices, DPIA process IT health check reports & remedial action plans.

Ref.	Minimum requirement	Control reference	Compliance Metric
2.7	Implement appropriate procedures and controls to protect intellectual property rights to ensure compliance with legal, statutory, regulatory, and contractual rights. Intellectual property rights include software or document copyright, design rights, trademarks, patents, and source code licenses. **Examples of relevant best practices:** • Define compliant use of software and information products • Acquiring software only through known and reputable sources to ensure that copyright is not infringed upon • Maintaining appropriate asset registers and identifying all assets with requirements to protected intellectual property rights	ISO 27002:2022 5.32 ISO 27002:2022 5.9 ISO 27002:2022 5.10 ISO 27002:2013 8.1.1 ISO 27002:2013 8.1.2 ISO 27002:2013 8.1.3 ISO 27002:2013 18.1.2 NIST CSF ID.AM-1 NIST CSF ID.AM-2 NIST CSF ID.GV-3	Review Intellectual property rights practices and asset registers
2.8	Establish policies and rules for acceptable use and handling of information to ensure information is appropriately protected, used, and handled. **Examples of rules for acceptable use of information:** • Expected and unacceptable behaviours of individuals from an information security perspective • Permitted and prohibited use of information • Access restrictions supporting protection requirements for each level of classification	ISO 27002:2022 5.10 ISO 27002:2013 8.1.3 NIST CSF ID.GV-1 NIST CSF ID.GV-2 NIST CSF ID.GV-3	Review of Acceptable Use Policies of information Interview staff, practitioners, third party stakeholders and senior managers
2.9	Employ information handling based on “Handling Policing Data Guideline” to ensure protection of information throughout all stages of the information lifecycle - Create, Store, Use, Share, Archive, Destroy. **Minimum measures to consider when handling and securing information:**	ISO 27002:2013 8.2.3 ISO 27002:2022 5.10 NIST CSF ID.GV-2 NIST CSF ID.GV-3	Review secure data handling processes, supplier contracts Audit of personnel security, vetting levels

Ref.	Minimum requirement	Control reference	Compliance Metric
	• Personnel security e.g. vetting clearance level applicable • Physical security e.g. security furniture • Technical security e.g. encryption **See also:** • Handling Policing Data Guideline GSCP		
2.10	All Individuals including external parties handling policing information should be appropriately vetted in accordance with their lawful need for access. **See also:** People management standard APP Vetting	ISO 27002:2022 6.1 ISO 27002:2013 7.1.1 NIST CSF PR.IP-11	Review vetting policy, supplier contracts Audit of personnel security, vetting levels, and register
2.11	Ensure access to information is authorised based on lawful need to know and principle of least privilege, and access is continually managed. Implement and maintain secure access controls to prevent unauthorised access to information and information systems. **Examples of relevant best practices:** • Role Based Access control (RBAC) • Joiners, Movers, Leavers (JML) Policy • Access Control list (ACL) • Privilege Access Management (PAM) • Multi-Factor authentication (MFA)	ISF IM1.6 ISO 27002:2022 5.15 ISO 27002:2022 5.16 ISO 27002:2022 5.18 ISO 27002:2022 8.2 ISO 27002:2013 9.1.1 ISO 27002:2013 9.1.2 ISO 27002:2013 9.2.1 ISO 27002:2013 9.2.2 ISO 27002:2013 9.2.3 ISO 27002:2013 9.2.5 NIST CSF PR.AC-4 NIST CSF PR.PT-3	Review access management policy and procedures Audit IAM tools, PAM tools, user permissions, password policies
2.12	All users including privileged users handling and administering policing data are informed, trained, and understand their roles and responsibilities. **Some benefits of training and awareness:** • Prevent accidental data breaches • Protection against cyber threats e.g. phishing emails, ransomware • Build a security culture • Effective incident response	ISO 27002:2022 6.3 ISO 27002:2013 7.2.2 NIST CSF PR.AT-1 NIST CSF PR.AT-2 NIST CSF PR.AT-3 NIST CSF PR.AT-4 NIST CSF PR.AT-5	SyAP assessment of: NIST CSF PR.AT.1 NIST CSF PR.AT.2 NIST CSF PR.AT.3 NIST CSF PR.AT.4 NIST CSF PR.AT.5 Review training and awareness policy, incident response policy, data

Ref.	Minimum requirement	Control reference	Compliance Metric
	See also: - People management standard		handling procedures, AUP Audit training and awareness activities, campaigns Interview staffs, practitioners, third party stakeholders and senior managers
3	**Information storage**		
3.1	Ensure information in all forms is securely stored at rest to protect against unauthorised disclosure, tampering and loss. Implement physical and logical access controls so that only authorised users can access and modify information. **Examples of relevant best practices:** - Appropriately encrypt data at rest e.g., disc encryption, file encryption, server/client-side encryption - Locking sensitive documents in suitable security cabinets - Restrict and review access privileges to sensitive information - Information systems are appropriately assured - Use of assured end point devices - Secure areas - Secure furniture	CIS 3.11 ISO 27002:2013 6.2.1 ISO 27002:2013 11.2.9 ISO 27002:2013 9.2.3 ISO 27002:2013 8.3.3 ISO 27002:2022 7.7 ISO 27002:2022 7.9 ISO 27002:2022 7.10 ISO 27002:2022 8.1 ISO 27002:2022 8.2 ISO 27002:2022 8.24 NIST CSF PR.DS-1 NIST CSF PR.PT-2 NIST CSF PR.PT-3	Review data at rest policy Examine physical access controls, secure cabinets Audit physical security controls, PASF / TPAP
3.2	Information should be backed up regularly to ensure data can be recovered in case of any disaster, cyber-attack, or system crash.	ISO 27002:2022 8.13 ISO 27002:2022 8.24 ISO 27002:2013 12.3.1 NIST CSF PR.DS-4	Review information back-up policy

Ref.	Minimum requirement	Control reference	Compliance Metric
	Backups should support Business Continuity Plans and Disaster Recovery Plans. Backups should be tested after implementation and on a defined basis to ensure information is recoverable. Ensure that data backup responsibilities are understood when using Cloud Services. **Examples of back-up best practices:** • Off-site storage • Encrypt back-ups • Regular and frequent back-ups • Automated back-ups • Test back-ups • Multiple back-ups – “3-2-1 rule”	NIST CSF PR.IP-4	Audit back-ups and back-up test activities/reports
4	**Using and processing information**		
4.1	Systems and services that processes policing data should undergo appropriate information assurance and governance processes to ensure adequate protection of Confidentiality, Integrity, Availability and Privacy of Information. **Examples of relevant processes:** • PDS Security by design (SbD) • Security governance • DPIA • Business impact analysis • Threat profiling • Supplier assurance • PASF / TPAP • Risk assessment • ITHC	ISO 27002:2013 6.1.5 ISO 27002:2013 14.1.1 ISO 27002:2013 14.2.1 ISO 27002:2013 14.2.5 ISO 27002:2022 5.8 ISO 27002:2022 8.25 ISO 27002:2022 8.27 NIST CSF PR.IP-2	Review local supporting standards and supporting procedures. Audit information assurance processes and system assurance documents Examine system ITHC reports, Remediation Action plans, Risk assessments,
4.2	Third parties managing and processing policing information should undergo Third-Party Assurance Process (TPAP) and meet the organisation’s security requirements.	ISO 27002:2013 6.1.1 ISO 27002:2013 7.2.2 ISO 27002:2013 15.1.1	Review organisation’s internal TPAP process, supplier contracts, SAL, PASF

Ref.	Minimum requirement	Control reference	Compliance Metric
	Ensure robust contracts are in place with third party stakeholders to protect policing information appropriately. **Examples of relevant practices:** • Police Digital Service (PDS) TPAP • Supplier Assurance • Security Aspects Letter (SAL) / Security Standards Agrement	ISO 27002:2013 15.1.2 ISO 27002:2013 15.2.1 ISO 27002:2013 15.2.2 ISO 27002:2022 5.2 ISO 27002:2022 5.19 ISO 27002:2022 5.20 ISO 27002:2022 5.21 ISO 27002:2022 5.22 ISO 27002:2022 5.23 ISO 27002:2022 6.3 ISO 27002:2022 8.30 NIST CSF ID.AM-6 NIST CSF PR.AT-3	/ TPAP report, Service Level Agreements set with suppliers Audit third party providers' controls and processes determining organisational requirements are met continually
4.3	Employ protections against data leakage and loss with Data Loss Prevention/Data Leakage Prevention (DLP). DLP monitor endpoint devices, systems, and networks to ensure sensitive data to prevent sensitive information from being disclosed to unauthorised individuals or systems.	CIS 3.13 ISO 27002:2022 8.12 NIST CSF PR.DS-5	Review DLP process Audit DLP tools Testing of DLP controls
4.4	Employ data masking techniques where applicable to limit the exposure of sensitive data including PII to comply with legal, statutory, regulatory, and contractual requirements. **Examples of data masking techniques:** • Obfuscation • Anonymisation • Pseudo-anonymisation • Dynamic data masking	ISO 27002:2022 8.11 ISO 27002:2013 NIST CSF PR.DS-5	Review data masking policies and processes Interview practitioners, senior managers, DPO
4.5	Employ clean desk and clear screen policy to reduce the risk of unauthorised access, loss of and damage to information on desks, screens and in	ISO 27002:2013 11.2.9 ISO 27002:2013 11.1.4	Review clean desk and clear screen policy

Ref.	Minimum requirement	Control reference	Compliance Metric
	other accessible locations during and outside normal working hours. **Examples of relevant best practices:** • Locking away sensitive or critical business information • Protecting user endpoint devices by key locks • Clearing sensitive or critical information on whiteboards and other types of displays when no longer required • Turning off pop-ups on screens during presentations or screen sharing	ISO 27002:2013 11.2.1 ISO 27002:2022 7.7 ISO 27002:2022 7.5 ISO 27002:2022 7.8 NIST CSF PR.IP-5	Audit physical sites and facilities
5	**Information sharing**		
5.1	Establish Information transfer policy, information sharing agreements and security agreements with all individuals or third parties who access critical or sensitive information and systems. Information should only be shared with authorised parties based on lawful need to know principle and appropriate business case. Ensure security obligations are clearly communicated to all employees or external individuals and formally accepted, providing legal and contractual protection. **Examples of relevant best practices:** • Terms and conditions of employment • Non-disclosure agreements (NDA) • Robust contractual obligations • Information sharing agreements	ISO 27002:2022 5.14 ISO 27002:2022 5.20 ISO 27002:2022 6.6 ISO 27002:2013 13.2.2 ISO 27002:2013 13.2.1 ISO 27002:2013 15.1.2 ISO 27002:2013 13.2.4 NIST CSF PR.AC-3 NIST CSF PR.PT-4	Review information transfer policy and process, non-disclosure agreement, third party contracts, SAL, employment terms and conditions Interview staff, practitioners, and senior managers
5.2	Ensure information is appropriately protected in transit from unauthorised disclosure. **Examples of relevant best practices:** • Appropriately encrypt data in transit e.g. TLS 1.2 • Use secure remote access e.g. VPN	CIS 3.10 ISF IM1.4 ISO 27002:2022 5.14 ISO 27002:2022 8.24 ISO 27002:2013 13.2.1	Review data in transit policy, secure remote access policy, cryptography policy

Ref.	Minimum requirement	Control reference	Compliance Metric
	• Use secure removable media e.g. FIPS 140-2 compliant • Use secure protocols to transfer data e.g. SFTP • Secure email channels e.g. mutual TLS **See also:** • Cryptography standard	ISO 27002:2013 13.2.2 ISO 27002:2013 13.2.3 NIST CSF PR.AC-3 NIST CSF PR.DS-2 NIST CSF PR.DS-5 NIST CSF PR.PT-4	Testing and ITHC of cryptography controls
5.3	Physical storage media transfer including paper should be secure to protect the data from unauthorised access, tampering and loss. **Examples of relevant best practices:** • Use approved courier • Secure storage media • Use tamper evident bags, containers • Ensure correct addressing and transportation of the message **See also:** • Physical asset management standard	ISO 27002:2022 5.14 ISO 27002:2022 5.10 ISO 27002:2022 7.10 ISO 27002:2013 13.2.1 ISO 27002:2013 13.2.2 ISO 27002:2013 8.2.3 ISO 27002:2013 8.3.1 ISO 27002:2013 8.3.3 NIST CSF PR.AC-2 NIST CSF PR.DS-3 NIST CSF PR.PT-2	Review storage media transfer policy Interview staff, practitioners, and senior managers Audit storage media transfer process, devices, logs
5.4	Ensure verbal transfer of information is protected to prevent unauthorised disclosure. **Examples of relevant best practices:** • Need to know and least privilege principles. • Conduct conversations in settings appropriate to their sensitivity. • Ensure appropriate room controls are implemented e.g., soundproofing, closed doors • Only leave non-sensitive messages on voicemail systems. • Be screened to the appropriate level to listen to the conversation	ISO 27002:2022 5.14 ISO 27002:2013 13.2.1 ISO 27002:2013 8.3.3	Review local information handling policies, employment terms and conditions Interview staffs and senior managers

Ref.	Minimum requirement	Control reference	Compliance Metric
6	**Information Archive and Retention**		
6.1	Information and records should be securely retained in accordance with organisational, legal, statutory, contractual, and regulatory requirements. Identify period of retention requirements and securely protect the data and records from data manipulation, unauthorised disclosure, loss, and corruption.	CIS 3.4 ISO 27002:2022 5.31 ISO 27002:2022 5.33 ISO 27002:2013 18.1.1 ISO 27002:2013 18.1.3 NIST CSF ID.GV-3	Review information retention policy Audit retained data and records
7	**Secure information deletion**		
7.1	Securely sanitise information stored in information systems, devices, or storage media for re-use to prevent data breaches and unauthorised disclosure. Media sanitisation ensures residual data is unrecoverable and unreadable. Media can be any device that stores data e.g., external hard drives, USB drives, memory cards, mobile devices, laptops, office equipment such as printers, photocopiers, cameras. **Examples of sanitising techniques:** • Data overwriting • Magnetic degaussing • Crypto shredding	ISO 27002:2022 7.10 ISO 27002:2022 7.14 ISO 27002:2022 8.10 ISO 27002:2013 11.2.7 ISO 27002:2013 8.3.2 NIST CSF PR.DS-3 NIST CSF PR.IP-6	Review information sanitisation policy and practices Audit sanitisation practices and records
7.2	Information stored in information systems, endpoints, storage media and cloud systems should be securely deleted and disposed when no longer needed to prevent unauthorised access, data breaches and non-compliances with legal and regulatory requirements. Verify deletion method provided by cloud service providers and suppliers is acceptable and meets organisation's secure deletion requirements. **Examples of deletion techniques:** • Physical destruction • Degaussing	CIS 3.5 ISO 27002:2022 8.10 ISO 27002:2022 7.10 ISO 27002:2022 7.14 ISO 27002:2013 11.2.7 ISO 27002:2013 8.3.2 NIST CSF PR.DS-3 NIST CSF PR.IP-6	Review secure data deletion policy and practices Audit secure data deletion practices and records

Ref.	Minimum requirement	Control reference	Compliance Metric
	• Crypto shredding • Use approved, certified providers of secure disposal services		
8	**Test data**		
8.1	Only test data should be used in a testing environment when conducting tests on system and any exceptions needs to gain an authorisation from IAO or system owner. **Several rationales of using test data:** • Preserve integrity of real data • Comply with legal and compliance requirements • Prevent data breach • Prevent loss of real data	ISO 27002:2022 8.33 ISO 27002:2013 14.3.1 NIST CSF PR.DS-7	Review testing policies and practices
9	**Logging and monitoring**		
9.1	Employ logging and monitoring of activities in information systems to detect anomalous activities, compromises, attempted bulk exports of data and prove non-repudiation. Examples of relevant best practices: • Security related events should be recorded in logs, stored centrally, protected against unauthorised change, and analysed on a regular basis. • To help identify threats that may lead to an information security incident, maintain the integrity of important security related information, and support forensic investigations. **See also:** • Technical Security Management standard	ISO 27002:2022 8.15 ISO 27002:2022 8.16 ISO 27002:2013 12.4.1 ISO 27002:2013 12.4.2 ISO 27002:2013 12.4.3 NIST CSF PR.PT-1 NIST CSF RS.AN-1	Review Logging and monitoring policy and practices Audit logs and examine monitoring use cases

10	**Incident management and Reporting**		
10.1	Establish an incident management process and incident response plan to ensure quick, effective, consistent, and orderly response to information security incidents, including communication on information security events. Roles and responsibilities to carry out the incident management procedures should be determined and effectively communicated to the relevant internal and external interested parties. All individuals within the organisation and suppliers should report incidents using the organisation's defined reporting procedure. **See also:** • Threat and Incident management standard	ISO 27002:2022 5.24 ISO 27002:2022 5.25 ISO 27002:2022 5.26 ISO 27002:2022 5.27 ISO 27002:2022 6.8 ISO 27002:2013 16.1.1 ISO 27002:2013 16.1.2 ISO 27002:2013 16.1.3 ISO 27002:2013 16.1.4 ISO 27002:2013 16.1.5 ISO 27002:2013 16.1.6 NIST CSF RS.RP-1 NIST CSF RS.CO-1 NIST CSF RS.CO-2 NIST CSF RS.AN-1 NIST CSF RS.AN-2 NIST CSF RS.AN-4 NIST CSF RS.MI-1 NIST CSF RS.MI-2	Review incident management policy and incident response plan Interview staff, practitioners, and senior managers Audit incident logs
10.2	Establish and maintain contact with relevant authorities to ensure appropriate flow of information takes place with respect to information security between the organisation and relevant legal, regulatory, and supervisory authorities. Organisation should specify when and by who authorities should be contacted and how identified information security incidents should be reported in a timely manner. **Examples of relevant authorities:** • ICO • PIAB • NPCC • PDS	ISO 27002:2022 5.5 ISO 27002:2013 6.1.3 NIST CSF RS.CO-2	Review processes for contacting authorities Interview staff, practitioners, and managers Audit logs and records of contacting authorities

10.3	Establish and maintain contact with special interest groups to ensure appropriate flow of information takes place with respect to information security. Special interest groups can provide several benefits such as stay up to date with relevant security information, receive early warnings of security alerts, exchange information about new threats, gain access to specialist information security advice etc. **Examples of special interest groups:** • NCSC • ISF • PDS • NMC	ISO 27002:2013 6.1.4 ISO 27002:2022 5.6 NIST CSF ID.RA-2	Review processes for contacting special interest groups Interview staff, practitioners, and managers Audit logs and records of contacting special interest groups
10.4	Formalise and communicate a disciplinary process to take against personnel and other relevant parties who have committed an information security policy violation. A disciplinary process ensures personnel and other relevant parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant parties who committed the violation. **See also:** • People Management standard	ISO 27002:2022 6.4 ISO 27002:2013 7.2.3	Review disciplinary process, employment terms and conditions, contractual terms

Communication approach

This standard will be communicated as follows:

1. Internal peer review by the members of the National Cyber Policy and Standards Working Group which includes PDS and representatives from participating forces.

2. Presentation to the National Cyber Policy and Standards Board for approval.

3. Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed with information security officers (ISOs) and Information Management teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.
Measurables generated by adopting this standard can also form part of regular cyber management.

Review Cycle

This Policy will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)