CYBER STANDARDS DOCUMENT

DECOMMISSIONING

ABSTRACT:
This standard is intended to provide a framework of controls to support the secure decommissioning of police information systems.

ISSUED	May 2025
PLANNED REVIEW DATE	May 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

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 Framework and associated documents sets out National Policing requirements for the decommissioning of police systems and information.

Introduction

The policing community use a wide range of systems and storage media. In addition to this, other forms of information also exist, such as paper. These assets, which contain sensitive information and often provide a critical business function, can be stored and processed within police premises, or those of third parties, such as partner organisations or suppliers. To manage the associated risk of this information and the availability of live services, it is necessary to implement a robust set of controls. The application of these controls will be dependent on the type of decommissioning activity being undertaken.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this document is to provide a framework of controls that an organisation must adopt in order to carry out decommissioning activities securely, managing cyber and information risk, whilst abiding by relevant laws and regulations. This decommissioning standard can be applied to a range of activities involving sensitive systems and information. This includes decommissioning applications, hardware, and locations storing and processing sensitive information in support of organisational objectives.

The standard provides supporting controls which must be implemented across an organisation prior to commencing decommissioning activity. For suppliers, this means implementing the controls during the contracting stage of any third-party agreements. Using the standard as a checklist of controls applied during decommissioning will likely result in an inability to comply with a number of controls. However, the Requirements section may be referred back to, in order to guide live decommissioning tasks.

The standard also provides a compliance metric for each control. This provides examples of evidence that an organisation should retain during decommissioning activities to provide confidence to internal stakeholders and audit personnel.

The requirements stated in this standard are mapped across from specialised industry standards, including:

- International Security Forum Standard of Good Practice (ISF SoGP) 2024
- International Organisation for Standardisation (ISO) 27002: 2013 & 2022
- Centre for Internet Security (CIS) (v8)
- National Institute for Standards and Technology (NIST) Cyber Security Framework (CSF) (v1.1 & v2.0 - to support future adoption)
- NIST Special Publications (e.g. 800-53r5)
- Cloud Control Matrix (CCM) (v4)

This standard should be considered alongside other relevant standards. Where another standard provides continuity of controls or is considered particularly relevant to the activity, it is referenced in the controls below.

Audience

This standard is aimed at:

- Member Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs), Information Security Officers (ISOs), Data Protection Officers (DPOs), information security practitioners.
- Information & Cyber risk practitioners and managers who are responsible for the implementation of suitable standards design to manage cyber risk, and evidencing compliance during audits.
- Programme or Project Managers who are responsible for the end-to-end delivery cycle of systems and infrastructure.
- Technical personnel who are responsible for the decommissioning of IT systems and infrastructure.
- 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

In Scope:

- Implementing organisational controls for planning and decommissioning assets that contain police information or provide operational police services.

Out of Scope:

- Decommissioning systems and data that are classified above OFFICIAL-SENSITIVE.
- Evidential material.

Requirements

The following controls aim to support organisations to achieve compliance with the following Security Assessment for Policing (SyAP) controls, within the context of decommissioning:

- NIST CSF v1.1:
  - PR.DS-3
  - PR.IP-6

- NIST CSF v2.0 (to support future adoption)
  - GV.SC-10
  - ID.AM-8
  - PR.PS-03
  - PR-PS-06

Additional NIST CSF controls have been included within the steps below. The implementation of these additional controls will support the organisation's overall ability to maintain holistic alignment to NIST CSF through any business change that comes with decommissioning.

To aid police forces, references to the Police Information and Records Management Code of Practice have been included at the end of each section, where applicable. These requirements have been included to signpost to the reader where additional consideration may be required in the context of decommissioning activities. It is important that designated roles within police forces have a deep understanding of the Code of Practice and the individuals responsible for these roles are engaged where appropriate during decommissioning activities.

Controls are provided in the logical order in which they may be encountered during decommissioning activity. However, the order of certain events may vary depending on the organisation and the activity being undertaken.

Ref.	Minimum requirement	Control reference	Compliance Metric
1.	**Identifying a business purpose, planning, and seeking approval to initiate decommissioning activities**		
1.1.	**Strategy** Include decommissioning of systems and facilities as a key component of any project or product, ensuring that delivery plans include the removal of any components no longer required. This includes any components used to facilitate delivery, such as development environments, or old technologies replaced by new. Reduce the organisation's attack surface and exposure to cyber risk by decommissioning any systems that are no longer required. Define and implement documented decommissioning plans for end-of-life, unsupported and obsolete components. Integrate cybersecurity considerations throughout the full system life cycle, including decommissioning. Time the decommissioning of assets to coincide with the point that assets reach their projected end of life date. Avoid situations where policy and procedures cannot be complied with. For example, where the swelling of a lithium battery on a device used beyond its expected lifespan presents a fire risk.	ISF SoGP 2024: SD4.4 NIST SP 800-88: 4.6	Routine decommissioning and planning activity can be evidenced in asset register item statuses, change management board minutes, and IT management or project documentation. The recorded activity can be justified and linked to planned equipment replacement projects (e.g. budget forecasts), or equipment end-of-life dates, rather than as a reactive decision to mitigate unseen risks.

Ref.	Minimum requirement	Control reference	Compliance Metric
1.2.	**Architecture** Further reduce the attack surface of the organisation's digital systems by removing architectural layers that are made redundant as a result of the planned decommissioning activity.	ISF SoGP 2024: TI2.1.7	Architecture roadmaps and board minutes.
1.3.	**Supplier Management** Establish a procedure (prior to the commencement of a contractual relationship) for the termination or exit of third-party services under both normal and adverse conditions. This will include procedures for removing access, returning data and other assets, along with the transition of any live services. This plan will also address technical, security, privacy, property and legal considerations.	NIST CSF v2.0: GV.SC-10 CRI Profile v2.0: EX.TR	Supply-chain risk management policy and procedure. Contractual clauses covering relevant scenarios of termination. Evidence of the return or deletion of the organisation's information in emails, logs, or media transport plans.
1.4.	**Authorisation** Obtain formal decommissioning approvals from the IAO, SIRO, and other key stakeholder groups, where necessary.	NIST CSF v1.1: ID.SC-1	Signed risk assessments, decommissioning, or movement plans. Emails or documents, electronically signed which provide authorisation for decommissioning, along with acceptance of plans.
1.5.	**Governance** Implement and follow organisational governance for decommissioning and disposal activity. Issue formal decommissioning notices to IT General Management Practices, IT Asset Management, and Change Control, including the reason, scope, and timeline for decommissioning.	NIST CSF v1.1: PR.IP-3	Emails or service management tool references, containing stakeholder communications, workflows and approvals.

Ref.	Minimum requirement	Control reference	Compliance Metric
1.6.	**Change Management** Conduct robust change management activities to ensure that changes are authorised, scheduled, and all risks are identified and managed. Determine a staged decommissioning plan and identify appropriate success and failure criteria for each stage. In each critical phase, provide a recovery plan to roll back the change to a previously working state. Implement the physical changes in a staged approach. As part of each stage assess to determine whether the success criteria has been met prior to moving into the next phase.	ITIL 4: Change Control ISO/IEC 27002:2022 8.32 COBIT 2019 BAI06	Change Management policy. Change board minutes. Change request forms.
2.	**Obtain an inventory and classification of assets to be decommissioned**		
2.1.	**Asset Lifecycle** Implement and develop documented procedures for managing the life cycle of hardware. Ensure the protection of the organisation's data throughout any decommissioning or transfer. See also NCSP Physical Asset Management standard For Radio terminals see also Code of Practice for Policing issued by the Home Office	ISF SoGP 2024: HE1.1.1 NIST CSF v2.0 / CRI Profile v2.0: ID.AM-08 NIST CSF v1.1: PR.DS-3: ITIL 4: Service Configuration Management COBIT 2019 BAI09	Asset Management policy. This includes asset onboarding, tracking, through to disposal. Sanitisation and Destruction policy.

Ref.	Minimum requirement	Control reference	Compliance Metric
2.2.	**Asset Inventory** Create a detailed inventory of all hardware, software, and data assets (e.g., servers, storage devices, licenses). Map assets in scope of decommissioning to the organisation's information asset registers and Configuration Management databases. Classify data and system sensitivity using organisational data classification policies. Identify accounts, data flows, and enterprise data within systems for decommissioning. See also NCSP Physical Asset Management standard	CIS Controls v8.0: 15.7: Securely decommission service providers ISO/IEC 27002:2022 (5.9): Inventory of information and other assets NIST CSF: ID.AM-01: Maintain an inventory of hardware assets ID.AM-02: Maintain an inventory of software assets ID.AM-03: Communication and data flow mapping	Asset Management policy. Contains suitable references to the management of assets. Asset register, with evidence of recent changes, or updates. Information Classification policy. Classification labels assigned to systems/data. Information Management policy. Data flow maps and information asset register, linked to information processing components.
2.3.	**Data Flow Mapping** Document a data flow map of systems in scope of decommissioning activity to provide an understanding of dependencies.	SP 800-53 Rev 5: CM-13: Data action mapping	Information Management policy. Data flow maps and information asset register, linked to information processing components.

Ref.	Minimum requirement	Control reference	Compliance Metric
2.4.	**Record of Processing Activities** Maintain the Data Controller and Data Processor records for personal data processing activities by assessing the decommissioning activity for any changes to processing activity. For example, details of the controller, purpose of processing, transfers to third countries or international organisations.	UK General Data Protection Regulation (GDPR): Article 30 Data Protection Act (DPA) 2018: Section 61	Information Management/ Data Protection policy. Updates to data processing records to coincide with recent changes.
3.	**Perform an Information/Cyber Risk Assessment**		
3.1.	**Risk Appetite** Consult the organisation's risk management policy to identify risk appetite applicable to the information assets and systems in scope of decommissioning. Identify the key roles and their responsibilities for risk ownership within the organisation to establish suitable individuals responsible for accepting risks on behalf of the organisation.	NIST SP 800-221A: GV.PO-1	The organisation has a risk management policy, which sets out the risk appetite for systems/information, roles, and responsibilities.
3.2.	**Risk Assessment** Conduct a risk assessment to identify sensitive data, regulatory obligations (e.g., UK GDPR), and dependencies on the infrastructure. Document potential threats arising from the planned activity. For example, a building sold to an external party is likely to expose the organisation to more threats than if the building were to be repurposed within the same organisation. Another example may be IT equipment that will be returned to a	NIST SP 800-53 Rev 5: RA-03 NIST SP 800-30 R1: Risk Assessment	Risk assessments covering decommissioning activities. Risk assessments align to organisational policy. For example, impact and likelihood ratings appear as directed in policy. Risks are accepted at the correct level, according to policy.

Ref.	Minimum requirement	Control reference	Compliance Metric
	supplier or sold to a third party, rather than destroyed on site. Document possible risks during the activity. For example, unauthorised access to sensitive information that is left in a building or on a device storage drive. Finally, identify and implement mitigating controls to reduce the severity of risks to within the organisation's risk appetite for each information type. It is important that organisations understand where there is flexibility to manage risk and where there is a specific compliance requirement to implement a control in order to meet laws, regulations, and standards.		
3.3.	**Risk Framework** Manage and respond to identified risks in accordance with organisational risk management policies. For more information on policing information risk management, consult the *National Police Information Risk Management Framework*.	SP 800-53 Rev 5: RA-07 COBIT 2019: APO12, APO12.06	Risk registers or risk assessments containing risk treatment plans for decommissioning-related risks. Registers and assessments align to organisational policy on risk management.
3.4.	**Data Protection Impact Assessment** Consider the impact to existing Data Protection Impact Assessments (DPIA) and whether there is a need to produce an assessment to cover the activity to be undertaken, or whether any amendments are required to existing assessments. Within the decommissioning risk assessment, ensure that regulatory requirements relating to data security	UK GDPR: Article 5(1)(f), Article 32, Article 35 DPA 2018: Section 64, Section 66	Security working group minutes covering data protection aspects. DPIA reviews or update entries on DPIA version control sheets. Specific changes resulting from decommissioning activity in the last 12-month period.

Ref.	Minimum requirement	Control reference	Compliance Metric
	are met throughout. It is important to engage with the Data Protection Officer where decommissioning activities have the potential to impact upon systems that process or store personal data.		
4.	**Secure Data Backup, Validation and Retention**		
4.1.	**Backup & Service Restoration Strategy** Implement the tools and systems to backup systems and recover from systems failure.	Code of Practice on UK Police Information and Records Management: Principle 5 (4.38), Organisational Capability (5.5) NIST SP 800-34 R1: Contingency Planning	Backup policy. Disaster recovery plans. Asset register entries for backup and recovery systems. Architectural diagrams showing backup systems and their purpose/function. Documented recovery procedures. Defined backup schedules.
4.2.	**Backup Management** Backup information required for legal, operational, or compliance purposes. Establish and implement data retention and deletion practices for physical and electronic data in accordance with requirements, laws and regulations. Validate backup integrity by testing backups.	ISO/IEC 27002:2022 8.13 ISO/IEC 27002:2013 12.3.1 CCMv4.0: DSP-16	Retention schedule contains the appropriate electronic information retention periods. Backup policy. Backup test outcomes in knowledge bases or in supplier service reports. Physical security policy includes requirements for physical security audits of sites containing backups.

Ref.	Minimum requirement	Control reference	Compliance Metric
4.3.	**Backup Security** Store backups with an appropriate level of protection, appropriate to the level of risk identified and consistent with other sites storing and processing the same information.	NIST CSF: PR.DS-01	
4.4.	**Physical Security** Implement and develop policies to record and manage the physical locations of data, including data backup locations *See also NCSP Physical and Environmental Security Management Standard.*	CCMv4.0: DSP-19	Backup policy details the approved backup storage locations. Physical security policy includes requirements for physical security audits of sites containing backups.
4.5.	**Backup Retention** Where information retention extends beyond the lifecycle of premises or systems. Retain and manage information in accordance with organisational policy, codes of practice, regulations, and laws. Engage the organisation's records management policy to ensure information is retained correctly.	SP 800-53 R5: SI-12	Retention policy. Retention schedule.
4.6.	**Codes of Practice** The retention of information must be a deliberately directed action, rather than simply keeping information in case it's needed in the future. Implement IT systems sufficient to meet legal and regulatory requirements.	Code of Practice on UK Police Information and Records Management: Principle 6 (4.40)	Emails or other formats of formal requests made to manually remove physical records no longer required. Confirmation of the completion of the required activity. Service requests for the manual deletion of information no longer required for retention. Technical policies, aligned to organisational policy enforcing the labelling and removal of data after a set period.

Ref.	Minimum requirement	Control reference	Compliance Metric
4.7.	**Regulations** Ensure backups comply with data protection requirements, such as the right to erasure and lawful destruction of personal information.	UK GDPR: Article 17 DPA 2018: Section 47	Organisational policies. Accepted timeframe for the removal or correction of records. Requests for records to be erased or corrected. Managed and completed via a workflow system. Product manuals and procedures for implementing the removal or correction of records held in backup.
4.8.	**Backup Formats** Keep backups in a format which is resilient to changes in the systems used to access the data. For example, storing data in non-proprietary format. Update file formats to ensure readability is maintained. Keep metadata intact with the original backup.	Code of Practice on UK Police Information and Records Management: Principle 6 (4.41)	Backup policy. Investigation of file formats used by backup systems. Documentation evidencing metadata storage.
4.9.	**Disposal of Backups** Dispose of records that are no longer needed or at the end of a retention period. Archive records for public interest purposes or securely destroy. Clearly record the purpose for archiving or destruction. Implement measures to prevent access to information or render unusable, until a physical destruction method can be applied. Conduct assessments to identify any records which need permanent archive in accordance with laws, regulations, or standards.	Code of Practice on UK Police Information and Records Management: Principle 7: Disposal	Data protection policy. Information management policy. Emails, service requests, and other workflow systems, evidencing the disposal, archive, or retention of information. Specific assessments undertaken to manage information, prior to physical destruction. Roles and responsibilities for individuals required to manage legal and regulatory requirements.

Ref.	Minimum requirement	Control reference	Compliance Metric
	Maintain a data processing contract when using a third-party provider to archive information.		Data processing agreements.
4.10.	**Bespoke Applications** Archive information stored or processed by end-user developed applications in accordance with retention requirements.	ISF SoGP 2024: UA2.1.12	Backup policy. Change board minutes.
5.	**Physical Decommissioning**		
5.1.	**Advanced Physical Searches** Utilise specific business skills and expertise where appropriate to verify that rooms, buildings and sites are clear of any sensitive information. Engage suitably trained personal for specialist searches.	Police Search Advisor (PolSA) Counter Terrorism Security Advisors (CTSA)	Organisational policy requiring final inspection of facilities, prior to reuse or disposal. Requests for PolSA. Where decommissioning activity has occurred, the outcomes of PolSA search are captured, or confirmation that one was not required.
5.2.	**Security Incident Management** Record and respond to any security incidents or near-misses during decommissioning that affect the confidentiality, integrity, and/or availability of information/systems. For more information on security incident management, consult the *Monitoring and Evaluation of Force Information Security Incidents Guideline*.	ISO/IEC 27002:2022 5.26	Information security incident management policy. Security incident reports. Details of the response to incidents. Investigation reports.
5.3.	**Personnel Security** Personnel with access to sensitive information or operational systems are vetted to an appropriate level to mitigate the risks they pose.	NIST CSF v1.1: PR.IP-11 ISO/IEC 27002:2022 6.1	Third-party personnel have vetting requirements stated within contract. Security aspects letter setting out assets and associated security levels.

Ref.	Minimum requirement	Control reference	Compliance Metric
	For more information on personnel security, consult the *People Security Management Standard*.		Vetting spot checks undertaken on third-party personnel during the decommissioning process.
6.	**Migration of systems and data**		
6.1.	**Supplier Agreements** In third-party agreements specify contractual requirements for data format (e.g. non-proprietary) upon contract termination. Document the length of time any data will be stored, along with the application of applicable security controls, laws and regulations. See also NCSP Third Party Assurance for Policing standard	CCMv4.0: IPY-04	Supply-chain management policy sets out the requirements for suitable information management controls to be implemented within third-party agreements. Contractual clauses in third-party agreements covering the termination of services, return of information, and security controls.
6.2.	**Secure Transfer** Develop and implement procedures for the secure transfer of equipment, data and information to an alternative location. Protect data in transit from unauthorised access, processing, loss, or corruption. Test, assess, and evaluate the effectiveness of controls to ensure the security of data during transfer. Ensure electronic data is protected using secure cryptographic algorithms, such as AES-256. Where available, use data obfuscation or masking where possible to render data illegible to unauthorised parties.	CCMv4.0: DCS-02 UK GDPR: Article 32 DPA 2018: Section 66	Organisational policy that covers the large-scale movement of data in a decommissioning or migration scenario. Removable media policy details the encryption requirements for removable storage drives. Physical security policy details the requirements for security of sites sending and receiving information. Risk assessments completed in response to the need to move information between locations. Network (or similar) Security policy, detailing the requirements for electronic data transfer.

Ref.	Minimum requirement	Control reference	Compliance Metric
	For more information on the secure transfer of information, consult the *NCSP Information Transfer Guideline*.		Commonly used mechanisms included in annual IT Health Checks. A review of the scope section will confirm this. Information Management policy setting out the requirements for physical transfers.
6.3.	**Regulations** Ensure that the target location/system(s) offer the required level of conformance with data protection requirements, such as the right to rectification or erasure. For example, ensure that a data subject's right to erasure is still achievable if the data is migrated to a new location or system.	UK GDPR / DPA 2018: Chapter 3 DPA 2018: Section 47	Contractual agreements. Procurement assessment of technical options. Requirements are included in non-functional requirements when tendering for systems.
6.4.	**Supply-Chain Assurance** Undertake appropriate checks to ensure a third party's reliability where they are used to process police data on behalf of a police force. Contracts must be in place prior to processing. For more information on supply-chain assurance in policing, consult the *Third-Party Assurance for Policing (TPAP) Standard*.	Code of Practice on UK Police Information and Records Management: Principle 4 (4.34)	Supply-chain management policy detailing the requirements for checks/assessments against third parties. Supply-chain risk assessments or records of TPAP audits against data processors. Contractual agreements for all data processing activities.
6.5.	**Data Processing Agreements** When using a data processor to carry out personal data processing on behalf of the controller, ensure a written contract between the controller and the processor is in place setting out mandatory data protection requirements.	DPA 2018: Section 59	Contracts in place for all data processors. Data protection requirements included in contracts.

Ref.	Minimum requirement	Control reference	Compliance Metric
6.6.	**Joint Controller Agreements** Joint controllers must transparently determine their responsibilities for compliance and designate a contact point for data subjects.	DPA 2018: Section 58	Data processing and joint controller agreements setting out compliance responsibilities between parties. Data privacy notice with the contact information of the responsible Data Protection Office.
6.7.	**Data Sharing Agreements** Documented procedures must be in place covering the transfer of information within the organisation and between the organisation and other parties.	ISO/IEC 27002:2022 5.14	Data sharing agreements setting out transfer responsibilities between parties.
6.8.	**Bespoke Applications** Decommission end-user developed applications by migrating any required data to a suitably secure platform and uninstalling the application.	ISF SoGP 2024: UA2.1.12	Asset register entries for decommissioned applications. Change board minutes and documents detailing any bespoke data migration plans.
7.	**Transporting assets for the purposes of migration, sanitisation, or destruction** **See also NCSP Information Transfer Guideline**		
7.1.	**Authorisation** Obtain formal authorisation for the transfer of assets.	ISO/IEC 27002:2013 11.2.5 ISO/IEC 27002:2022 7.10	Documented authority from information owners for the transportation of assets, including the intended outcomes (e.g. sanitisation, destruction, or migration).

Ref.	Minimum requirement	Control reference	Compliance Metric
7.2.	**Specialist Capabilities** Evaluate the use of specialist business capabilities to ensure the security of assets in transit. For example, using police officers to escort assets, where the impact resulting from compromise is determined to be High/ Very High.	N/A	Documented planning and discussion with organisational planning teams, responsible for organising specialist support. Risk assessments detailing specific measures for protecting assets in transit.
7.3.	**Electronic Protection** Protect data in transit from unauthorised access, processing, loss, or corruption. Test, assess, and evaluate the effectiveness of controls to ensure the security of data during transfer. Use a minimum of AES-256 encryption, protected with a strong password, which is communicated via a separate secure channel.	NIST CSF: PR.DS-1, PR.DS-2 UK GDPR: Article 32 DPA 2018: Section 66	Risk assessments and risk management plans. Commonly used mechanisms included in annual IT Health Checks. A review of the scope section will confirm this. Cryptographic policy stating the requirements for applying encryption in transit. Password policy stating the requirements for communicating passwords.
7.4.	**Physical Protection** Protect sensitive physical information in transit by using techniques, such as: • Minimising distribution • Separating from non-sensitive items • Securely packaging (i.e. double envelopes, tamper seals, and specialised packaging)	ISF SoGP 2024: IM2.2.5, IM1.5.8 CCMv4.0: IPY-03 NPSA (formerly CPNI) Secure Destruction of	Documented media transport plans. Risk assessments for the transportation of assets outside of the organisation. Documented information transfer agreements.

Ref.	Minimum requirement	Control reference	Compliance Metric
	• Clearly labelling with recipient details • Keeping records of authorised recipients • Tracking consignments • Using secure couriers (e.g. Royal Mail Special Delivery) • Recording consignment details (including time, date, classification, information details, etc.) A risk assessment conducted by suitably qualified personnel will identify suitable transit protection measures. Any information transfer agreements must specify the approved methods of transferring physical media Engage certified third-party logistics providers for transportation, ensuring compliance with data protection regulations.	Sensitive Items: (10. Transport of sensitive items)	Security aspect letters (or contractually binding clauses) stating the handling requirements for specific types of information. Supply-chain risk management policy defining the required controls for evaluating third-party compliance with organisational controls. Contractual agreement specifying security clauses.
7.5.	**Chain of Custody** Throughout any transfer, a chain of custody must be recorded as evidence to support the traceability and integrity of sensitive information. This information must be retained in accordance with the organisation's retention requirements. Responsibilities and liability in the event of an incident must be agreed and documented by all parties. Consider additional obligations that may apply in the case of assets under governance of Crypto or AccSec Custodian	ISF SoGP 2024: IM1.5.3 ISO/IEC 27002:2022 7.9(c), 5.14	Retention policy and schedule with entries covering information transfer records. Transfer documents detailing a signed and dated chain of custody for transfers. Contractual agreements stating responsibilities at all stages of transfer.

Ref.	Minimum requirement	Control reference	Compliance Metric
7.6.	**Unauthorised Access** Prevent unauthorised access opportunities to assets during transportation.	NIST CSF: PR.AC-2	Risk assessment of transfer plan. Media transport plans.
7.7.	**Removable Media** The use of any removable storage media must be covered by a policy or procedure detailing the controls to be applied.	ISO/IEC 27002:2022 7.10	Removable media policy.
8.	**Data Sanitisation and Secure Destruction**		
8.1.	**Acceptable Use of Assets** Ensure that business procedures are in place to delete data that is no longer required. This ensures that data is not kept for longer than is necessary and also helps to reduce the risk to information during decommissioning activities.	ISO/IEC 27002:2022 8.10	Information management and data protection policies. Decommissioning procedure. Asset management policy covering the responsibilities of the user in deleting information prior to returning assets. Records of information security incidents raised in response to assets being returned with data on.
8.2.	**Asset Decommissioning** Verify if storage media is contained within equipment or premises prior to decommissioning.	ISO/IEC 27002:2022 7.14	Data sanitisation and secure destruction policy, asset management policy, or decommissioning procedure, containing suitable checks to determine compliance.
8.3.	**Off-Site Sanitisation and Destruction** Develop and implement procedures for the secure destruction of equipment outside of the organisation's premises, where this is necessary. For example, if the organisation does not possess the necessary destruction equipment.	CCMv4.0: DCS-01	Data sanitisation and secure destruction policy.

Ref.	Minimum requirement	Control reference	Compliance Metric
	For physical assets, full disk encryption (data-at-rest) may be considered a control to mitigate risks during transit to a sanitisation or destruction facility. However, it must not be used to fully replace final sanitisation or destruction outcomes.		
8.4.	**Awareness & Training** Provide awareness and training to information risk owners, ensuring they understand their obligations in respect of data disposal. See also NCSP People Security Management standard	Code of Practice on UK Police Information and Records Management: Principle 4 (4.25)	Information management policy controls covering awareness and training. Calendar invites, training material, and certificates of competence/attendance at training events.
8.5.	**Regulations** Personal data must be kept secure throughout the sanitisation or destruction process.	UK GDPR: Article 1(f)	Data sanitisation and secure destruction policy. Asset management policy. Risk assessments and management plans for the sanitisation and destruction of information and assets.
8.6.	**Policy & Procedure** Implement and develop policies that ensure data destruction or sanitisation techniques are commensurate with the data classification and national standards.	NIST CSF: PR.IP-6 CCMv4.0: DSP-02	Data sanitisation and secure destruction policy. Risk assessments and management plans for the sanitisation and destruction of information and assets. Different service routes documented (or the limitation of services) for information disposed

Ref.	Minimum requirement	Control reference	Compliance Metric
			of at OFFICIAL and SECRET (where applicable).
8.7.	**Sanitisation & Destruction Outcomes** Select sanitisation and destruction services and techniques which meet the required sanitisation and destruction outcomes for the classification of asset held. Alternatively, a bespoke set of sanitisation and destruction outcomes may be documented. Any risks of sanitisation and destruction outcomes not meeting a specified standard must be recorded on the organisation's risk register and accepted by the responsible risk owner. For radio terminals ensure compliance with Code of Practice for Policing and the Assurance Guidance Note No. 7008 Disposal of Baseline Airwave TEA2 Radio Terminals.	NPSA: Secure Destruction of Sensitive Items NCSC: Secure Sanitisation and Disposal of Storage Media HMG IA Standard No. 5 NIST SP 800-88 Rev. 1 – Media Sanitisation, Appendix A DOD 5220.22-M	Procurement analysis of suppliers, through requests for information or invites to tender. Including bespoke non-function requirements for sanitisation and destruction. Secure information disposal policy. Supplier registered under an independent assurance scheme (e.g. CAS-S) which covers data sanitisation or destruction.
8.8.	**Third-Party Responsibilities** Contracts must cover the responsibilities of third parties who are selected to sanitise and destroy assets on behalf of an organisation. Ensure; (i) appropriate clearance of 3rd party personnel or action to be witnessed by personnel with appropriate clearance (ii) requirement for PASF if undertaken offsite See also NCSP Third Party Assurance for Policing standard	NIST CSF: PR.IP-6	Contractual agreements between the organisation and its third-party services provider(s).

Ref.	Minimum requirement	Control reference	Compliance Metric
8.9.	**Validation of Third-Party Claims** Any claims made by a sanitisation and destruction supplier to meet sanitisation and destruction outcomes must be thoroughly vetted to ensure full compliance. This vetting must go beyond verification of an independent assurance scheme (e.g. NCSC CAS-S) and into the detail of the attestation by a third party, including the specific details of the destruction outcome required.	CCMv4.0: DSP-02	Analysis of procurement options. Service/supplier reviews. Contract/supplier audits. Supplier registered under an independent assurance scheme (e.g. CAS-S, or NPSA) which covers data sanitisation or destruction. Specific checks to ensure that assurance claims made by a supplier who is registered under an independent scheme extend to the specific task being performed. For example, a supplier who has a sanitisation method assured to meet OFFICIAL outcomes for hard disk drives, is not using the same assurance for solid state (flash) storage drives. Details of product testing (e.g. NSA/NPSA approved products).
8.10.	**Other Forms of Media** Implement and develop procedures for disposing of hardware or physical forms of media and information in a secure manner. Securely destroy sensitive information stored on equipment or in physical form (e.g. paper) prior to decommissioning, selling, or transferring hardware or assets (e.g. buildings).	ISF SoGP 2024: HE1.1.1, HE1.2.1, HE1.2.12, IM.2.2.1	The organisation's secure data sanitisation and secure destruction policy extends to other office equipment, including paper formats, photocopiers, fax machines, etc.

Ref.	Minimum requirement	Control reference	Compliance Metric
8.11.	**Asset Return** Securely destroy information before equipment is returned to a third party.	ISF SoGP 2024: HE1.2.9	The organisation's data sanitisation and secure destruction policy extends to equipment loaned from suppliers or returned under warranty conditions.
8.12.	**Evidence Retention** Retain certificates of sanitisation and destruction in line with retention policies and standards.	ISO/IEC 27002:2022 7.9(c)	Certificates of destruction or sanitisation from third parties, detailing asset numbers, date & time, and personnel signatures.
8.13.	**Bespoke Applications** Decommission end-user developed applications by destroying the data and uninstalling the application.	ISF SoGP 2024: UA2.1.12	Asset records of decommissioned applications. Documented processes covering the removal of applications.
8.14.	**Crypto-Shredding** Revoke and destroy any cryptographic encryption keys that are no longer required due to the decommissioning of any infrastructure or services. Apply this method to data objects held within third-party cloud providers, where validation of the physical sanitisation or destruction may not be feasible.	CCMv4.0: CEK-14 NCSC Cloud Principles - Principle 2.4: Data Sanitisation and Equipment Disposal	Cryptographic policy covering the decommissioning and disposal of keys. Audits of key material, showing keys in use and keys revoked and decommissioned.
8.15.	**Cloud Backups** Sanitise and/or destroy any copies of information held for resilience or redundancy that are no longer required. Obtain a formal written confirmation of destruction.	NIST CSF: PR.IP-6	Formal written confirmation of destruction. Service description / procedure describing destruction & sanitisation methods.
9.	**Revoke Access, licenses and sensitive information** See also NCSP Identity & Access Management & System Access standards		
9.1.	**Access Control** Disable user accounts, service accounts, and API keys associated with the systems or services being decommissioned.	CIS Controls v8.0: 15.7	Access control policy. Decommissioning plans submitted to a change board.

Ref.	Minimum requirement	Control reference	Compliance Metric
	See also NCSP System Access and Identity & Access Management standards	ISO/IEC 27002:2022 5.18 NIST CSF: PR.AC-1	
9.2.	**Asset Return** Implement and maintain a policy for the return of assets owned or controlled by the organisation upon the termination of employment, contract or commercial agreement. Ensure that the policy extends beyond end user devices, to include specialist equipment, authentication hardware, and physical copies of information.	CCMv4.0: HRS-05	Asset management policy detailing recovery controls. Employment contracts covering the return of assets and information. Commercial agreements stipulating conditions for the return of assets and information.
9.3.	**Manual Deprovisioning** Deprovision any authorisations for systems which are not integrated into automated processes. Manual and automatic processes should be identified and documented through subject matter expert engagements. These would normally take place during the Change Control and asset inventory/discovery stages of the decommissioning process.	CCMv4.0: IAM-07	Access control policies setting out procedures for manual deprovisioning. Decommissioning plans. Change board minutes. Service management requests.
9.4.	**Logging and Metadata** Remove sensitive information from access controls and surveillance systems prior to leaving a premises.	ISO/IEC 27002:2022 7.14	Physical security policy. Decommissioning plans. Contractual/lease agreements covering the return or deletion of sensitive access or surveillance data at the end of an agreement.
9.5.	**Licenses**	UK GDPR: Article 25, Article 32	Asset management policy.

Ref.	Minimum requirement	Control reference	Compliance Metric
	Remove licenses for decommissioned systems to allow licenses to be reallocated or retired. Remove access to systems which are to be decommissioned to support the maintenance of up-to-date records and permissions for systems and applications.	DPA 2018: Section 66 Code of Practice on UK Police Information and Records Management: Principle 4 (4.36)	Asset management records showing decommissioned and reallocated licenses. Access control policies. Decommissioning plans.
10.	**Update Documentation and Monitoring Tools**		
10.1.	**Information Flow Maps** Update baselines and data flows within the organisation's network environment following any significant changes to its infrastructure. This includes communication to third parties, ports, protocols, and services.	NIST CSF: ID.AM-03	Data flow map updates are version controlled. Architectural design documents are applied using version control to reflect changes to any services, ports, or protocols.
10.2.	**Logging and Monitoring** Update monitoring and event management tooling to reflect any changes in the network environment.	NIST CSF: DE.AE-01	Change records detailing updates to log sources, analysers, log collectors, and Security Incident and Event Management systems/tools.
10.3.	**Updating Knowledge and Records** Update asset registers, network diagrams, and configuration management databases (CMDBs). Retain decommissioning records (e.g. sanitisation certificates and disposal receipts) for audit purposes.	NIST CSF: ID.AM-01, ID.AM-02	Asset status updates on asset register. Destruction or sanitisation reports are linked to decommissioned assets recorded on the register. An asset containing data can be tracked from a serial/asset number through to a certificate of decommissioning, without any break in the chain of custody.

Ref.	Minimum requirement	Control reference	Compliance Metric
			Records are kept in accordance with the retention schedule.
10.4.	**Encryption Management** Update any cryptographic key management systems to reflect a change in status for decommissioned assets and assigned encryption keys and digital certificates.	CCMv4.0: CEK-21	Audits of systems do not show keys or certificates for systems which have been decommissioned.
10.5.	**Information Asset Registers** Update records for Information Asset Registers and data processing activities to ensure an accurate enterprise map of information assets and data processing, for which the organisation acts as a controller and a processor.	UK GDPR: Article 30 DPA 2018: Section 61	Information asset registers have been updated following any identified decommissioning activity.
11.	**Compliance Verification**		
11.1.	**Auditing of Compliance** Conduct a post-decommissioning audit to verify compliance with policies and standards. Confirm data destruction certificates and disposal logs are archived. Conduct an audit to review compliance against the organisation's information security policy.	ISO/IEC 27002:2022 5.36 ISO/IEC 27002:2013 Clause 9	Formal documentation showing an audit of decommissioning activity against documented decommissioning procedures.
11.2.	**Continuous Monitoring** Update the organisation's continuous monitoring program ensuring that any cyber-related lessons learned are incorporated into future compliance audits. Lessons learned may include improvement in Change Control, IT asset registers, or supply chain management. Improvements will improve future decommissioning procedures by applying appropriate scrutiny and control to	NIST SP 800-53 R5: PM-31	Continuous improvement logs reflect any lessons learned during audits of the organisation's decommissioning process. Minutes of continuous improvement discussed at an appropriate organisational board.

Ref.	Minimum requirement	Control reference	Compliance Metric
	individual activities within the overall process.		
11.3.	**Laws and Regulations** Verify that the decommissioning activity has been conducted in conformance with data protection regulations.	UK GDPR: Article 5 (2) DPA 2018: Section 66	Audits of decommissioning activity that focus on compliance with laws and regulations.
12.	**Final Reporting, Closure and Continuous Improvement**		
12.1.	**Reporting** Issue a decommissioning closure report to stakeholders to cover the action taken and assets affected. This will also provide an analysis of any incidents encountered, lessons learned, and improvement actions implemented. Archive all documentation and close the request in the IT service management tool. Apply continuous improvement techniques by analysing the completed activity and implementing accepted recommendations and corrective actions as a result of any gaps identified.	COBIT 2019 MEA01.05 ITIL 4 Continual Improvement	Decommissioning closure reports for stakeholders. The report should cover, any gaps identified during decommissioning or auditing of decommissioning activity.
12.2.	**Continuous Improvement: Decommissioning** Apply knowledge gained from any security incidents or near-misses during decommissioning to reduce the likelihood of future incidents.	ISO/IEC 27002:2022 5.27	Changes to policy or procedure resulting from historic incidents. Policy version control showing updates to documentation that coincides with post-incident reviews.
12.3.	**Continuous Improvement: Commissioning** Apply lessons learned into all aspects of new system commissioning ensure that data protection by design is built into the full life cycle of systems.	DPA 2018: Section 57 Code of Practice on UK Police Information and Records	Updates to policies addressing the commissioning of systems, as a result of improvements identified during decommissioning reviews or audits.

Ref.	Minimum requirement	Control reference	Compliance Metric
		Management: Principle 3 (4.27)	
12.4.	**Regulations** Develop organisational data protection policies where appropriate to address any risks relating to data protection regulations identified during decommissioning activities.	UK GDPR: Article 24 DPA 2018: Section 56	Changes to information management or data protection policies to address any issues identified during the decommissioning process or audit.
12.5.	**Quality Management** Designs and maintenance must ensure the quality and value of information and records systems.	Code of Practice on UK Police Information and Records Management: Principle 3 (4.20), (4.26)	Updates to organisational policies which address updates to improve data quality and value.
12.6.	**Information Management** Information and records management principles must be built into design, development, procurement, and functionality.	Code of Practice on UK Police Information and Records Management: Principle 3 (4.26)	Updates to organisational policies resulting from decommissioning reports or audits to address data protection by design principles.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

For external use (outside PDS), this standard should be distributed within force departments who are responsible for decommissioning 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.

Review Cycle

This standard 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 standard continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

Adapt this statement according to Force or PDS Policy needs.

Equality Impact Assessment

The implementation of this standard should have no impact on equality. In some cases, special applications may well be needed for reasonable adjustments, however the applications required under these circumstances will pass through the same rigorous review, documentation and inventory management processes.

This statement may be adapted according to Force or PDS Policy needs.

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial draft	02/25
1.0	PDS Cyber	Updated following internal reviews	03/25

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	22/05/25

Document References

Document Name	Version	Date
National Police Information Risk Management Framework	N/A	05/2023
Physical and Environmental Security Management Standard	1.1	01/2025
Monitoring and Evaluation of Force Information Security Incidents Guideline	1.0	02/2025
People Security Management Standard	1.0	05/2024
Information Transfer Guideline	1.0	02/2025
Third-Party Assurance for Policing (TPAP) Standard	2.0	05/2024
ISF - Standard of Good Practice (for Information Security)	2024	03/2024
ISO 27002 - Information security, Cybersecurity and privacy protection – Information security controls	2013 & 2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1 / v2.0	04/2018
NIST Special Publications: 800-30r1, 800-34r1, 800-53r5, 800-88r1, 800-221A	N/A	N/A
CSA Cloud Controls Matrix	v4	01/2021
NCSC Cloud Security Principles (Principle 2) Principle 2: Asset protection and resilience - NCSC.GOV.UK	Web Page	05/2022
NCSC Sanitisation Guidance Secure sanitisation and disposal of storage media - NCSC.GOV.UK	Web Page	02/2025
Government Threat Model on OFFICIAL Guidance 1.5 - Considerations for Security Advisors (HTML) - GOV.UK	Web Page	08/2024
NCSC Sanitisation Assurance Scheme	Web Page	

Document Name	Version	Date
An introduction to Sanitisation Assurance (CAS-S) - NCSC.GOV.UK		Unknown
NCSC Assured Service CAS Service Requirement	2.1	11/2018
HMG IA5 – Data Sanitisation and Secure Destruction	V5.0	
Police Vetting Code of Practice https://www.gov.uk/government/publications/police-vetting-code-of-practice/vetting-code-of-practice gov.uk publications or College of Policing	N/A	July 2023
Police National Vetting Service Non-Police Personnel Vetting https://www.warwickshire.police.uk/police-forces/warwickshire-police/areas/warwickshire-police/about-us/about-us/police-national-vetting-service/about-the-police-national-vetting-process/	N/A	April 2024
UK GDPR https://www.legislation.gov.uk/eur/2016/679/contents	N/A	See section
DPA 2018 https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf	N/A	
Police Information and Records Management: Code of Practice Police information and records management: code of practice (accessible) - GOV.UK	N/A	07/2023