# CYBER STANDARD DOCUMENT

## PHYSICAL ASSET MANAGEMENT

## ABSTRACT:

The standard aims to ensure that physical assets are acquired securely, configured properly, maintained regularly, and disposed of safely and securely, while ensuring the confidentiality, integrity, and availability of the information they handle. By adopting this standard, organisations can ensure that they are protecting their assets against potential threats, mitigating risks, and complying with regulatory requirements.

| | |
|---|---|
| **ISSUED** | February 2024 |
| **PLANNED REVIEW DATE** | November 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 | Ginu Mammen | Initial version | 10/05/23 |
| 0.2 | Ginu Mammen | Updates following internal peer review | 18/10/23 |
| 0.3 | Ginu Mammen | Updates following NCPSWG review | 03/11/23 |
| 0.4 | Tim Moorey | Minor amendments following NCPSWG review | 06/12/23 |

### Approvals

| Version | Name | Role | Date |
|---|---|---|---|
| V1.0 | National Cyber Policy & Standards Board | National authority for Cyber standards | 25/01/24 |

## 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 |
| ISO/IEC 19770-1:2017- Information technology IT asset management | Edition 3 | 12/2017 |
| BS EN 15713:2009 Information destruction. | | |
| CIS Controls | v8 | 05/2021 |
| NIST Cyber Security Framework | v1.1 | 04/2018 |
| 10 Steps to Cyber Security - NCSC.GOV.UK | Web Page | 05/2021 |

## 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.

## Introduction

Physical asset management involves the systematic and coordinated management of physical assets throughout their life cycle to ensure that they deliver value to the organisation. Effective physical asset management enables organisations to optimise asset performance, minimise risks, and reduce costs associated with maintenance and repairs. To help organisations achieve these goals, several leading standards organisations have developed physical asset management standards.

Physical asset management is critical to maintaining the confidentiality, integrity, and availability of an organisation's information and systems. This standard is based on the guidelines provided by National Institute of Standards and Technology (NIST), International Organisation for Standardisation (ISO), and the Center for Internet Security (CIS) to help organisations establish a comprehensive physical asset management program.

Effective asset management can lead to better efficiency and lower costs, while poor practices can result in potential risks.

## Owner

National Chief Information Security Officer (NCISO).

## Purpose

The purpose of this standard is to assist community members in demonstrating compliance with the following NCSP policy statements:

- Protect physical assets, including endpoint devices (e.g., workstations, laptops and servers); office equipment (e.g., network printers and multifunction devices); and specialist devices and equipment (e.g., heating, ventilation and air conditioning (HVAC) systems, radio equipment and Internet of Things (IoT) devices) throughout their lifecycle, addressing the information security requirements for their acquisition (e.g., purchase or lease), configuration, maintenance and disposal.
- Protect mobile devices (including tablets and smartphones), the applications they run and the information they handle against loss, theft and unauthorised disclosure by: configuring security settings; restricting access; installing security software; and managing devices centrally through an Enterprise Mobility Management (EMM) solution.

This standard aims to ensure that the organisation's physical assets are protected against all types of threats and that the sensitive information handled by these assets is secured using the principles of confidentiality, integrity, and availability. The standard also helps the organisation to comply with the guidance provided by the National Cyber Security Centre (NCSC) to protect physical assets from cyber threats.

## Audience

This standard is aimed at:

- Staff across PDS and policing who build, implement and maintain ICT systems, either on behalf of National Policing or at a local force level.
- The user community, including those who have escalated privileges to provide administrative functions.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors and penetration testers providing assurance services to PDS or policing

## Scope

1. The standard applies to all physical assets owned, leased, or used by the organisation, including endpoint devices such as workstations, laptops, and servers, office equipment such as network printers and multifunction devices, and specialist devices and equipment such as heating, ventilation and air conditioning (HVAC), radio equipment, and Internet of Things (IoT) devices.
2. The requirements laid out in this standard aim to ensure the confidentiality, integrity, and availability (CIA) of the information processed, stored, or transmitted by these physical assets. Assets must be protected against all types of threats, including physical, environmental, and cyber threats, throughout their lifecycle.
3. The standard covers the information security requirements for the acquisition, configuration, maintenance, and disposal of physical assets. Assets must be acquired from trustworthy sources, configured securely, maintained regularly, and disposed of safely and securely.
4. The standard also covers the security requirements for mobile devices, including tablets and smartphones. Security features and settings must be configured, access restricted, security software installed, and be managed centrally through an Enterprise Mobility Management (EMM) solution. This is to ensure that the applications they run and the information they handle are protected against loss, theft, and unauthorised disclosure.

## Requirements

This section details the minimum requirements for physical asset management to protect policing assets. Compliance metrics are suggested to aid control performance measurement, audit and management reporting.

Note references are made to National Cyber standards which may not be published at the time of issue. These standards will be available within 3 months of this standard's issue date.

| **Section 1 - High Level Requirements** | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 1.0 | **Acquisition of assets**<br><br>Ensure the selection requirements for new assets include legal, regulatory and National Community Security Policy and standards requirements.<br><br>Ensure that suppliers have undergone due diligence and security assessment | | Supplier reviews and assessments.<br>Contractual controls.<br><br>Procurement or purchasing procedures. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| | such as Third Party Assurance for Policing (TPAP).<br><br>Ensure that the procurement and purchasing of assets is through controlled, approved channels.<br><br>Ensure that the receipt of supplied assets includes integrity checks to reduce the risk of damaged / tampered assets being introduced into use. | | Records of approved purchases, receipt of goods checks. |
| 1.1 | **Asset register**<br><br>An asset register must be in place, maintained so that all physical assets can be identified and protected against threats.<br><br>As a minimum the register should include;<br>• asset name<br>• category<br>• priority / criticality<br>• accountable owner<br>• custodian (current user)<br>• location<br>• warranty date<br>• financial information<br>• depreciation<br>• expected life<br>• maintenance date.<br><br>Further information is available through ISO/IEC 19770-1:2017<br><br>A senior role shall be accountable for the asset register. | NIST Controls - ID.AM-1 ISO 27002 5.09, CIS controls v8 1.1, | Asset owner in place.<br>Asset register in place.<br>Local procedures in place to identify assets and maintain the asset register. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| | | | |
| 1.2 | **Asset Management**<br><br>Assets are subject to a formal process throughout removal, transfers, and disposal.<br><br>The movement of assets should be tied into joiners, movers & leavers processes to track movement.<br><br>Regular audits and physical verification of assets are conducted to provide assurance that the asset register is accurate.<br><br>Controls should be in place to protect assets when transferring between locations, including approved secure couriers, physical security controls and tracking. | NIST Controls PR.DS-3, PR.MA | Validation of local procedures for asset inventory, maintenance of equipment, protect assets, manage vulnerabilities, and properly manage assets removal, transfers, and disposal.<br><br>Records of asset audits.<br><br>Records of asset movements / transfers. |
| 1.3 | **Provision of new assets**<br><br>Before use, new hardware shall be subject to security reviews and testing to ensure that functionality and potential vulnerabilities are understood and are within risk appetite.<br><br>Reviews and testing should based around reviewing the asset against relevant security controls described in the CIS 18 critical controls and NCSC guidance. | NIST Controls – ID.RA, PR.MA | Local procedures for provisioning assets.<br>Records of testing and results.<br>Risk assessments. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| | | | |
| 1.4 | **Define standard security 'builds'**<br><br>Ensure that all physical assets provide only the required functionality and does not compromise the security of critical or sensitive information and systems. See section 2 for more detail.<br><br>Ensure that assets are not deployed with insecure manufacturer default settings that could increase exposure to vulnerabilities.<br><br>Security hardening configurations or 'builds' are defined and applied according to the target devices.<br><br>Builds should be defined according to business needs as well as cyber security controls.<br><br>Builds should remove default manufacturer settings that are not required such as default passwords and unnecessary services.<br><br>Standard builds should be regularly reviewed and updated according to vulnerabilities and technology / feature changes.<br><br>Deviations from standard builds shall be subject to a risk balance case.<br><br>This includes all networking equipment and any device that forms part of the ICT infrastructure. | ISO 27002 Controls-5.09, 7.13, 7.14, 8.08, 8.10.<br>NIST Controls – ID.AM-1, ID.AM-5, PR.AC-2, PR.DS-3, PR.DS-8 PR.IP-5, PR.MA-1.<br>CIS Control V8– 4.7 | Validation of policies for asset inventory, maintenance of equipment, protect assets, manage vulnerabilities, and properly manage assets removal, transfers, and disposal. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 1.5 | **Endpoint devices including; servers, desktops, laptops and tablets.**<br><br>Apply a baseline level of security hardening to all endpoint devices commensurate with the information processed or stored on them.<br><br>Apply security hardening builds depending upon the target devices and business functionality required.<br><br>**See section 2 for more detail.** | ISO 27002 Controls- 7.07, 8.01, 8.09, 8.17, 8.18.<br>NIST Controls – PR.IP-1, PR.PT-3.<br>CIS Controls V8 – 2.5, 3.6, 3.1, 3.11, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.8, 4.1, 4.11, 9.1, 9.4, 10.1, 10.2, 10.3, 10.4. | Baseline security build defined and applied. Validation of endpoint device policy, Secure baseline configuration, Clear desk policy. |
| 1.6 | **Office equipment**<br>Office equipment includes printers, multi-function devices, communication devices and similar.<br><br>Ensure a baseline of security hardening is applied commensurate with the information processed or stored on them.<br><br>Where it is not possible to apply security hardening consider controls such as network segregation / firewalling.<br><br>Limit the ability of devices to send policing information back to manufacturer / third party support online services.<br><br>**See section 2 for more detail.** | ISO 27002 Controls – 5.14<br>NIST Controls - ID.AM-1, PR.AC-2, PR.AC-7 | Baseline security build defined and applied. Validate Users, devices and other assets are authenticated, accessed, protected appropriately with the risk of the business. Information transfer controls are in place. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 1.7 | **Mobile devices**<br>Mobile devices includes mobile phones, tablet devices, radio equipment, mobile recording devices.<br><br>Ensure a baseline of security hardening is applied to mobile devices.<br><br>Include specific controls to protect them and the information they hold or access should they be lost or stolen.<br><br>**See section 2 for more detail.** | ISO 27002 Controls – 8.01<br>NIST Controls - PR.AC-2, PR.IP-1, DE.CM-3, DE.CM-5.<br>CIS Controls V8 - 3.6, 4.11. | Baseline security build defined and applied. Validate mobile devices policy. Ensure encryption, Secure baseline configuration, Monitoring and Remote wiping is applied |
| 1.8 | **Other devices**<br><br>These devices include Heating, Ventilation & Air Conditioning (HVAC), building management systems, physical access control systems, CCTV systems, 'black boxes', vehicle telemetry equipment, GPS 'sat navs', diagnostic equipment, body/vehicle cameras, conference room equipment, room booking systems and internet of things (IoT) devices.<br><br>Ensure a baseline of security hardening is applied to<br>specialised computing equipment and devices.<br><br>Where it is not possible to apply security hardening consider controls such as network segregation / firewalling.<br><br>**See section 2 for more detail.** | ISO 27002 Controls – 5.09.<br>NIST Controls – PR.MA, ID.AM-1. | Validate inventory of information and other associated assets. Baseline security build defined and applied. |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 1.9 | Ensure that sensitive information stored on removable media is protected from unauthorised disclosure. | ISO 27002 Controls – 7.10.<br>NIST Controls - PR.PT-2.<br>CIS Controls V8 - 3.9. | Validate management of removable media. |
| 1.10 | Ensure that the risks associated with industrial control systems (ICS) are managed.<br><br>Measures include;<br>• Inventory of ICS assets,<br>• Baseline secure configurations,<br>• Asset vulnerability scanning,<br>• Maintenance & change management,<br>• Monitoring and roles and responsibilities. | NIST Controls - ID.AM-1, ID.AM-5, ID.BE-2, ID.GV-2, ID.RA-1, ID.RM-3, PR.AT-3, PR.AT-5, PR.IP-1, PR.MA-1, DE.AE-2, DE.CM-1. | |
| 1.11 | Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access and align with organisational policy | NIST Controls - PR.AC-3, PR.MA-2<br>CIS Controls V8 - 2.5, 4.3, 4.8, 4.1, 4.11, 4.12. | Review of remote access management, Mobile device policy |
| 1.12 | Ensure that critical and sensitive information processed by applications on mobile devices is adequately protected. | CIS Controls V8 – 4.12 | Review of mobile device policy and ensuring separate workspace profile management is applied based on sensitivity. |
| 1.13 | The organisation's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | ID.RM-3 | Review the organisation's overall approach to information security supports the risk appetite and has appropriate governance in place |
| 1.14 | Asset vulnerabilities are identified and documented | ID.RA-1 | Validate the organisation address vulnerabilities quickly and effectively |

| Section 1 - High Level Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 1.15 | Cyber security roles and responsibilities are coordinated and aligned with internal roles and external partners | ID.GV-2 | Review the roles and responsibility, security activities are properly performed throughout the organisation, reducing information risk in a consistent manner |
| 1.16 | The organization's place in critical infrastructure and its industry sector is identified and communicated | ID.BE-2 | Review the policy and or process in line with the organisation and communicated. |
| 1.17 | Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | ID.AM-5 | Review the assets are classified and prioritised based on the classification, criticality and business value. |
| 1.18 | Physical devices and systems within the organization are inventoried | ID.AM-1 | Validate inventory of organisational assets |

| Section 2 – Asset Hardening Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 2.2 | Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access | PR.MA-2 | Review the policy, procedures and logs for the remote assets management. |
| 2.3 | Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools | PR.MA-1 | Validate the process and policy, controls applied and logs from the tools used. |
| 2.4 | Local regulations and requirements regarding the physical operating environment for organisational assets are met | PR.IP-5 | Review the devices policy and procedures |
| 2.5 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) | PR.IP-1 | Review the baseline configuration and evaluate the systems with the baseline configuration applied. |
| 2.6 | Integrity checking mechanisms are used to verify hardware integrity | PR.DS-8 | Review the anti-tamper protection control. |
| 2.7 | Assets are formally managed throughout removal, transfers, and disposition | PR.DS-3 | Validation of policies for asset inventory, and properly manage assets removal, transfers, and disposal. |
| 2.8 | Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational risks) | PR.AC-7 | Validate Users, devices and other assets are authenticated, accessed, protected appropriately with the risk of the business. Information transfer controls are in place. |
| 2.9 | Remote access is managed | PR.AC-3 | Review of remote access management, Mobile device policy |
| 2.10 | The network is monitored to detect potential cybersecurity events | DE.CM.1 | Review network monitoring, roles and responsibilities. |

| Section 2 – Asset Hardening Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 2.11 | Physical access to assets is managed and protected<br><br>**See also:**<br>• Physical & Environmental Security standard | PR.AC-2 | Review the Physical access to assets are controlled managed and protected. |
| 2.12 | The attempted installation or use of unauthorised software is prevented and detected. | DE.CM-5 | Review the acceptable and unacceptable mobile code and mobile code technologies; and authorise, monitor, and control the use of mobile code within the system. |
| 2.13 | Personnel activity is monitored to detect potential cybersecurity events | DE.CM-3 | Review the end users account management, audit records, monitoring of information disclosure and continuous monitoring. |
| 2.14 | The network is monitored to detect potential cybersecurity events | DE.CM-1 | Review network monitoring, roles and responsibilities. |
| 2.15 | Detected events are analysed to understand attack targets and methods | DE.AE-2 | Review the process of log analysis, incident handling and reporting in line with the organisational policies, and regulations |
| 2.16 | Implement an allowlist of authorised software | CIS 2.5 | Review the process for software implementation and controls applied. |
| 2.17 | Encrypt sensitive data in transit<br><br>**See also:**<br>• Cryptography Standard | CIS 3.1 | Evaluate and review the encryption applied for data in transit. |
| 2.18 | Encrypt sensitive data at rest<br><br>**See also:**<br>• Cryptography Standard | CIS 3.11 | Evaluate and review the encryption applied for data at rest. |

| Section 2 – Asset Hardening Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 2.19 | Encrypt data on end user devices<br><br>**See also:**<br>• Cryptography Standard | CIS 3.9 | Review the end user device policy and validate the encryption is applied. |
| 2.20 | Establish and maintain a secure configuration process | CIS 4.1 | Review the baseline configuration applied and is maintained. |
| 2.21 | Enforce Automatic Device Lockout on Portable End-User Devices | CIS 4.10 | Review the end user device configuration for lockout in line with the organisation policy |
| 2.22 | Enforce Remote Wipe Capability on Portable End-User Devices | CIS 4.11 | Evaluate the remote devices configuration process, deployment and validate the configuration applied |
| 2.23 | Separate Enterprise Workspaces on Mobile End-User Devices.<br><br>Consider using Mobile Device Management / Work profiles. | CIS 4.12 | Review separate enterprise workspaces are used on mobile end-user devices deployed based on the organisational policy. |
| 2.24 | Establish and Maintain a Secure Configuration Process for Network Infrastructure | CIS 4.2 | Validate organisation maintain a secure configuration process for network infrastructure. For example security standards and baselines. |
| 2.25 | Configure Automatic Session Locking on Enterprise Assets | CIS 4.3 | Review the inactivity timeout configuration and behaviour based on the organisational policy. |
| 2.26 | Implement and Manage a Firewall on End-User Devices | CIS 4.5 | Review the policy and or procedures for the baseline configuration validate the end user devices firewall is implemented and maintained. |

| Section 2 – Asset Hardening Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 2.27 | Securely Manage Enterprise Assets and Software | CIS 4.6 | Review the organisation policy and process, asset inventory, secure configuration, Asset monitoring, reporting and management of assets in use. |
| 2.28 | Manage Default Accounts on Enterprise Assets and Software | CIS 4.7 | Review the process of managing or disabling the default accounts and passwords in line with organisation security policy or standard. |
| 2.29 | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software | CIS 4.8 | Review the secure configuration of assets and software implemented and ensure services not required are disabled or removed. |
| 2.30 | Ensure Use of Only Fully Supported Browsers and Email Clients | CIS 9.1 | Review the organisational use of web browsers and email clients, validate they are supported versions and appropriately managed. |
| 2.31 | Restrict Unnecessary or Unauthorised Browser and Email Client Extensions | CIS 9.4 | Review the secure configuration to restrict the use of non-standard features. |
| 2.32 | Deploy and Maintain Anti-Malware Software | CIS 10.1 | Review and validate the Anti-Malware implementation and management. |
| 2.33 | Configure Automatic Anti-Malware Signature Updates | CIS 10.2 | Review the AV Signature updates deployment and management of Anti-Malware software |
| 2.34 | Disable Autorun and Autoplay for Removable Media | CIS 10.3 | Review the configuration policy and implementation |
| 2.35 | Configure Automatic Anti-Malware Scanning of Removable Media | CIS 10.4 | Review and validate the configuration of the Anti-Malware software for scanning removable media |

| Section 2 – Asset Hardening Requirements | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 2.36 | Physical and cybersecurity personnel understand their roles and responsibilities | PR.AT-5 | Review the roles and responsibility of the security personnel |
| 2.37 | Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities | PR.AT-3 | Review the 3rd party stake holder engagement and ensure they understand roles and responsibilities and documented |
| 2.38 | Removable media is protected and its use restricted according to policy | PR.PT-2 | Review the removable media policy and validate it is protected and prevent unauthorised data leakage, malware infections and other threats from removeable media. |

| Section 3 - Asset Decommissioning & Disposal | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 3.2 | An NCSC / Common Criteria certified product (See NCSC web site or Data Protection folio at commoncriteriaportal.org) shall be used to ensure the erasure / sanitisation of assets. Certificates of destruction shall be retained in accordance with local records management requirements.<br><br>Secure erasure / sanitisation should also be used on assets before reuse at a lower classification.<br><br>Secure erasure / sanitisation should be used before selling / recycling assets. | PR.IP-6, PR.DS-5, ID.SC-2 | Certified product being used.<br>Certificates of destruction.<br>Asset records. |
| 3.3 | Third parties appointed to sanitise or dispose of assets shall be approved through local or national Third Party Assurance Procedures (TPAP.)<br><br>This applies to on or off-site sanitisation or disposal.<br><br>Third parties must be able to ensure that assets are protected whilst in transit in accordance with asset classification.<br><br>Refer to B*S EN 15713:2009* Information destruction.<br><br>**See also:**<br>• Policing guidance on the Government Security Classification Policy. | PR.IP-6, PR.DS-5, ID.SC-2 | Third party assurance records.<br>Contracts.<br>Records of assessments / reviews of supplier(s)<br>Contract performance reviews. |

| Section 3 - Asset Decommissioning & Disposal | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 3.4 | Records of all sanitisation or disposal of assets shall be kept in the asset register. | PR.DS-3. PR.IP-6, PR.DS-5 | Certificates of destruction.<br>Asset records. |
| 3.5 | Hardware settings shall be reset to manufacturer defaults and all policing references / settings shall be removed before disposal. | PR.DS-5, PR.PT-2 | Hardware decommissioning procedures and records. |
| 3.6 | Where physical destruction is used, shredding, disintegration, pulverizing, or incineration may be used subject to local environmental and regulatory restrictions.<br><br>Any shredding / disintegration shall ensure that reconstitution is highly unlikely. See Annex A NPSA Secure Destruction of Sensitive Items standard and BS EN 15713:2009 Information destruction.<br><br>All asset disposals must comply with environmental regulation and local organisation policy | PR.DS-3. PR.IP-6, PR.DS-5 | Certificates of destruction.<br>Asset records.<br><br>Records of compliance with environmental regulations |
| 3.7 | **Cloud / third party hosted assets**<br>Contractual controls and obligations shall be in place to ensure that certificates of destruction / sanitisation are provided by third parties for all assets used to process or store classified policing information.<br><br>Contracting bodies are responsible for ensuring that every effort is taken to remove classified information from third party assets. | PR.DS-3. PR.IP-6, PR.DS-5 | Contracts<br>Certificates of destruction / erasure.<br>Asset records. |

| Section 4 – Training, Education & Awareness | | | |
|---|---|---|---|
| ***Reference*** | ***Minimum requirement*** | ***Control reference*** | ***Compliance Metric*** |
| 4.0 | Ensure that all personnel who access, use, procure, maintain or dispose of assets are aware of the following;<br><br>• Acceptable use<br>• Correct procurement / purchasing methods<br>• Correct methods of transferring ownership<br>• Requirement to return redundant assets<br>• Recovering issued assets from leavers<br>• Protecting from loss / theft<br>• Reporting of loss / suspected or actual security events<br>• Controls when travelling overseas<br>• Approved disposal procedures | PR.AT | Training objectives<br>Training / awareness materials<br>Records of training delivered & received<br>Records of incidents reported<br>Asset register<br>HR processes<br>Certificates of destruction |

## 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 Nation Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

This standard should be socialised with IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with your Force SIRO / 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 reporting.

## 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.)*