# CYBER STANDARDS DOCUMENT

# *NCSP APPLICATION MANAGEMENT*

**ABSTRACT:**
This standard is intended to guide the reader through the process of securely managing business applications, both internally developed and externally sourced, regardless of whether locally installed or cloud based. Centred around stocktaking, documenting and actively managing those applications, this standard should enable the visibility of all business utilised applications, ensuring all are appropriately assessed for risk, appropriately controlled, and managed in such a way as to not introduce cyber security risk going forward.

| | |
|---|---|
| **ISSUED** | November 2024 |
| **PLANNED REVIEW DATE** | November 2025 |
| **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 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 application management.

## Introduction

The Application Management Standard is intended to minimise cyber risk arising from the use of unsanctioned or poorly managed applications. Application management can be defined as the process for managing application lifecycles, from acquisition, delivery and support, through to decommissioning.

The intention of this standard is to introduce security controls into and around applications management to protect the confidentiality, availability, and integrity of information processed by these applications. The premise behind these controls is to take stock of existing applications, record their existence, purpose, owner and condition in an asset inventory, and maintain this going forward for all business applications. Through this inventory, visible applications can be protected by ensuring their configuration is secure, necessary, and any internally developed applications are following a secure development methodology.

## Owner

National Chief Information Security Officer (NCISO).

## Purpose

The purpose of this standard is to:

- Establish a documented process which can be consistently applied for managing the risks associated with acquiring and introducing new applications within an organisation

- Ensure business applications are protected against loss of availability, unauthorised access, invalid connections, and unauthorised disclosure of sensitive information.
- Reduce specific risks associated with cloud/web applications.
- Protect critical/sensitive information stored in or processed by applications.
- Ensure End User Developed Applications (EUDA) function correctly, meet security requirements and are developed in a standardised way.
- Assure the accuracy of information processed by critical spreadsheets and protect that information from disclosure to unauthorised individuals.
- Assure the accuracy of information processed by critical databases and protect that information from disclosure to unauthorised individuals.

Furthermore, this standard helps organisations demonstrate compliance with the following NPCSP policy statements:

Application Management

- *Incorporate security controls into applications (including specialised controls for web applications) to protect the confidentiality and integrity of information when it is input to, processed by, and output from these applications.*
- *Develop critical [EUDA], such as spreadsheets, Power BI, etc, in accordance with an approved development methodology, recording them in an inventory, and protect them by configuring security settings in vendor software; validating input; implementing access controls; restricting user access to powerful functionality; and managing changes diligently.*

The requirements stated in this standard are mapped across from the following industry standards:

- International Security Forum Standard of Good Practice (ISF SoGP) 2024
- ISO 27002:2022
- CIS Controls
- NIST Cyber Security Framework v1.1

This Application Management Standard must be considered alongside the System Development standard when developing applications.

## Audience

This standard is aimed at:

- Organisations and individuals who procure, build, implement and manage IT applications for and on behalf of UK policing. This includes those within PDS, national policing, and local forces.
- The end-user community that has administrative privileges which allow them to install applications on End User Devices (EUDs) and servers (virtual and physical), or that produce EUDAs (e.g., complex macro enabled spreadsheets, Power Platform Applications (including Power BI, Power Automate, Power Apps), visual programming, etc.).
- Member Senior Information Risk Owners (SIRO), Information Asset Owners (IAO), Platform Asset Owners (PAO), Information Security Officers (ISO), 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

- New and existing applications.
- Prospective application purchases or application subscriptions.
- On-premises applications.
- Cloud-based applications.
- Mobile applications installed on tablets and smartphones.
- End-User Developed Applications (e.g. Power Apps, Visual Basic for Applications).
- Information assets such as databases, and data flows that are associated with business applications.

## Requirements

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **1.0** | **Acquisition, design/ development and implementation**<br>**Linked Documents:**<br>• Information Security Risk Management Guidance<br>• System Development Standard<br>• Management of High-Risk Applications Standard | | |
| **1.1** | Every effort should be made to acquire, lease or deploy robust, reliable software and software components (including open-source software). A documented process must be in place to manage the acquisition of software applications that from the outset, considers security requirements and identification of any security deficiencies. | **ISF SoGP**<br>IR2.5<br>SD1.4.7<br>SD1.3.7<br>SD2.3<br>**NIST CSF**<br>ID.AM-5<br>ID.GV-3<br>ID.RA-5<br>ID.SC-1<br>ID.SC-2<br>ID.SC-3<br>ID.SC-4<br>**ISO 27002:2022**<br>5.8b<br>5.21<br>5.23<br>5.32<br>8.25<br>8.26<br>**CIS v8**<br>15.4<br>16.1<br>16.2<br>16.5 | A documented software/application aquisition process that is consistently applied through policy. |
| **1.2** | A risk assessment must be run against any purchase, lease or onboarding of any applications (including the supplier of the application), taking into consideration the assessment output to make an informed decision before moving forward. | | Engagement with ISO or equivalent role, which is consistent with new acquisition decisions.<br>Information Risk Assessments |
| **1.3** | Applications must be subject to a screening process for information risk and data protection issues. Where necessary (in accordance with the Data Protection Act 2018) Data Protection Impact Assessments (DPIA) must be reviewed, updated or created, prior to the processing of personal data. | | A record of DPIAs consistent with the application asset register.<br>Evidence of DPO engagement. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **1.4** | The criticality and service classification of the application must be documented following an assessment of business impact. | | Business Impact Assessments. |
| **1.5** | Consideration must be given to the use of software escrow agreements for bespoke closed-source applications - providing a business-critical service that cannot be migrated to a new application provider without significant cost, impact, or downtime. This provides a level of resilience towards the continued ability for the application to meet the business requirements if the supplier is unable to maintain the development and support of the application (e.g., due to an inability to operate). | | Legal software escrow agreements for bespoke applications identified as business critical. Alternatively, evidence of a risk recorded where the decision to use escrow services has been considered. |
| **2.0** | **Application Management**<br>**Linked Documents:**<br>• Information Management Standard<br>• Physical Asset Management | | |
| **2.1** | A register of all business applications, their associated data, and application owners must be maintained:<br>• Suitable service management tools should be used to manage this where possible (i.e., a Configuration Management Database).<br>• The register must contain information relevant to the application being managed such as the name, the version number, the vendor, the business owner, | **ISF SoGP**<br>BA1.1<br>SM2.6<br>SR1.3<br>**NIST CSF**<br>ID.AM-2<br>ID.AM-4<br>ID.AM-5<br>PR.DS-3<br>PR.AT-2<br>PR.AT-3<br>PR.IP-2 | An actively maintained asset register. Dynamic system discovery tools configured correctly will support compliance.<br>Record of reviews of the asset register or audit of an approved |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
|  | the license and support status and conditions, as well as the license renewal date if applicable. Additionally, the register entry for an application should refer to the business value (or classification) of the application, as well as the sensitivity of the data processed by the application and whether a DPIA has been carried out.<br>• Consideration shall be given to customisable components of applications such as plug-ins, extensions or add-ins. | PR.MA-2<br>DE.CM-7<br><br>**ISO27002:2022**<br>5.9<br>6.3<br>8.26<br>8.28<br>8.32<br><br>**CIS v8**<br>1.1<br>1.2<br>1.3<br>1.4<br>1.5<br>2.1-2.7<br>15.7<br>16.4 | application list and an allow-list of applications that are permitted to run. |
| **2.2** | A process must exist to identify applications that are no longer required. These applications must be securely decommissioned and withdrawn from use. |  | Defined and implemented plans for software end-of-life support and obsolescence management.<br><br>Evidence of asset register reviews and outcomes, resulting in the removal of applications from the IT environment. |
| **2.3** | Applications that are no longer supported (e.g., software updates) must be decommissioned, or subject to robust risk management to manage the risks posed (e.g., through software vulnerabilities). |  | Risk management plans for applications that are no longer receiving security updates or unable to apply patches |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | | due to dependencies. |
| **2.4** | Applications must be deployed and decommissioned following change control procedures.<br>Records of decommissioned applications must be retained in accordance with local retention policies. | | Records of change management procedures being applied.<br>An entry on the organisation's Retention Schedule covering retired system information.<br>Records of applications on the asset register held for the correct retention period. |
| **2.5** | Application deployment and maintenance tools must be used to control the access, deployment, maintenance, and decommissioning of applications. To ensure coverage for all applications, consideration must be given to the capabilities of these tools when used to support Microsoft and non-Microsoft (third-party) applications. | | IT application management tools (e.g. Microsoft Intune) applied and details of their configuration, showing patch deployment cycles. This should be compared with the asset register to highlight discrepancies between deployed applications and those which are |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | | detailed on the register.<br>Scans of endpoints and servers will highlight discrepancies between approved applications and those installed on systems. This can demonstrate a level of confidence in the efficacy of the asset register. |
| **2.6** | Technical policies must block the use of unsanctioned applications by default. Organisations should favour application allow-lists (rather than deny-lists), which support the principle of default denial, or denying anything which hasn't been explicitly authorised the approval to run. | | A technical policy for applications and servers that implicitly denies non-approved applications. |
| **2.7** | Application support teams must have the knowledge, skills, and experience necessary to support the application and any investigations into security incidents. | | Job profiles detailing responsibilities for application support, along with the accompanying skills and experience. Records of training and/or certifications. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | | |
| **3.0** | **Application Protection**<br>**Linked Documents:**<br>- Identity and Access Management Standard<br>- System Access Standard. | | |
| **3.1** | All business applications must be securely architected, hardened to industry standards, connections validated, and access controlled.<br>The level of protection will be determined from compliance requirements, along with controls identified during the risk assessment that must be run before onboarding the application (ref 1.2). | **ISF SoGP**<br>BA1.2<br>**ISO 27002:2022**<br>8.4<br>8.26<br>8.27<br>8.31<br>**NIST CSF**<br>PR.AC-1<br>PR.AC-4<br>PR.AC-6<br>PR.IP-1<br>PR.DS-6<br>PR.DS-7<br>DE.CM-3<br>DE.CM-4<br>DE.CM-5<br>DE.CM-6<br>DE.DP-4<br>**CIS v8**<br>2.2<br>2.6<br>2.7<br>4.6<br>4.8<br>16.1<br>16.7 | Apply vendor or industry standard recommended configurations that enforce the organisation's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality). |
| **3.2** | Secure configuration must be achieved by implementing vendor recommendations, industry best practice (e.g. CIS), and balancing these with the functionality and risks arising from documented business requirements. | | Monitoring of any exceptions or deviations from recommended configurations or baselines. |
| **3.3** | Organisations must consider the use of separate environments for production and non-production (test) systems. For example, where system changes can be tested or developed safely, without the risk of disruption to the live service. | | Low-level design detailing non-production or test environment, or documented risk-based decisions not to implement test instances. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **3.4** | The use of logging and Protective Monitoring must be considered based on the outputs of the risk assessment, where appropriate. Organisations shall establish whether existing security monitoring is sufficient to manage risk, or whether additional monitoring is required to address specific risks. | 16.8<br>16.10<br>16.11<br>16.12 | Application risk assessment, including reference to Protective Monitoring controls.<br>Protective Monitoring Use Cases that map to risks identified during the assessment stage. |
| **4.0** | **Vulnerability Management & Security Testing**<br>**Linked Documents:**<br>• Vulnerability Management Standard<br>• Penetration Testing and ITHC Guidance | | |
| **4.1** | Organisations must conduct Penetration Testing against applications to manage the risks from technical exploitations, which could lead to compromise of the application and/or hosting environment. | **ISF SoGP**<br>BA1.2<br>TP2.1<br>TP2.2<br>TP2.3<br>**NIST CSF**<br>ID.RA-1<br>ID.RA-2<br>PR.IP-12<br>DE.CM-8<br>RS.AN-5<br>RS.MI-3<br>**ISO 27002:2022**<br>8.8<br>8.26<br>8.29 | Records of Penetration Tests and audit of Remediation Action Plans. |
| **4.2** | A Secure Development Lifecycle must be adopted (for example aligned to https://cloudsecurityalliance.org/secure-development-lifecycle ) encompassing secure design and appropriate testing for any software developed by or on behalf of the organisation.<br>Code reviews, such as static and dynamic testing must be conducted against software developed by the organisation, using appropriate tools. | | Evidence of code testing to a recognised methodology or standard, along with remediation plans. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **4.3** | Threat intelligence sources must be documented and monitored to provide advance warning of known software vulnerabilities, active exploits, or supply-chain breaches of security.<br>Threat Intelligence sources must be documented, along with the responsibility for review and analysis to determine the importance of each alert. | **CIS v8**<br>7.1-7.7<br>15.7<br>16.2<br>16.3<br>16.6<br>16.13<br>18.1-18.5 | References within a Vulnerability Management Policy, detailing sources and responsibility for review and action.<br>Details of alerts received and evidence of a workflow leading to remediation or risk management activity. |
| **4.4** | A vulnerability management tool must be deployed to the organisation's environment and appropriately configured to scan areas of the environment hosting applications. | | Vulnerability scan reports. |
| **4.5** | Vulnerability scans must be run on a scheduled basis. To limit any adverse impact to the live environment, organisations may decide to scan limited segments of the environment at a time. However, over a period defined within the Vulnerability Management Policy, the whole environment must be scanned.<br>The deployment scope of the tool must cover the full environment (e.g. Demilitarized Zones, or pocket networks). | | Technical configurations within the tool displaying the vulnerability scan schedule. This must align with the policy and should also be reviewed in conjunction with a network diagram to demonstrate the full coverage of the scans. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **4.6** | A process must exist to review, and prioritise vulnerabilities identified through scans and other sources, leading to the timely remediation of important application/software vulnerabilities. | | Records of remediation action taken combined with Threat Intelligence to demonstrate where an organisation has prioritised remediation of a vulnerability, as a result of identifying a proof of concept or active exploitation. |
| **4.7** | Organisations will already have an established patching process, which will aim to keep the version of the application at the latest version released by the application vendor. This will be achieved through established change control procedures to minimise any adverse impacts arising from application updates.<br>Vulnerability management must be used to complement the established patching processes by verification that all updates have been applied correctly, removing any vulnerabilities present in previous versions. | | A vulnerability & patch management procedure defining the organisations approach to patching vulnerabilities.<br>Change management process and supporting records. |
| **4.8** | In some circumstances organisations will need to take a risk-based approach to vulnerabilities that do not have a fix published by the application vendor. Organisations must document decisions, | | A Risk Register entry for vulnerabilities which are present in the |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | along with risk management plans where there is a need to continue using a vulnerable application that has no new patch release available.<br>Consideration shall be given to ensuring the vulnerability management of customisable components of applications such as plug-ins, extensions or add-ins.<br>See also:<br>NCSP Vulnerability Management standard | | environment but mitigated or documented as accepted risks. |
| **5.0** | **Acceptable Use** | | |
| **5.1** | Acceptable use policies must define the organisation's rules on how employees and third-party users of the organisation's systems are permitted to use business applications.<br>Certain conditions of acceptable use may vary from one organisation to another. However, these conditions must be in an accessible format, and clearly documented without ambiguity. | **ISF SoGP**<br>SM1.2<br>**NIST CSF**<br>PR.AT-1<br>**ISO 27002:2022**<br>5.10 | Acceptable Use Policy exists which describes the acceptable/unacceptable use of business applications.<br>Evidence of communication to employees (e.g., through onboarding, or awareness training). |
| **6.0** | **Web Application protection** | | |
| **6.1** | Appropriate security controls (both technical and administrative) commensurate to compliance requirements and risk must be in place for web applications and web content. | **ISF SoGP**<br>BA1.3<br>**ISO 27002:2022**<br>5.23 | A formal IT Health Check, or at the very minimum an appropriately scoped web |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | 8.23<br>8.26<br>8.27<br>**NIST CSF**<br>ID.GV-3<br>ID.RA-5<br>PR.AT-3<br>PR.IP-4<br>PR.PT-5<br>DE.CM-1<br>**CIS v8**<br>4.4<br>9.3<br>13.1<br>18.1-18.5 | application will confirm the web application protection is sufficient in a proactive manner. |
| **6.2** | When developing or acquiring cloud applications, organisations must adopt processes which apply the NCSC Cloud Security Principles, in accordance with risk assessments and compliance requirements. | | Application-specific risk reports detailing threats, risks, and controls applied. |
| **6.3** | Technical security controls, such as a Web Application Firewall (WAF) must be utilised. Organisations must consider any risks identified to build on minimum core protection rules (OWASP core rules are a good start), providing mitigation against the most likely vulnerabilities. | | Low-Level Design and Risk Assessment detailing controls to be used and controls applied within design. |
| **6.4** | Where applicable, and in accordance with the service classification of the application, single points of failure must be avoided in the application design. The use of load balancing and/or other components and services to balance capacity with service demand should be considered.<br>High-availability components will assist in avoiding service downtime due to faults or maintenance. | | Low-Level Design document, detailing the compliance with the application service classification. For example, a critical business application has high-availability architecture – dual data centre, no single points of failure, load balancing, and flexible resources. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | | |
| **6.5** | Web content must be appropriately categorised and/or labelled for intellectual property rights, and/or appropriate attribution to the source material. | | Sample of information available on web application. |
| **6.6** | Protective monitoring of the web application will apply reactive verification of the web application protection. | | Protective monitoring logs and events. |
| **7.0** | **Information validation** | | |
| **7.1** | The confidentiality, integrity, and availability of information processed by business applications (including web applications) must be protected by appropriate security controls.<br>Minimum protection requirements must validate input type, size, and appropriateness, including checks for code injection and malware insertion. | **ISF SoGP**<br>BA1.3<br>**NIST CSF**<br>PR.AC-6<br>RS.AN-5<br>**ISO 27002:2022**<br>8.26<br>8.29 | A web application Penetration Test will test input and output validation.<br>A completed Remediation Action Plan will demonstrate that vulnerabilities have been assessed, prioritised, and remediated according to importance. |
| **8.0** | **End-User Developed Applications**<br>**Linked Documents:**<br>• Management of High-Risk Applications Standard<br>• System Access Standard<br>• Identity and Access Management Standard | | |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | • Information Management Standard<br>• Robotic Process Automation Guidance<br>• Information Transfer Guidelines | | |
| **8.1** | A process or methodology, documented in policy, must be adhered to for the development of End User Developed Applications (EUDA) in order to meet the organisation's security requirements. | **ISF SoGP**<br>BA2.1<br>SA1.1<br>SA1.2<br><br>**NIST CSF**<br>ID.GV-3<br>PR.IP-2<br>PR.IP-3<br>PR.AT-2<br>PR.AC-1<br>PR.AC-4<br>PR.AC-6<br>PR.PT-3<br><br>**ISO 27002:2022**<br>5.9<br>5.15<br>8.3<br>8.26<br><br>**CIS v8**<br>5.6<br>6.8<br>16.10 | Documented EUDA development methodology.<br><br>Documented policy covering specific deployment and use topics. |
| **8.2** | The term EUDA provides a broad term for defining user developed systems. Therefore, organisations must identify which industry recommended development practices are applicable and apply these through the process. This may include controls such as version control, staged development, training and testing before rolling into live, change management and end of life processes. | | Documented EUDA development and lifecycle methodology.<br><br>Audit of repository of EUDAs.<br><br>Job role profiles defining the responsibility for the development of EUDAs.<br><br>Records of training or competency for individuals who are responsible for EUDAs. |
| **8.3** | Organisations must consider data privacy and protection aspects (see Ref 1.3 – DPIA) when developing EUDAs. | | See 1.3 |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | | |
| **8.4** | Input validation, access controls and user restrictions to powerful functionality must be applied to critical EUDAs created using office productivity suites (including word processing, spreadsheets, lists and presentations). | | Review of risk assessments or application design, detailing aspects such as access control, permissions (read/write), and input validation (e.g. pre-defined inputs).<br>Review of application showing controls applied during use. |
| **8.5** | Controls must be considered for automation and business information analysis tools. This is especially important for critical functions.<br>This helps to prevent data breaches or unauthorised disclosures of data. | | Review of risk assessment outputs or application design, detailing aspects such as automation, workflows, and sharing permissions. |
| **8.6** | Open access to powerful functionality and systems must not be granted unless explicitly required for the execution of the task. Any process/tool accessing data or services of a powerful or sensitive nature must be uniquely identified, appropriately authorised and have accesses restricted to least privilege. | | Audit records of access requests for applications.<br>Privileged access request records. |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | Access to enhanced permissions or privileges must be through elevation of privileges, for no longer than necessary for the task. | | Access Control Policy.<br>Elevation of privileges for no longer than necessary. |
| **8.7** | When sharing content, organisations must have procedures which make use of document content inspection tools to identify hidden or automated content and remove it to prevent unauthorised data disclosure. | | Documented processing procedures.<br>Use of file conversion within procedures (e.g. converting to PDF to prevent hidden information being disclosed). |
| **9.0** | **Protection of Application Databases**<br>**Linked Documents:**<br>• System Access Standard<br>• Identity and Access Management Standard | | |
| **9.1** | Many software applications rely on databases that also contain sensitive information. Therefore, open access to databases must not be granted. Any database being accessed must have each entity accessing that database uniquely identified in logs, appropriately authorised, and have accesses restricted to least privilege. | **ISF SoGP**<br>BA2.3<br>SA1.1<br>SA1.2<br>**ISO 27002:2022**<br>5.15<br>8.3<br>**NIST CSF**<br>PR.AC-1<br>PR.AC-4<br>PR.AC-6<br>PR.AT-2 | Audit of access requests for applications.<br>Audits of access control lists will highlight discrepancies between access permissions and access requests.<br>Audits of activity within applications by privileged and |

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| | | PR.PT-3<br>**CIS v8**<br>3.1<br>3.3<br>5.6<br>6.7<br>6.8<br>16.10 | non-privileged users, bound to credentials, supporting the non-repudiation principle. |

## 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 IT 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.

## 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

This statement may be adapted 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 version | 14/08/2023 |
| 0.2 | PDS CYBER | Initial feedback applied | 20/10/23 |
| 1.1 | PDS CYBER | New template applied and controls updated | 01/10/24 |

## Approvals

| Version | Name | Role | Date |
|---|---|---|---|
| 1.0 | NCPSB | National Cyber Policy & Standards Board | 30/11/23 |
| 1.1 | NCPSB | National Cyber Policy & Standards Board | 26/11/24 |

## Document References

| Document Name | Version | Date |
|---|---|---|
| ISF - Standard of Good Practice (for Information Security) | v2024 | 03/2024 |
| 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 |
| 10 Steps to Cyber Security - NCSC.GOV.UK | Web Page | 05/2021 |
| NCSC Cloud Security Principles | Web Page | 09/2024 |