NPCC
National Police Chiefs' Council

POLICE
DIGITAL
SERVICE

CYBER STANDARDS DOCUMENT

Systems Management

ABSTRACT:
This standard defines the requirements which, when applied, will assist with the secure management of systems and networks.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

ISSUED	February 2025
PLANNED REVIEW DATE	January 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 design, building and managing systems hosting policing systems and data.

Introduction

The System Management standard specifies requirements regarding design, build and management of systems to enable them to operate securely and cope with current and predicted workloads. It aims to provide PDS and policing with clear direction for properly designing, building and managing systems hosting policing systems and data.

Examples of how this may be achieved are:

Configuration of systems and networks, including

- Web Servers,
- Virtualisation and containerisation technologies
- Network Storage Systems

Ensuring proper maintenance through

- Service Agreements
- Performance and Capacity Monitoring
- Backups
- Change Management

These examples and other related actions that ensures robust system management are the focus of this document and are detailed throughout.

Applying system management controls will ensure the confidentiality, integrity and availability of policing systems and data. This concept is echoed in the National Policing Community Security Policy principles 4, 5 and 6, which specifically address confidentiality, integrity, and availability as integral to the foundation of all information security activity.

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.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

- Design and build systems, including web servers and virtual instances (including containers), to operate securely and cope with current and predicted workloads. Configure them in a consistent, accurate manner to protect them (and the information they process and store) against malfunction, cyber-attack, unauthorised disclosure, corruption, and loss.
- Manage the security of systems by performing regular backups of essential information and software, applying a rigorous change management process, managing capacity requirements, and monitoring performance against agreed service agreements.

This standard describes the formal requirements, which detail system management processes, actions and configurations that can be applied to policing systems.

Audience

Members of the Policing Community of Trust.

More specifically the standard is targeted at IT architects, developers, IT administration & support personnel, and security experts tasked with designing and building solutions and applications.

The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of the use of technology within policing:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Auditors providing assurance services to PDS or policing.

Finally, Policing's reliance on third parties means that suppliers acting as service providers or developing products or services for PDS or policing, should also be made aware of and comply with the content of this standard, in relation to their work on Policing systems and data.

Scope

1. This standard applies to systems handling policing data within the OFFICIAL / OFFICIAL-SENSITIVE tier of the Government Security Classification Policy (GSCP). National policing IT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.
2. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.
3. Additional controls may be applicable based upon the security classification of the information being processed by the external supplier's ICT systems, applications, or service implementations.

Requirements

Ref	Minimum Requirement	Industry best practice	Control Reference	Compliance Metric
1.1	**System and Network Installations**			
1.1.1	Standards or procedures must exist which require systems and networks to follow the organisation's security architecture principles, and other requirements such as business, security and compatibility, as well as foreseeable changes in the use of IT. **See also:** NCSP Physical Asset Management NCSP Network Security standard	CIS Controls and Configurations from CIS Benchmarks	**NIST CSF 1.1** PR.MA.1 PR.PT.4 PR.IP.1 DE.AE.1	Local documentation that describes patterns, builds and standards for systems and networks. Evidence that projects and managed changes adhere. Critical systems and networks are demonstrably protected from untrusted / lower criticality environments.

Ref	Minimum Requirement	Industry best practice	Control Reference	Compliance Metric
1.1.2	Critical systems and networks should be segregated from untrusted networks physically or virtually. **See also:** NCSP Network Security standard			
1.1.3	Design networks to Consider the segregation of traffic with different security requirements, levels of trust, or purposes e.g. high-volume traffic such as VOIP / SAN data. Use firewalls to restrict traffic to flow as designed. Minimise untrusted gateways. Use device authentication by default, including within datacentres and server rooms. Enable the removal or quarantine of unauthorised or potentially compromised devices. **See also:** NCSP Network Security standard			Network designs include decisions or show consideration for these points. Security testing.

Ref	Minimum Requirement	Industry best practice	Control Reference	Compliance Metric
1.1.4	System and Network installations should follow the National cyber security architecture principles: • Security Fundamentals (Core Security) • Security by Design • Segregation and • Segmentation • Virtualisation • Application Security • Protective Monitoring • Automation and Orchestration • Defend as One Additionally implementing: • Principle of Least Privilege • Use of Naming Conventions • Avoiding Single points of Failure • Fail secure • Having appropriate capacity • Ensuring available options for ongoing maintenance and enabling continued support • Restricting and logging access to administrative tools **See also:** National Cyber Security Architectural Principles			Network designs include decisions or show consideration for these points.

1.2	**Zero Trust and Micro Segmentation**			
1.2.1	Standards should exist to direct a Zero Trust approach for all networks and systems design. Protect critical resources by micro-segmentation including using: • Identity and Access management to control which resources can be accessed. Use SSO and MFA to strengthen this for users. • Segmentation gateways to enforce access control at the application layer. • Monitor and analyse access to identify and flag events for further investigation. **See also:** NCSP Identity & Access Management standard	Reviewing NIST.SP.800-207 Zero Trust guidance and principles CIS Controls	Not covered by NIST CSF 1.1	Network designs include decisions or show consideration for a zero-trust approach

1.3	**Web Server design and configuration**			
1.3.1	Documented standards/procedures should exist which require web servers to: • Avoid disclosure of system configuration information e.g. through http headers • Use controls to protect web application sessions • Redirect HTTP connections to HTTPS • Ensure that ALL resources are delivered over enforced TLS • Use a /.well_known/security.txt file to provide a safe means of being informed about security issues with services. • Protect web application sessions through ensuring that session IDs cannot be predicted, setting secure flags on cookies, ensuring that cookies are created limiting their access as much as possible **See also:** NCSP Physical Asset Management standard	Do Threat Modelling, review the OWASP Top 10 and consider appropriate controls to mitigate. A01:2021-Broken Access Control A02:2021-Cryptographic Failures A03:2021-Injection A04:2021-Insecure Design A05:2021-Security Misconfiguration A06:2021-Vulnerable and Outdated Components A07:2021-Identification and Authentication Failures A08:2021-Software and Data Integrity Failures A09:2021-Security Logging and Monitoring Failures A10:2021-Server-Side Request Forgery CIS Controls and Configurations from CIS Benchmarks	**NIST CSF 1.1** PR.PT.3	Web Server designs consider these points. ITHC reports do not highlight any of these issues which are commonly found.

1.3.2	APIs should: • be configured securely and exposed only to necessary networks • be managed using an API management tool • take into consideration compatibility requirements for future changes APIS on untrusted interfaces must: • be protected by an API gateway configured to block malformed or potentially malicious requests • be monitored			Network designs include decisions or show consideration for these points. Monitoring use cases. Security testing.
1.3.3	Outbound internet access should be managed, including ensuring that: • Users are authenticated • Access is only permitted to authorised websites • Web traffic is inspected for malicious content • Web traffic is logged for later investigation			A formal policy requiring adherence and technical controls preventing bypass.

1.3.4	• A register of internet domains should be maintained, recording details of domain name, registrar, service hosting location, ownership, any 3rd party support, certificates issued, and dates for domain name and certificate renewal. • Consider registering similar domains if appropriate, balancing cost and risk • Maintain a register of domain names outside of organisational control which may be illegitimate or used for nefarious purposes.			A formally owned and managed register with a documented process / procedure for management.
1.3.5	• Maintain a register of certificates used for TLS, including certificate authority and expiration dates. • Proactively move to automated certificate renewal wherever possible, aim for shorter life-span certificates to reduce exposure. • Monitor Certificate Transparency logs for certificates issued for all owned domains • Issue Certificate Authority Authorisation (CAA) records for all managed domains. **See also:**			An up-to-date register. A documented process showing the monitoring of CT logs. CAA records in place.

	NCSP Cryptography standard NCSP Technical Security Management standard			

1.4	**Foreign Sources Management**			
1.4.1	Consider and evaluate the use of Web Analytics services, ensuring that their scope (e.g. which pages are monitored, which form fields are collected) is appropriate and maintain a record of the approach taken.		Not covered by NIST CSF 1.1	A record of the evaluation of any such services in use.
1.4.2	A register of third-party applications integrated into systems must be maintained. These applications must be subject to a security review and approval prior to installation or integration.			A record of any such applications in use.

1.5	**Virtualisation and Containerisation**			
1.5.1	Physical Hardware hosting virtualised or containerised systems must meet the same standards as those that hosting services directly. E.g. Police Assured Secure Facility (PASF.) This includes: • physically protected within secured environments • restricting physical access • requiring authorisation prior to access. **See also:** NCSP Physical & Environmental Security standard	CIS Controls and Configurations from CIS Benchmarks	Not covered by NIST CSF 1.1	Designs show considerations for physical security requirements for hardware.
1.5.2	Virtualisation hypervisors and the procedures used to administrate them must: • Apply appropriate separation of virtual hosts according to system sensitivity requirements • Protect information in transit between virtual hosts e.g. using TLS • Ensure physical hardware does not become overloaded • Avoid unnecessary creation of virtual hosts			Designs show consideration of hypervisor security.
1.5.3	Virtual Instances must be configured to use a consistent, repeatable process to build each virtual instance to a well configured base image, with a known and consistent approach to patch management, system hardening, vulnerability scanning, instance monitoring, protective monitoring, and host-based security systems such as anti-malware and IDS/IPS. **See also:**			Designs and assurance show well managed and well configured instances.

	NCSP Technical Security Management standard			
1.5.4	Container Orchestration tools should be used to centrally manage all containers. All hosts which support containers, container engines, container orchestration tools or other dependent systems should be configured securely, hardened to reduce exposure of unnecessary ports or services, and managed centrally.			
1.5.5	Containers should be managed to ensure that information is protected in transit (e.g. TLS), containers are appropriately separated from other containers, or are grouped according to purpose and sensitivity, and operate with a minimal set of privileges. Where containerised applications are deployed through code, a secure development methodology must be used. **See also:** NCSP Cryptography standard			

1.6	**Network Storage Systems**			
1.6.1	Standards should exist to ensure that network storage systems, including NAS and SAN technologies are properly managed, including consideration of: • Design and configuration • Physical security • Malware protection and patch management • Encryption at rest and key management • Access control and anonymous access • Exposure of network interfaces • Encryption in transit **See also:** NCSP Security Management standard NCSP Cryptography standard	CIS Controls and Configurations from CIS Benchmarks	Not covered by NIST CSF 1.1	Standards or procedures showing these points are considered

1.7	**Service Agreements**			
1.7.1	Service Agreements should include: • Responsibilities for equipment and services being provided • Expected levels of service, including service criticality, hours of operation, capacity requirements, permissible downtime, RTO and RPO, and agreed penalties for failing to meet these requirements. • Requirements for vetting and clearance of staff • Methods of administration, including authentication, administrative interfaces, restrictions on connection (e.g. connectivity, suitable devices or source locations) • Requirements for role separation, segregation of duties, minimum levels of training and/or qualification for critical roles. • Requirements for technical controls such as encryption at rest and in transit, network monitoring, vulnerability management, change management and patch management. • Expectations for service design documentation, information assurance requirements and independent assurance obligations (e.g. CHECK ITHC) • Requirements for operational security management including security incident management, attendance at security boards. **See also:** NCSP Physical Asset Management standard		**NIST CSF 1.1** PR.AT.3	Service agreements reviewed and assessed by an information security specialist, approved by a business lead and the service provider, and evidence of regular review

1.8	**Change Management**			
1.8.1	Change management processes must exist and be adhered to for all modifications to systems and networks. Changes must be documented, tested and approved by appropriate roles to ensure that they are technically appropriate, any impact to information security assurance (e.g. by impacting security controls, introducing unassured systems, changing the information being processed, or impacting compliance or regulatory requirements) is evaluated and undertaken, and that plans to implement and roll-back changes are suitable. The change management process should ensure that necessary parties are given pre-agreed notice of changes to allow proper evaluation. Changes undertaken as part of an incident response (such as an 'Emergency' or 'Priority 1' change) must follow an appropriate approval, or pre-approval route, and should still be required to be properly documented and evaluated. **See also:** NCSP Physical Asset Management standard	CIS Controls	**NIST CSF 1.1** PR.IP.3 - PR.MA.1	A change management process exists and is in use for all changes.

1.9	**Performance and Capacity Monitoring**			
1.9.1	Systems and networks should be monitored to ensure that they meet predefined needs for performance and capacity for business users. This monitoring should include alerting and agreed responses to indications of the services failing to meet the requirements. Responses may include restrictions to non-critical services, or prioritisation of critical services, or scaling of resources to meet requirements. Monitoring should include measurement of services provided to users as well as thresholds on resource use within systems. Capacity planning must also take place to ensure that systems are able to scale up or down according to predicted business needs.		**NIST CSF 1.1** PR.DS.4 DE.CM.6 RS.AN.1	Evidence of ongoing performance and capacity monitoring e.g. meeting minutes, capacity planning.

1.11	**Cyber Security Exercises**			
1.11.1	Periodic exercises should be conducted to a documented and approved schedule. A programme should include agreed techniques for planning and running repeatable exercises.	CIS Controls	**NIST CSF 1.1** PR.IP.10	
1.12	**Resilient Technical Environments**			
1.12.1	Critical services should have methods that ensure required OLA and SLAs. Where appropriate consider backup hardware, software and physical sites.		**NIST CSF 1.1** ID.BE.5 PR.PT.5	
1.13	**Security Architecture**			
1.13.1	Standards should exist to support the delivery of complex secure services across Policing.		**NIST CSF 1.1** PR.AC.4	

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.

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

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 according to Force or PDS Policy needs.)

Equality Impact Assessment

The implementation of this standard should include a local Equality Impact Assessment. Controls used for system management could exclude individuals with various disabilities, and these should be considered carefully as part of the impact assessment.

(Adapt 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
1.0	PDS Cyber	Original version	
1.1	PDS Cyber	Annual review	19/11/24

Approvals

Version	Name	Role	Date
1.1	NCPSB	National Cyber Policy & Standards Board	06/02/25

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