CYBER STANDARDS DOCUMENT

NCSP Network Security

ABSTRACT:

This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running network services on behalf of national policing. This standard details a minimum set of security requirements and controls that must be met to ensure security and segregation of network services.

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.

Introduction

This Network Security Standards document provides the list of controls that are required for business applications, information systems, networks and computing devices. This list of requirements ensures a baseline level of security to afford the necessary level of protection to its systems and data. Furthermore, the security controls presented in this standard are taken from examples of international best practice for information security and is intended to be used for National Policing Systems.

This document should be read in conjunction with other NCSP standards and guidelines.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running network services on behalf of national policing. This standard details a minimum set of security requirements and controls that must be met to ensure security and segregation of network services.

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

Networks and Communications

- Design physical, virtual, wireless and voice networks to be reliable and resilient; prevent unauthorised access; encrypt connections; and detect suspicious traffic. Configure network devices (including routers, firewalls, switches, and wireless access points) to segregate networks into domains, to function as required and to prevent unauthorised or incorrect changes.

Audience

This standard is aimed at:

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

Additionally, roles involved in information risk governance such as Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs) should have awareness of this standard.

Scope

1. This standard is to cover systems handling data within the OFFICIAL tier including OFFICAL-SENSITIVE special handling caveat 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 networking systems that are provisioned for policing community of trust use.
3. This standard is applicable for all networking systems used within the police community of trust including both physical and virtual environments.

Requirements

The following sections detail the minimum requirements for ensuring the secure and efficient management and operation of policing community of trust networks.

Consideration is given to the following areas:

Reference	Minimum requirement	Control reference	Compliance Metric
1. Secure Network			
1.1	Policing networks must be designed securely in line with security architectural principles, design standards and frameworks (e.g. Zero Trust, Defence-in-Depth, Security by design, Least Privilege), in line with compliance requirements and proportional configurations to defend networks against threats and protect resources within the network.	SOGP TI2.1 CISv8 16.10	Evidence of: • assurance process • design decisions • detailed requirements • security controls have been implemented and are effective through ITHC • detected incidents
1.2	Design documentation for networks and network devices must be maintained and include relevant configuration settings, technical information, topologies and network diagrams. An inventory of all communication equipment and services must also be held along with device backups. This information must be held securely with controlled access.	SOGP TI2.2 SOGP NC1.2 NIST CSF2.0 PR.PS-01, ID.AM-01, ID.IM-02	Evidence of: • documented network diagrams and topologies • managed inventories of equipment and services • security controls have been implemented and are effective through ITHC
1.3	Network segmentation must be enforced throughout designs to ensure isolation between applications, resources, workloads and environment types.	NIST CSF PR.AC-P5 SOGP NC1.2, TI2.2	Evidence of: • design decisions • detailed requirements • documented network diagrams and topologies

Reference	Minimum requirement	Control reference	Compliance Metric
	The level of segmentation and methods of implementing it will vary between use cases and should be determined using risk assessments. Segmentation can be achieved by one or more of the following: • network security appliances • network virtualisation • software-defined perimeters • host-based firewalls • network access control lists • resource security groups • demilitarised zones (DMZ)		• security controls have been implemented and are effective through ITHC
1.4	Zero-trust principles should be adopted to continuously verify, authenticate and authorise transactions to the policing network and between resources in segregated network segments.	SOGP TI2.1 NIST CSF PR.AC-5, PR.AC-7	Evidence of: • design decisions • security controls have been implemented to enforce Zero-Trust and are effective through ITHC
1.5	Production (live) environments must be segregated from non-production environments such as development and testing networks.	NIST CSF PR.AC-5, PR.DS-7	Evidence of: • assurance process • design decisions and network topology showing segmentation • security controls have been implemented and are effective through ITHC • documented environments with purposes and boundaries • documented promotional activities that move services and applications between environments

Reference	Minimum requirement	Control reference	Compliance Metric
1.6	Policing must ensure the appropriate availability of networks and services is maintained. Availability should be derived from assessment of BIA and network requirements which should consider: • single points of failure • target SLAs for underlying services and failover scenarios • high availability / clustering / availability zones • contracted support arrangements		
2. Cloud Network Security			
2.1	Network segments must be isolated from one another and grouped into related workloads. If network segments need to communicate with each other, then that traffic should be explicitly permitted and controlled with technical controls, such as those listed in 1.3	NIST CSF PR.AC-P5 SOGP NC1.1	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • Network topology showing the segmentation and grouping
2.2	Zero trust principles should be adopted to: • Explicitly verify all transactions by continuous authentication and authorisation • enforce least privilege access with Just-In-Time and Just-Enough-Access • minimise the blast radius of any incidents by segmenting networks with strong access controls	SOGP TI2.1 NIST CSF PR.AC-5, PR.AC-7	Evidence of: • design decisions • network topologies clearly showing the boundaries where zero-trust is applied and the rule documented that are being enforced • security controls have been implemented to enforce Zero-Trust and are effective through ITHC

Reference	Minimum requirement	Control reference	Compliance Metric
2.3	Identity-based controls should be applied to network resources to allow connectivity between resources and networks.	NIST CSF PR.AC-4, PR.AC-7, DE.AE-1	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • review of network security audit logs
2.4	All traffic flows, north-south, such as internet connectivity, and east-west, between clients, applications and service/resources, must be inspected, monitored and secured at network security boundaries.	NIST CSF PR.AC-5, PR.PT-3, DE.CM-1	Evidence of: • design decisions • a process for establishing a baseline traffic • security controls have been implemented and are effective through ITHC • network traffic inspection logs and reporting • review of network security audit logs
2.5	Ingress and egress traffic filtering must be applied at network security boundaries.	NIST CSF PR.AC-5, PR.PT-3, DE.CM-1, PR.PS-04	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • network traffic inspection logs and reporting • audit trail of ALCs review and change management process
2.6	Resources must not be exposed to the internet by default and traffic must be routed through the proxy or secure internet gateway.	NIST CSF PR.PR-4, PR.AC-5, PR.DS-5	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC

Reference	Minimum requirement	Control reference	Compliance Metric
			• audit trail of review of routing information
2.7	Encryption in transit must be enforced across all cloud services (see Cryptography Standard for cryptographic requirements)	NIST CSF PR.DS-2	Evidence that: • design decisions • encryption security controls have been implemented and are effective through ITHC
2.8	Network appliances and services must be configured to: • facilitate monitoring of capacity and highlight overload or exception conditions when they occur • log all security-related events in a form suitable for review, and available for review • integrate with access control mechanisms in services • alert when a change is made	NIST CSF PR.IP-1, PR.IP-3, PR.PT-1, PR.PS-01, PR.PS-04	Evidence of: • configuration decisions • audit trail of review of security log information and its availability • audit trail of review of device/service capacity • audit trail of change management
2.9	Network security should be continuously evaluated against security frameworks to improve and maintain policing's cloud network security posture.	NIST CSF PR.PT.4, DE.AE-1, PR.PS-01	Evidence of: • configuration decisions • audit trail of review of security controls
3. Network Device Configuration			
3.1	There must be documented practices for configuring and managing network appliances which cover the following areas: • standard security management practices • network appliance access management • vulnerability and patch management	SOGP TI1.2 NIST PR.IP-12, PR.PS-01	Evidence of: • documented assurance process • documented process for configurations and management of network appliances and its regular review • audit trail of the review cycle and documented

Reference	Minimum requirement	Control reference	Compliance Metric
	• modifications to device configurations and settings • regular reviews of network device configuration and set-up.		change management process • documented vulnerability management and remediation plan
3.2	Network appliances must follow standard security management practices, which include: • strong access control to management interfaces of network devices • running a fully supported operating system • hardening the operating system (e.g. by disabling unnecessary services and functionality, applying security patches and configuration best security practices) • utilising management tools for remote maintenance and support • security and health monitoring of network devices to identify issues and respond effectively review and verification of configurations and applied settings	NIST CSF PR.AC.1, PR.AC.4, PR.MA-2, PR.PS-01	Evidence of: • documented assurance process • security management practices and risk assessments upon which security controls and security practices have been derived • review documented change management process • review of vulnerability management and remediation plan
3.3	Network devices must be configured to: • facilitate network appliance monitoring of resources • use common trusted time source to ensure consistency of timestamps (e.g. using GPS-based time servers, atomic clock or trusted NTP pools)	NIST CSF PR.DS-4, PR.AC-7, DE.AE-1, PR.IR-2, PR.PS-01	Evidence of: • documented assurance process • documented process for configurations and management of network appliances and its regular review

Reference	Minimum requirement	Control reference	Compliance Metric
	• log security-related events • integrate with access control mechanisms in other devices or service to provide strong authentication • use port-level access control (e.g. using 802.1x or similar network access control protocols) • limit malicious activity and lateral movement in the event one or more network zones/segments become compromised.		• security implemented security controls and its effectiveness through ITHC
3.4	Access to network devices must be restricted to only authorised staff and aligned to the principle of least privilege.	NIST CSF PR.AC-5, PR.AC-7	Evidence of: • documented process for configurations and management of network appliances and its regular review • implemented security access controls and its effectiveness through ITHC
3.5	A process for vulnerability management in network devices must include: • continuous monitoring for known vulnerabilities (e.g. by monitoring security vendor websites, NMC threat intel bulletin or running vulnerability scanning software) • testing patches prior applying them in a timely manner with a	SOGP TP2.1 NIST CSF ID.RA-1, PR.IP.12, DE.CM.8	Evidence of: • documented vulnerability management plan including patching and risk acceptance • policies and schedules for vulnerability discovery • vulnerability risk mitigation activities • documented “failed-patch” restore process

Reference	Minimum requirement	Control reference	Compliance Metric
	recovery steps ready upon a failed vulnerability patch that can be applied See Vulnerability Management Standard.		
3.6	Network appliances that perform routing should make use of dynamic routing protocols. They must also be configured to prevent unauthorised or incorrect updates by: • verifying the source of routing updates • verifying the destination of routing updates (e.g. by transmitting updates only to specific routers) • routing information must be protected by authenticating the exchanges (e.g. passwords/passphrases) and the encrypting the routing information being exchanged.	SOGP NC1.1 NIST CSF PR.AC-5, PR.PT-4, IR-01, PR.PS-01	Evidence of: • Security controls have been implemented and tested through the ITHC • Routing configurations have been fully tested and reviewed
3.7	Network appliances that require Domain Name System (DNS) must be configured to use trusted DNS servers (e.g. enterprise-controlled DNS servers).	SOGP NC1.1 NIST CSF PR.AC-5, PR.PT-4, PR.IP-1	Evidence of: • documented process for configurations and management of network appliances and its regular review
3.8	Network devices must be reviewed on a regular basis to verify configuration settings (e.g. routing tables and parameters), evaluate password strengths and to assess activities performed on the network device (e.g. by automatically inspecting exported logs and generating alarms when needed).	SOGP NC1.1 NIST CSF - PR.DS.6, PR.IP.3, PR.PT-4	Evidence of: • documented process for configurations and management of network appliances and its regular review • controls and configurations security

Reference	Minimum requirement	Control reference	Compliance Metric
			verification report through ITHC testing - Alerts or rules for alerts documented
3.9	Technologies like Cisco's Dynamic Trunking Protocol (DTP), that make VLAN hopping trivial, must be turned off on all user facing network ports.	SOGP NC1.1 NIST CSF PR.IP.3	Evidence of: - documented process for configuration of network appliances and its regular review - controls and configurations security verification report through ITHC testing
4. Physical Network Security			
4.1	Telecommunication cabling, depending on criticality, must be protected by: - labelling communications equipment and cables - securely routing the communication cabling, using appropriate conduits and avoiding exposure to public access - securing access to termination points - providing alternative feeds or physical routing of cables - ensuring that power cables are segregated from communications cables to prevent interference - use of appropriate cable types depending on requirements	SOGP NC1.2 NIST CSF PR.AC.2 NIST CSF2.0 PR.PT.4	Evidence of: - documented cabling standards and diagrams - audit trail of physical inspections being carried out.
4.2	Network appliances and wireless access points must be protected by:	SOGP NC1.1, NC1.2	Evidence of:

Reference	Minimum requirement	Control reference	Compliance Metric
	• installing them in secure environments (e.g. locked rooms or cabinets) disabling any unused ports on them by default	NIST CSF PR.AC.2	• documented cabling standards and diagrams • audit trail of physical inspections of cabling and secure environments being carried out.
4.3	Network documentation (e.g. labels, diagrams, inventories and schedules) must clearly identify high-risk environments and data flows that could lead to significant business impact should they be compromised.	SOGP NC.1.2 NIST CSF ID.RA-4	Evidence of: • documented cabling standards and diagrams • audit trail of review of documentation, configurations and risk position
4.4	Critical or sensitive communication cabling and equipment must be: • regularly inspected to detect any physical damage or the presence of any unauthorised devices • verified against network documentation	SOGP SD1.4, SD2.8 NIST CSF PR.DS.6, PR.IP.3	Evidence of: • documented cabling standards and diagrams • audit trail of regular review of documentation and change control • audit trail of physical inspections of cabling and secure environments being carried out.
5. Wireless Access			
5.1	Wireless access which has direct onward connectivity to the force network must be subject to an information risk assessment and signed off by an Information Asset owner and/or SIRO, prior to its implementation.	SOGP NC1.1, NC1.3, AS1.1 NIST CSF - PR.AC.4	Evidence of: • risk assurance process and risk approval
5.2	There must be documented practices for configuring and management of wireless access appliances to the network which cover the following:	SOGP NC1.1, NC1.3	Evidence of: • documented process for configurations and management of network

Reference	Minimum requirement	Control reference	Compliance Metric
	• location and configuration of wireless access points • use of strong authentication of users and devices • use of secure encryption algorithms for protecting information in transit (see Cryptography Standard) • maintaining an asset inventory of authorised wireless access points • prevent and detect against unauthorised wireless access points and wireless devices	NIST CSF PR.IP-1, PR.AC-5	appliances and its regular review • controls and configurations security verification report through ITHC testing
5.3	Wireless access points must: • be configured to the required power setting that delivers the range required within organisation-controlled boundaries • be placed in locations that minimise the risk of interference • be configured and managed using a unified portal with restricted access to authorised users • be protected by using a Service Set Identifier (SSID) that does not reveal important information about the network • have its SSIDs disabled when not intended for use	SOGP NC1.1, NC1.3 NIST CSF PR.IP-1,PR.AC-5	Evidence of: • documented process for configurations and management of network appliances and its regular review • controls and configurations security verification report through ITHC testing
5.4	Wireless access must be protected by: • network access control (e.g. IEEE 802.1X)	SOGP NC1.1, NC1.3, SM2.3	Evidence of: • documented process for secure configurations and

Reference	Minimum requirement	Control reference	Compliance Metric
	• device authentication (e.g. EAP-TLS) or user authentication • using encryption (e.g. Wi-Fi Protected Access (WPA) version 2 or 3 • segregating wireless networks used for access by non-corporate devices (i.e. guest networks) • regularly scanning the wireless network to detect unauthorised wireless access points and wireless devices	NIST CSF PR.IP-1, PR.AC.4	management of network appliances and its regular review • controls and configurations security verification report through ITHC testing • audit trail of network scanning logs review
5.5	Critical/sensitive wireless access connections must be subject to additional security controls, such as Virtual Private Networks (VPNs).	SOGP NC1.1, NC1.3 NIST CSFPR.IP-1, PR.AC-4	Evidence of: • documented process for secure configurations and its regular review • controls and configurations security verification report through ITHC testing
6. External Network Connections			
6.1	External network connections to the organisation's systems and networks must be managed and documented to specify the following: • external connections must be identified, verified and logged • external access must be denied by default, and explicitly granted upon request • only authorised types of remote access device are permitted	SOGP NC2.1 NIST CSF PR.AC.7, PR.PT.4	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • audit trail of external connections review

Reference	Minimum requirement	Control reference	Compliance Metric
	• external connections must be removed when no longer required.		
6.3	Systems and networks accessible by external connections must be protected by methods of: • restricting external traffic to only required and specified parts of systems and networks through defined endpoints (e.g. API, reverse proxies, load balancers and network gateways) • validating the source of external connections (e.g. UK only IP addresses, or organization’s IP specific range) • blocking the IP address ranges of known bad actors or hostile nations • security-related activity must be logged and monitored • connection-related activity must be logged and monitored for established connections (e.g. the internet, VPN) • ability to identify possible security policy violations (e.g. attempts from unauthorised external networks to communicate directly with internal systems) • ability to isolate critical subnetworks if the network is under attack.	SOGP NC2.1 NIST CSF PR.AC-7, PR.AC.7, PR.PT.4, DE.CM-1	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • audit trail of external connections and log of any security-related events review

Reference	Minimum requirement	Control reference	Compliance Metric
6.4	Access to externally facing systems and networks must meet conditional access requirements, which includes verifying that devices: • have been authorised • are running up-to-date malware protection • have up to date operating systems and software patches installed • are connecting over a secure and encrypted network (e.g. a Virtual Private Network (VPN)) are running an up-to-date host-based (or personal) firewall with a predetermined standard configuration.	SOGP NC2.1 NIST CSF PR.AC.1, PR.IP-1	Evidence of: • security controls have been implemented and are effective through ITHC • audit trail of review of security controls and the log of authorised connections
6.5	Untrusted devices - those that do not meet minimum security configuration requirements specified by the security policy - must be automatically connected to an isolated network to update their configuration.	SOGP NC2.1 NIST CSF PR.IP.1, PR.AC-5	Evidence of: • security controls, including conditional access polices, have been implemented and are effective through ITHC • design decisions for segregated networksaudit trail of untrusted connections being connected to a dedicated network
6.6	External access to systems and networks (e.g. via internet connections) must be restricted and consideration given to the following technical controls: • establishing segmentation through means of demilitarised zone (DMZs) between internal	SOGP NC1.4, NC1.5, TS1.1, IR2.3 NIST CSF PR.AC.5, DE.CM.1	Evidence of: • design decisions • security controls, including conditional access polices, have been implemented and are effective through ITHC

Reference	Minimum requirement	Control reference	Compliance Metric
	networks and untrusted networks • access must be restricted to specific target (e.g. application, systems, resource) • routing network traffic through firewalls at the perimeter or internally between network segments • geolocation mechanism should prevent traffic from unauthorised locations		• audit trail of connection logs review
6.7	External access must be provided using managed remote access service/server, which: • provides reliable and complete authentication for external connections (e.g. by running an authentication system such as RADIUS or TACACS+, virtual workspaces or fully managed services) • provides required logs and information for security, health and performance monitoring	SOGP NC2.1 NIST CSF PR.AC-3, DE.CM-1	Evidence of: • security controls, including conditional access polices, have been implemented and are effective through ITHC • audit trail of connection logs review
6.8	External access to systems and networks must be: • subject to strong authentication (e.g. smartcards, tokens, biometrics or challenge/response devices featuring one-time passwords) • Automatically blocked if unauthorised or unusual activity is detected	SOGP NC2.1 NIST CSF PR.AC-7, PR.IP-1, DE.CM-1	Evidence of: • security controls, including conditional access polices, have been implemented and are effective through ITHC • audit trail of connection and security logs review

Reference	Minimum requirement	Control reference	Compliance Metric
	• Removed when no longer required		
6.9	Policing must ensure the availability of access to managed services and hybrid architectures by: • ensuring reliable and highly available internet connectivity • establishing multiple methods of connection (e.g. wired networks, wireless, mobile) • providing required network bandwidth between the organisation's network and the managed service	SOGP NC2.1 NIST CSF PR.DS-4	Evidence of: • design decisions and detailed requirements • security controls, including conditional access polices, have been implemented and are effective through ITHC • audit trail of health and performance logs review
7. Firewalls			
7.1	Networks should be protected from malicious or unnecessary traffic on other networks or sub-networks (internal or external) by using firewalls that can monitor, detect and block any unauthorised traffic.	SOGP NC2.2 NIST CSF PR.AC.5, PR.IP-1, DE.AC-1, DE.CM-1, DE.CM-7	Evidence of: • design decisions • security controls have been implemented and are effective through ITHC • audit trail of security logs review
7.2	Policing must use layer 7 firewalls to protect business applications, networks and services both on-premises and in cloud, by the use of technologies such as: • stateful network inspection firewalls, typically located at the boundary of a policing network for inbound and outbound traffic routing and analysis • application proxy firewalls	SOGP NC2.2 NIST CSF PR.AC.5, PR.PT-4, DE.CM-1	Evidence of: • design decisions • detailed requirements • security controls have been implemented and are effective through ITHC

Reference	Minimum requirement	Control reference	Compliance Metric
	• web application firewalls (WAFs) • other network device with capabilities similar to firewalls, such as network traffic filtering, inspection and blocking		
7.3	There must be documented practices for configuring and management of firewalls which cover the following: • filtering of specific types or sources of network traffic such as IP addresses, network ports and state of communication flow • blocking or otherwise restricting particular types or sources of network traffic • developing predefined rules (or tables) for filtering network traffic • restricting access to only authorised individuals • limiting the disclosure of information about networks and network devices • applying security architecture principles during configuration • regularly reviewing firewall rules and configurations	SOGP NC2.2 NIST CSF PR.AC-4, PR.AC.5, PR.IP-1, DE.AE-1	Evidence of: • documented assurance process • documented process for configurations and management of network appliances and its regular review • audit trail of change management process review
7.4	All firewalls must be recorded in the asset inventory with configurations stored in the CMDB and maintained throughout its lifetime, including the following details: • type of traffic being monitored	SOGP NC2.2 NIST CSF PR.IP-1, PR.IP-3, ID.AM-1,	Evidence of: • documented process for configurations and its management in the CMBD

Reference	Minimum requirement	Control reference	Compliance Metric
	• firewall rules and polices • justification for allowed and prohibited traffic • owner responsible for the firewall device type (e.g. hardware, software or cloud-based)	AD.IM-2, PR.AC.7	• audit trail change management process review
7.5	Firewalls must be configured to: • filter traffic so that only expected traffic flows are permitted • protect communication protocols that are prone to abuse (e.g. HTTPS, SSH, SMTP, DNS) • prevent denial of service attacks by enforcing rate limiting and DoS protection capabilities blocking ICMP, UDP network packets • block both incoming and outgoing traffic where the source address is known to have been spoofed based on threat intelligence feeds or a manual block list	SOGP NC2.2 NIST CSF PR.AC.5, PR.IP-1, DE.AE-1, PR.PT-4	Evidence of: • documented process for configurations firewalls and verification of controls through ITHC • audit trail change management process review
7.6	The firewalls configurations must be consistent (template/blueprint) with specific ruleset applied as required, and be: • developed, tested and maintained by trusted specialist and undergo formal approval	SOGP NC2.2 NIST CSF PR.IP-1, PR.IR-3	Evidence of: • documented process for configurations firewalls and verification of controls through ITHC • audit trail of change management process review

Reference	Minimum requirement	Control reference	Compliance Metric
	• default deny and fail closed principles must be used • use clear and consistent naming standards • are grouped, where possible have a comment to help understand the rule, including the change reference that created or updated it • are version-controlled and subject to change control		
7.7	Application firewalls should be used to protect organisation's applications, networks and systems by: • performing deep packet inspection on decrypted network traffic between IP-enabled components • handling protocol-specific rules, to help defeat attacks against protocol vulnerabilities • performing ruleset tunning to improve effectiveness • validating network services using automated source/destination groups for standard cloud-based applications (e.g. Microsoft Office 365), which allows the content of the group to be updated automatically and removes the need for regular rule changes when managing access to cloud services using IP intelligence to block unapproved IPs/domains and unwanted bots	SOGP NC2.2 NIST CSF PR.AC.5, PR.IP-1, DE.CM-01	Evidence of: • documented process for configurations firewalls and verification of controls through ITHC • audit trail of firewall rules, configuration and change management process review

Reference	Minimum requirement	Control reference	Compliance Metric
	- utilising the industry standard ruleset (e.g. OWASP CRS) to detect attacks		
7.9	All rules, new or modified, must be tested, tuned, reviewed and approved by the responsible person (network or system owner).	SOGP NC2.2 NIST CSF PR.AC-5, PR.PR-4	Evidence of: - approval process - documented process for configurations firewalls and verification of controls through ITHC - registers with an audit trail of the firewall rules and configuration review cycle and documented change management process - audit trail of the tested or modified rules and their effectiveness
7.10	Firewalls must be protected against attack by: - restricting administrative access to a limited number of authorised individuals through strong access controls incorporating the principle of least privilege access, RBAC, and where possible, just-in-time authorisation and multi-factor authentication - blocking management access on public IP addresses while permitting access only from the management LAN (VLAN) - administrative access to firewalls must be secure and encrypted	SOGP NC2.2 NIST CSF - PR.AC.5, PR.AC-7, PR.IP-1, DE.CM-01	Evidence of: - documented process for configurations of firewalls and management of access and verification of controls through ITHC

Reference	Minimum requirement	Control reference	Compliance Metric
	• unified centralised portal should be used to manage firewalls administrative access to firewalls • preventing firewall type and version information disclosure		
8. Remote Management			
8.1	Access to policing systems and networks by external individuals for remote maintenance purposes must be managed by: • restricting access to a limited number of authorised and vetted engineers • providing dedicated maintenance workstations or managed remote access services (e.g. Microsoft Bastion, hardened VDIs, VPN to a hardened jump box) • agreed scope of planned work • authorising connectivity before access is granted • strong access controls incorporating the principle of least privilege access, RBAC, Just-in-time and multi-factor authentication • requiring that access credentials be assigned to individuals, rather than shared • logging and monitoring activity undertaken throughout the duration of the session • performing an audit of remote maintenance activity.	SOGP NC2.3 NIST CSF PR.AC.3, PR.PT-4, PR.AC-4, DE.CM-1, DE.CM-3, DE.CM-7, PR.MA-2	Evidence of: • security controls for managing remote access have been implemented and are effective through ITHC • audit trail of the remote access sessions review

Reference	Minimum requirement	Control reference	Compliance Metric
8.2	Maintenance ports on network equipment must be protected by access controls (e.g. passwords, port blockers).	SOGP NC2.3 NIST CSF PR.AC-3, PR.MA-2,	Evidence of: • security controls for managing remote access have been implemented and are effective through ITHC • audit trail of maintenance port inspections review
8.3	Non-disclosure agreement(s) and security vetting must be signed and obtained by external suppliers' IT and information security staff prior to being granted access to the policing applications, systems or networks.	SOGP NC2.3 NIST CSF PR.IP-11	Evidence of: • the documented vetting and approval process and contractual agreements • audit trail of suppliers/contractors contracted to carry out the required work review

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

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

Forces should consider local impacts as a result of this standard being applied.

Document Information

Document Location

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

Revision History

Version	Author	Description	Date
0.1	PDS Cyber Architect	Initial version	10/10/23
0.2	PDS Cyber Architect	Updated following internal peer review	15/12/23
1.1	PDS Cyber Architect	Annual review	3/10/23
2.0	PDS Cyber Architect	Annual review	4/12/24

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for cyber standards	25/01/24
2.0	National Cyber Policy & Standards Board	National authority for cyber standards	06/02/25

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/24
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/22

CIS Controls	v8	05/21
NIST Cyber Security Framework	v1.1	04/18
NIST Cyber Security Framework	V2.0	09/24
CSA Cloud Controls Matrix	v4	01/21
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/21
NSCP Cryptography Standard	v2.0	25/07
Vulnerability Management Standard	V1.0	11/23