CYBER STANDARD DOCUMENT

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 within PDS & policing systems. This standard details a minimum set of security requirements and controls that must be met to ensure security and segregation of network services. Consideration is given to the following areas network device configuration, physical network management, wireless access, external network connections, firewalls and remote maintenance.

ISSUED	January 2023
PLANNED REVIEW DATE	November 2024
DISTRIBUTION	Community Security Policy Framework Members

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

Members should ensure that they are consulting the currently valid version of the documentation.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Andy Huffer	Initial version	10/10/2023
0.2	Andy Huffer & James Hyde	Updated following internal peer review.	15/12/23

Approvals

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

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
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

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 (NCSP) Framework and associated documents sets out National Policing requirements for network security.

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, 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 updates.

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: -

- Network Device Configuration
- Physical Network Management
- Wireless Access
- External Network connections
- Firewalls
- Remote Maintenance

Reference	Minimum requirement	Control reference	Compliance Metric
1. Network Device Configuration			
1.1	There must be documented standards/procedures for configuring network devices (e.g. routers, firewalls, switches and wireless access points), which cover: • security architecture principles • standard security management practices • device configuration • restricting access to network devices • vulnerability and patch management • changes to routing tables and settings in network devices • regular reviews of network device configuration and set-up.	SOGP – TS1.1, ISO: 27002:2022 – 8.27, CSA CCM v4: - IVS-05, NIST CSF - PR.AC.4, SOGP – IR2.4, SOGP – TM1.1, CSA CCM v4: - TVM-01, 03,05, NIST CSF - ID.RA.1	Evidence of document assurance process, formal review and document change control procedures.
1.2	Network devices must be configured to enforce segmentation of different networks, network zones or network domains, that are: • allocated different security zones/levels (e.g. segregating dedicated, classified networks from the corporate network) • assigned to different organisational units (e.g. human resources, finance, marketing) • trusted from untrusted networks (e.g. external	SOGP – NC1.1 NIST CSF - PR.AC.5, NIST CSF - PR.PT.3, NIST CSF - PR.PT.4, NIST CSF - PR.IP.1	ITHC report and remediation plan.

Reference	Minimum requirement	Control reference	Compliance Metric
	networks, operational networks or the Internet) • managed by the organisation from networks not controlled by the organisation (e.g. those run by a vendor or business partner).		
1.3	Security arrangements applied to network devices must incorporate security architecture principles (e.g. 'secure by design', 'defence in depth', 'secure by default', 'default deny', 'fail secure', 'secure in deployment' and 'usability and manageability').	SOGP – NC1.1, NIST CSF - PR.AC.4	Evidence of Security By Design process, including Threat Modelling, Business Impact Assessments and implementation of security controls within designs.
1.4	Network devices must be subject to standard security management practices, which include: • restricting physical access to network devices, to authorised staff (e.g. by locating them in protected data centres or dedicated, locked storage rooms) • running a fully supported and updated operating system • hardening the operating system (e.g. by patching all known vulnerabilities; disabling unnecessary services; removing unnecessary scripts, drivers, features and sub-systems; and changing insecure vendor-	SOGP – SA1.2, SOGP – SA1.4, NIST CSF - PR.AC.1 NIST CSF - PR.AC.4 SOGP – IR2.4 SOGP – PE1.2	Evidence of a risk management methodology adopted as part of the SbD (Secure-by-Design) process, incorporating cyber security controls, security management best practice and cyber assurance.

Reference	Minimum requirement	Control reference	Compliance Metric
	supplied default parameters such as passwords and Simple Network Management Protocol (SNMP) community strings) • applying a comprehensive set of management tools (e.g. maintenance utilities, remote support and enterprise management tools) • keeping network devices up to date (e.g. by applying change management and patch management) • monitoring network devices (e.g. using SNMP) so that events such as hardware failure and external attacks can be detected and responded to effectively.		
1.5	Network devices must be configured to: • facilitate monitoring of capacity and highlight overload or exception conditions when they occur • log specified security-related events in a form suitable for review, and record them on a separate system • integrate with access control mechanisms in other devices (e.g. to provide strong authentication) • use port-level access control (e.g. using 802.1x, or similar network access control protocols) • limit malicious activity in the event one or more network zones become compromised.	SOGP – SM2.3 SOGP – SY1.1 SOGP – SY2.2 SOGP – NC1.1 NIST CSF - DE.AE.1 NIST CSF - PR.DS.4	Evidence of a risk management methodology adopted as part of the SbD (Secure-by-Design) process, incorporating cyber security controls, security management best practice and cyber assurance.

Reference	Minimum requirement	Control reference	Compliance Metric
1.6	Access to network devices must be restricted to a limited number of authorised network staff, using access controls that support individual accountability, and protected from unauthorised physical access.	SOGP – PE1.1 SOGP – SA1.1 NIST CSF - PR.AC.1	Evidence of an Access Control Policy that defines user groups and technical access policies for users and admins.
1.7	There must be a process for dealing with vulnerabilities in network devices, which includes: • monitoring them for known vulnerabilities (e.g. by monitoring security vendor websites, tracking CERT advisories, subscribing to vulnerability notification services, using intelligence service providers or running vulnerability scanning software) • testing patches for network devices and applying them in a timely manner • issuing instructions to network specialists on the action to be taken if a network device fails • automatically re-routing network traffic to an alternative network device.	SOGP – TM1.1 NIST CSF - ID.RA.1 NIST CSF - ID.RA.2 NIST CSF - PR.IP.12 NIST CSF - DE.CM.8	Evidence that: • Security controls have been implemented through an up to date ITHC and remediation plan • Automatic re-routing has been tested • There are documented processes detailing action to be taken if a device fails • Notification/intelligence service subscriptions are in place
1.8	Network devices that perform routing (e.g. routers and switches) must be configured to prevent unauthorised or incorrect updates by: • verifying the source of routing updates • verifying the destination of routing updates (e.g. by	SOGP – SM2.6 NIST CSF - PR.DS.3 NIST CSF - PR.DS.3	Evidence that: • Security controls have been implemented through an up to date ITHC and remediation plan

Reference	Minimum requirement	Control reference	Compliance Metric
	transmitting updates only to specific routers) • protecting the exchange of routing information (e.g. by using passwords/passphrases) • encrypting the routing information being exchanged.		• Routing configurations have been fully tested • Penetration testing has taken place to validate encryption
1.9	Network devices must be configured to use trusted Domain Name System (DNS) servers (e.g. enterprise-controlled DNS servers and/or reputable, externally accessible DNS servers).	SOGP – NC1.1	ITHC and remediation plan with DNS servers in scope.
1.10	DNS servers must be configured to filter traffic using denylists, including: • forward resolution domain denylisting (i.e. blocking a lookup based on the query's domain name value) • forward resolution IP denylisting (i.e. blocking a DNS lookup's answer's IP address value) • reverse resolution domain denylisting (i.e. blocking a reverse DNS lookup's answer's domain name value) • reverse resolution IP denylisting (i.e. blocking a reverse lookup based on the query's IP address value) • hierarchical domain denylisting (i.e. blocking the resolution of any subdomain of a specified domain name) • homoglyph denylisting (i.e. blocking DNS queries that are deceptively similar to legitimate domain names).	SOGP – NC1.1 NIST CSF - PR.PT.4	Evidence that controls have been implemented through an ITHC.

Reference	Minimum requirement	Control reference	Compliance Metric
1.11	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 inspecting logs).	SOGP – SD1.4 SOGP - SD2.8 NIST CSF - PR.DS.6 NIST CSF - PR.IP.3	Evidence of: • Change control processes and up to date ITHC • Log audit procedures are in place and being carried out
2. Physical Network Management			
2.1	Telecommunication cables (i.e. network and telephone cables), depending on criticality, must be protected by: • attaching identification labels to communications equipment and cables • concealing the installation of cabling, avoiding routes through publicly accessible areas • using armoured conduits and electromagnetic shielding • locking inspection/termination points • providing alternative feeds or routing • segregating power cables from communications cables to prevent interference.	SOGP – NC1.2 NIST CSF - PR.AC.2 NIST CSF - PR.PT.4	Cabling standards documentation is in place and regular checks are being carried out.
2.2	Network access points must be protected by: • locating them in secure environments (e.g. locked rooms or cabinets) • disabling them on the network device (e.g. a network switch) until required.	SOGP – NC1.1 SOGP – NC1.2 NIST CSF - PR.AC.2	Evidence that the physical environment has been assessed through a process such as PASF. Regular penetration testing to ensure unused devices are disabled.

Reference	Minimum requirement	Control reference	Compliance Metric
2.3	Networks must be supported by documentation, which includes: • network configuration diagrams, showing nodes and connections • an inventory of communications equipment, software, links and services provided by external parties • an understanding of which network devices represent the network boundary (i.e. act as an interface between private and public networks) • one or more diagrams of in-house cable layouts for each physical location • configurations and settings for in-house telephone exchanges • details about telephones and associated wiring/cables.	NIST CSAF - ID.AM.1 SOGP - SM2.6 NIST CSF - DE.AE-1 SOGP - UEM-07	Evidence that the security controls have been implemented and tracked through a Configuration Management Database (CMDB) or Service Management tool.
2.4	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 - IR1.1 NIST CSF - ID.GV.4	Evidence that the security controls have been implemented and tracked through a CMDB or Service Management tool.
2.5	Network documentation (e.g. diagrams, inventories and schedules) must be: • kept up to date • readily accessible to authorised individuals • reviewed regularly by network specialists • generated automatically, using software tools.	SOGP – SD1.4 SOGP - SD2.8 NIST CSF - PR.DS.6 NIST CSF - PR.IP.3	Evidence that the security controls have been implemented and tracked through a CMDB or Service Management tool.

Reference	Minimum requirement	Control reference	Compliance Metric
2.6	Cabling and equipment must be subject to: • regular physical inspection to detect damage or the presence of any unauthorised devices • reconciliation against network documentation • investigations of suspected or actual misuse.	SOGP – SD1.4 SOGP - SD2.8 NIST CSF - PR.DS.6 NIST CSF - PR.IP.3	Evidence that the security controls have been implemented and tracked through a CMDB or Service Management tool.
3. Wireless Access			
3.1	Wireless access to the network (e.g. using Wi-Fi, satellite, microwave links, Bluetooth, infrared or ZigBee) 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, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence of approval and assurance.
3.2	There must be documented standards/procedures for controlling wireless access to the network, which cover: • placement and configuration of wireless access points (hardware devices that provide interfaces between the wireless network and a wired network) • treating wireless access as an external connection for environments that process critical or sensitive information • methods of limiting access to authorised users • use of encryption (e.g. Wi-Fi Protected Access 2 (WPA2)) for protecting information in transit	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	• maintaining an inventory of authorised wireless access points, which includes a documented business justification for each one • detection of unauthorised wireless access points and wireless devices (e.g. using automated discovery/mapping tools).		
3.3	Wireless access points must be: • configured to the minimum power setting that delivers the range required • placed in locations that minimise the risk of interference (e.g. away from radio transmitters, microwave equipment and cordless telephones) • configured and managed centrally (e.g. in a Network Operations Centre (NOC)) • protected by using a Service Set Identifier (SSID) that does not reveal important information about the network (which may be useful to an attacker).	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
3.4	Networks must be protected against unauthorised wireless access by using a security filtering device (e.g. a firewall or edge server).	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
3.5	Wireless access must be protected using layers of access control, including: • network access control (e.g. IEEE 802.1X)	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through an ITHC and appropriate

Reference	Minimum requirement	Control reference	Compliance Metric
	• device authentication (e.g. EAP-TLS) • user authentication.		documented policies and procedures.
3.6	Wireless access must be protected by: • using encryption (e.g. Wi-Fi Protected Access 2 (WPA2 or 3)) between endpoint devices and wireless access points • creating dedicated wireless networks (using a virtual local area network (VLAN) and a firewall) for access by non-corporate devices (i.e. guest networks) • changing encryption keys regularly or using client-specific tokens • scanning the wireless network for unauthorised wireless access points and wireless devices (e.g. by walking around buildings with a wireless network detector) on a regular basis and at least annually.	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through regular ITHC and appropriate documented policies and procedures.
3.7	Critical wireless access connections must be subject to additional security controls, such as Virtual Private Networks (VPNs).	SOGP – NC1.1, SOGP – NC1.3 NIST CSF - PR.AC.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
4. External Network Connections			
4.1	There must be documented standards/procedures for managing external network access to the organisation's systems and networks, which specify that:	SOGP – NC1.4 NIST CSF - PR.AC.7 NIST CSF - PR.PT.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	• external connections must be identified • systems and networks must be configured to restrict access • only authorised types of remote access device are permitted • details of external connections must be documented • external connections must be removed when no longer required.	SOGP – IR2.3	
4.2	Systems and networks accessible by external connections must be designed to: • use an agreed set of security controls for information formats and communications protocols • conceal computer or network names and topologies from external parties (e.g. by using dual or split network directories/name servers) • protect sensitive information stored on systems and transmitted to external party locations (e.g. using encryption).	SOGP – NC1.4 NIST CSF - PR.AC.7 NIST CSF - PR.PT.4 SOGP – IR2.3	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures. Design documentation is in place with appropriate security controls addressed.
4.3	Systems and networks accessible by external connections must be protected by methods of: • restricting external network traffic to only specified parts of systems and networks • limiting connections to defined entry points (e.g. specific network gateways) • verifying the source of external connections (e.g. by checking	SOGP – NC1.4 NIST CSF - PR.AC.7 NIST CSF - PR.PT.4 SOGP – IR2.3	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	the source IP address or using Calling Line Identification (CLI)) • logging security-related activity (e.g. unsuccessful login attempts of authorised users and unsuccessful changes to access privileges for applications and resources) • recording details relating to external connections established (e.g. the internet, ISDN, VPN and dial-up) • identifying possible security policy violations (e.g. attempts from unauthorised external networks to communicate directly with internal systems) • temporarily isolating critical subnetworks if the network is under attack.		
4.4	Access to systems and networks must be restricted to devices that meet minimum security configuration requirements, which includes verifying that devices: • have been authorised • are running up-to-date malware protection • have the latest operating systems and software patches installed • are connecting over an 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 • do not allow end users to disable the device's personal	SOGP – SA1.1 NIST CSF - PR.AC.1 SOGP – IR2.3	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	firewall or alter its configuration.		
4.5	Untrusted devices - those that do not meet minimum security configuration requirements (i.e. fail a system integrity check) - must be automatically connected to an isolated network (e.g. a quarantine area such as a sandbox or container) where their configuration can be updated but no other changes are allowed.	SOGP – PA1.2 SOGP – NC1.1 NIST CSF - PR.IP.1	Evidence of configuration polices which will enforce a secure baseline for devices. Defined zero trust architecture. Defined conditional access policies based on the build of a secure baseline for devices.
4.6	External access to systems and networks (e.g. via internet connections) must be restricted and consideration given to the following technical controls: • establishing demilitarised zones (DMZs) between internal networks and untrusted networks (e.g. the internet) • routing network traffic through firewalls (e.g. stateful inspection firewalls (typically located in the perimeter of a network) or proxy firewalls (typically located between internal networks)) • limiting the methods of connection • using location-aware technologies to validate connections based on known equipment locations • granting access only to specific business applications, systems or specified parts of the network (e.g. domains).	SOGP – NC1.4 SOGP – NC1.5 SOGP – TS1.1 NIST CSF - PR.AC.5 NIST CSF - DE.CM.1 SOGP – IR2.3	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
4.7	External access must be provided using a dedicated remote access server, which: • provides reliable and complete authentication for external connections (e.g. by running an authentication system such as Radius or TACACS+) • provides information for troubleshooting (e.g. router and firewall logs) • logs all connections and sessions, including details of call start/stop time, call duration and user tracking • helps identify possible information security breaches (e.g. by logging events such as connections and terminations in a database and collating them centrally).	SOGP – IR2.3 NIST CSF - ID.RA.3 SOGP – NC1.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
4.8	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).	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented designs, policies and procedures.
4.9	Unauthorised external connections must be identified (e.g. for investigation or possible removal) by: • performing manual audits of network equipment and documentation to identify discrepancies with records of known external connections • employing computer and network management and diagnostic tools (e.g. port probes and network discovery/mapping tools)	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures. Implementation of IDS, SIEM, Endpoint Security, Network monitoring tools and Network Access Control (NAC)

Reference	Minimum requirement	Control reference	Compliance Metric
	• analysing network traffic to detect unauthorised or unusual activity • checking accounting records of bills paid to telecommunications suppliers and reconciling them against known connections.		Monitoring of audit logs and accounts is being carried out.
4.10	External access must be prevented if unauthorised (or when no longer required) by removing or disabling: • computer and network connections (e.g. by physically removing a network connection, modifying firewall rules, updating access control lists and configuring routing tables on network routers) • equipment (e.g. redundant modems and communications lines) • control settings (e.g. software configuration settings).	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures. Implementation of IDS, SIEM, Endpoint Security, Network monitoring tools and Network Access Control (NAC)
4.11	The organisation must ensure the availability of access to managed services (e.g. cloud services) by: • investing in robust, reliable internet connectivity • establishing multiple methods of connection (e.g. wired networks, wireless, 4G/LTE (long-term evolution) and 5G) • providing required network bandwidth between the organisation's network and the	SOGP – SY1.1 NIST CSF - PR.DS.4	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures. Service level agreements are in place with commitments to bandwidth and availability metrics that are being monitored.

Reference	Minimum requirement	Control reference	Compliance Metric
	managed service provider (i.e. to avoid poor network latency) • maintaining links with the organisation's legacy systems.		
5. Firewalls			
5.1	Networks must be protected from malicious traffic on other networks or sub-networks (internal or external) by one or more firewalls.	SOGP – NC1.5 NIST CSF - PR.AC.5	SbD process, Threat and Risk Assessments, Security Architect views
5.2	There must be documented standards/procedures for managing firewalls (or similar devices capable of filtering network traffic, such as switches and routers), which cover: • filtering of specific types or sources of network traffic (e.g. IP addresses, TCP ports or information about the state of communications and users) • blocking or otherwise restricting particular types or sources of network traffic • developing predefined rules (or tables) for filtering network traffic • protecting firewalls against attack or failure (e.g. by restricting access to only authorised individuals)	SOGP – NC1.5 NIST CSF - PR.AC.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	• limiting the disclosure of information about networks and network devices • applying security architecture principles during configuration • documenting and regularly reviewing firewall rules (e.g. monthly).		
5.3	Firewalls must filter network traffic based on: • source and destination addresses (e.g. IP addresses) and ports (e.g. TCP ports) • information about the state of associated communications (e.g. saving the outgoing port command of an FTP session so that an associated, incoming FTP communication can be checked against it) • information about the state of users (e.g. permitting access to users only where they have been authenticated in a previous communication) • the validity of a network service (e.g. by using an application proxy firewall).	SOGP – NC1.5 NIST CSF - PR.AC.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
5.4	Firewall configuration must incorporate security architecture principles (e.g. 'secure by design', 'defence in depth', 'secure by default', 'default deny', 'fail secure', 'secure in deployment' and 'usability and manageability').	SOGP – NC1.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
5.5	Firewalls must be configured to: • protect communication protocols that are prone to	SOGP – NC1.5 SOGP – BA1.2	Evidence that security controls have been implemented through an ITHC and appropriate

Reference	Minimum requirement	Control reference	Compliance Metric
	abuse (e.g. HTTPS, SSH, SMTP, DNS and UUCP) • block network packets typically used to execute denial of service attacks (e.g. ICMP Echo, UDP and TCP Echo, Chargen and Discard) • deny incoming traffic where the source address is known to have been spoofed (e.g. where the source address claims to be from the destination network) • deny outgoing traffic where the source address is known to have been spoofed (e.g. where the source address does not reflect the network from which it originates) • limit the disclosure of information about networks at the network level by using IP masquerading (i.e. network address translation (NAT) or port address translation (PAT)).	CISv8 – 13.1	documented policies and procedures.
5.6	Specialised firewalls must be used to protect critical networks and systems by: • performing deep packet inspection on network traffic between IP-enabled components, to help detect sophisticated attacks • processing and interpreting a wide range of proprietary or imprecisely defined network protocols (e.g. MODBUS, PROFIBUS, DNP3 and CIP) • handling protocol-specific rules, to help defeat attacks against protocol vulnerabilities.	SOGP – NC1.5 NIST CSF - PR.AC.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures..

Reference	Minimum requirement	Control reference	Compliance Metric
1.5.7	Firewalls must be configured to block or otherwise restrict communications based on specified source/destination: • addresses (e.g. a particular IP address) • ports (e.g. ports 20 and 21 for FTP and port 22 for SSH).	SOGP – NC1.5 NIST CSF - PR.AC.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
5.8	Filtering of network traffic must be based on predefined rules (or tables) that: • have been developed by trusted individuals, and are subjected to supervisory review • specifically enforce the principle of 'default deny' (e.g. by including a DENY-ALL rule (or equivalent) that applies after all other rules have been processed) • use clear, consistent naming conventions (e.g. host_name, IP_address or network_IP_range) • are grouped into sets of rules to help manage and understand long rule sections • are documented (with version control) and kept up to date • take account of the information security policy, network standards/procedures and user requirements.	SOGP – NC1.5 NIST CSF - PR.AC.5 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
5.9	Before new or changed rules are applied to firewalls, their strength and correctness must be tested, verified and signed off by the network owner.	SOGP – NC1.4 NIST CSF - PR.AC.7	Post Go-Live activity convene a CAB (Change Approval Board) where changes are validated for correctness and strength.

Reference	Minimum requirement	Control reference	Compliance Metric
			Defined in-house testing regime for firewall review based on change. Annual ITHC with firewall review, as a baseline for secure firewall posture.
5.10	Firewalls must be protected against attack by: • restricting administrator access to a limited number of authorised, skilled individuals, such as firewall administrators (e.g. by using strict access control mechanisms and strong authentication) • limiting administrator access to dedicated accounts that are only used for managing firewalls • encrypting administrator access (e.g. by using secure management consoles, secure remote login shells such as SSH or encrypted connections using TLS, IPsec or equivalent) • restricting administrator access to a central point (e.g. in a Network Operations Centre (NOC) using a minimum number of firewall management consoles) • preventing information about them (e.g. the manufacturer and model of the firewall, and the version numbers of the operating system and security software) from being disclosed on the network.	SOGP – NC1.4 SOGP – NC1.5 NIST CSF - PR.AC.5 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
5.11	Firewall configurations must be documented (e.g. in a configuration	SOGP – NC1.4	Evidence that security controls have been

Reference	Minimum requirement	Control reference	Compliance Metric
	management database (CMDB) or equivalent), and include justification for: • allowing standard services, protocols and ports that are permitted to pass through the firewall (e.g. HTTP (80), HTTPS (443) and SSH (22)) • prohibiting services, protocols and ports that are inherently susceptible to abuse (e.g. SQL Server (1433), FTP (21), NetBIOS (139), RPC (593), Telnet (23), POP3 (110), IMAP (143), PPTP (1723) and SNMP (161)).	SOGP – NC1.5 NIST CSF - PR.AC.5 NIST CSF - PR.AC.7	implemented through an ITHC and appropriate documented policies and procedures.
5.12	Firewall configurations must be reviewed on a regular basis (e.g. quarterly) to ensure that: • each firewall rule is approved and signed off by a business owner • expired or unnecessary rules are removed • conflicting rules are resolved • unused/duplicate objects (e.g. networks or systems) are removed • system administrators responsible for firewall management are aware of the current configurations, security policies, and operational procedures.	SOGP – NC1.4 SOGP – NC1.5 NIST CSF - PR.AC.5 NIST CSF - PR.AC.7	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
6. Remote Maintenance			
6.1	Access to critical systems and networks by external individuals for remote maintenance purposes (e.g. remote diagnosis/testing, software maintenance) must be managed by:	SOGP – PM1.5 NIST CSF - PR.AC.3 NIST CSF - PR.AT.5	Evidence that security controls have been implemented through an ITHC and appropriate

Reference	Minimum requirement	Control reference	Compliance Metric
	• restricting access to a limited number of authorised maintenance engineers • defining and agreeing the objectives and scope of planned work • authorising sessions individually • restricting access rights so that they do not exceed those required to meet the objectives and scope of planned work • logging all activity undertaken • requiring the use of unique authentication credentials for each implementation (rather than vendor default credentials) • requiring that access credentials be assigned to individuals, rather than shared • requiring the use of multi-factor authentication (MFA) and VPN for access • revoking access privileges and changing passwords immediately after agreed maintenance is complete • performing an independent review of remote maintenance activity.		documented policies and procedures. Monitoring is taking place of all access to systems through audit logs and account activity reviews.
6.2	Diagnostic ports on network equipment must be protected by access controls (e.g. passwords/passphrases and physical locks).	SOGP – SA1.2 SOGP – SA1.3 NIST CSF - PR.AC.1	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.
6.3	Non-disclosure agreement(s)/confidentiality clause(s) must be signed by external suppliers' IT and information security staff or incorporated into their employment	SOGP – PM1.2 NIST CSF - PR.AT.1	Evidence that a supplier assurance process has taken place and that appropriate security clauses are embedded

Reference	Minimum requirement	Control reference	Compliance Metric
	contracts prior to being granted access to the organisation's applications, systems or networks.		within any contractual arrangements
6.4	Maintenance of systems and networks, performed using remote control software (e.g. using Virtual Network Computing (VNC)), must be strictly managed by: • restricting access to only authorised maintenance engineers • authorising connectivity before access is granted • limiting the number of concurrent remote connections (e.g. only one at any time) • verifying the source of the remote connection (e.g. by confirming the MAC address of the remote system) • requiring a request for connection from the remote location, which can only be granted by the target system (e.g. a dedicated console or administrator desktop computer) • monitoring activities performed throughout the duration of the connection • disabling the connection as soon as the authorised activity is complete.	SOGP – PM1.5 NIST CSF - PR.AT.5	Evidence that security controls have been implemented through an ITHC and appropriate documented policies and procedures.

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.

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 policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)