CYBER STANDARDS DOCUMENT

NCSP Electronic Communications standard

ABSTRACT:
This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running electronic communications services within national policing systems. This standard details a minimum set of security requirements and controls that must be met to ensure security of electronic communications services. Consideration is given to the following areas of configuration, email systems, collaboration platforms and voice communications platforms.

ISSUED	February 2025
PLANNED REVIEW DATE	February 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 networks and communications security.

Introduction

This Electronic Communication 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 that is 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 and local policing systems.

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 IT services and managing vulnerabilities within National Policing Systems. This standard sets out the requirement to identify and address technical vulnerabilities in a timely and effective manner to reduce exposure to the risk of them being exploited, thereby reducing the risk of serious security breaches.
This standard helps organisations demonstrate compliance with the following NPCSP policy statements:

Electronic Communications

- Protect electronic communication systems (e.g. email, collaboration platforms and voice communication platforms) by setting policy for their use; configuring security settings; and hardening the supporting technical infrastructure.

Secondly, this standard provides a means to conduct compliance based technical security audits.

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 PDS or policing.
- Auditors and penetration testers providing assurance services to PDS or 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 electronic communications systems that are provisioned for the policing community of trust use.

3. This standard is applicable for all electronic communications systems used within the police community of trust including both physical and virtual environments.

Requirements

The following sections details the minimum requirements for ensuring the secure and efficient management and operation of electronic communications systems for National Policing IT Systems.

Consideration is given to the following areas: -

- Email communications
- Collaboration platforms
- Voice communication platforms
- Other electronic communications

Reference	Minimum requirement	Control reference	Compliance Metric
1. Email			
1.1	There must be documented standards/procedures for the provision and use of email, which should include: • methods of configuring mail servers (e.g. to limit the size of messages or user mailboxes) • scanning email messages (e.g. for malware, phishing, chain letters or offensive content) • enhancing the security of email messages (e.g. by the use of disclaimers, hashing, encryption and non-repudiation techniques) • guidelines for business and personal use (e.g. prohibition of personal use) • the types of email service permitted (e.g. corporate services such as Microsoft Exchange, Google Gmail or IBM Notes) • user guidelines for acceptable use (e.g. prohibition of the use of offensive statements) • details of any monitoring activities to be performed (e.g. scanning the content of messages and attachments) to detect malicious activity and accidental leakage of information. • Historical logging and storage of email messages for auditing and investigation purposes.	SOGP – NC2.1 **UA1.1**	Evidence of the SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence of procedural and standards documentation. Where risks are identified documented evidence of risk mitigations.

Reference	Minimum requirement	Control reference	Compliance Metric
	• Retention of logs and email must be in line with Police Information And Records Management: Code of Practice		
1.2	Email servers (or gateways) must be configured to: • prevent the messaging system from being overloaded (e.g. by limiting the size of messages and user mailboxes, and automatically identifying and cancelling email loops) • reduce the accidental disclosure of email and attachments to unauthorised individuals by enforcing encryption between email servers (e.g. using Transport Layer Security (TLS) or equivalent). Use MTA-STS to enforce this, and use TLS-RPT to monitor it. • block unnecessary file types such as executables (e.g. .exe, .js or .vbs) • deploy malware protection techniques (e.g. attachment scanning and/or sandboxing). • ALL services permitted to send emails from official domain names must be assessed and managed, and must use DMARC with DKIM signatures and SPF. • For all domains used by the organisation DMARC reporting must be enabled and reports must be monitored for legitimate service misconfiguration and malicious email spoofing.	SOGP – NC2.1 **UA1.1**	Evidence of tested configuration document sets. Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based on Threat and risk assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Reporting from NCSC MailCheck tools demonstrating secure configuration.

Reference	Minimum requirement	Control reference	Compliance Metric
1.3	Email client applications must be configured to prevent the accidental disclosure of email and attachments to unauthorised individuals by: • preventing users from configuring the auto-forward feature and using auto-complete in email address fields • restricting the use of large distribution lists (e.g. a list containing every individual in the organisation) • presenting users with a warning before they are able to use the reply all feature to a large number of recipients.	SOGP – NC2.1 **UA1.1**	Evidence of tested configuration document sets. Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based on Threat and risk assessments. Evidence that identified risks have been mitigated with technical and procedural security controls.
1.4	Email systems must be reviewed to ensure that requirements for up-time and future availability can be met.	SOGP – NC2.1 **UA1.1**	Evidence of documented requirements for the solution, during the SbD process. Configuration documentation HLD (business-level) and a traceability matrix that maps the

Reference	Minimum requirement	Control reference	Compliance Metric
			requirements to the design. Evidence of uptime and availability monitoring.
1.5	Email messages must be scanned for: • attachments that could contain malicious code (e.g. malicious code hidden in self-extracting zip files, Adobe PDF documents or embedded macros) • prohibited words or phrases (e.g. those that are racist, offensive, libellous or obscene) • phrases associated with malware (e.g. those commonly used in phishing, hoax viruses or chain letters).	SOGP – NC2.1 **UA1.1**	Evidence that identified risks have been mitigated with technical and procedural security controls where applicable. Evidence of SbD process used to assess the threat and risk. Evidence that scanning logs are routinely checked and remediation taken when threats are detected.
1.6	Email systems must protect messages by: • blocking messages that are considered undesirable (e.g. by using an email denylist consisting of known undesirable websites or mailing list servers) • using digital signatures to identify if email messages have been modified in transit and encrypting email messages	SOGP – NC2.1 **UA1.1**	Evidence of a SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture.

Reference	Minimum requirement	Control reference	Compliance Metric
	• ensuring non-repudiation of origin of important email messages (e.g. by using digital signatures) • providing non-repudiation of receipt of important messages (e.g. by returning a digitally signed receipt message) • verifying the source IP address of senders' emails (e.g. using an email validation system such as Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) or Sender ID that checks the Domain Name System (DNS)) to limit spoofing. • analysing the reputation score of the sender's Mail Transfer Agent (MTA).		Evidence of threat modelling and business impact assessments. Evidence that email systems have been functionally and penetration tested as part of regular IT Health checks.
1.7	The business integrity of email messages must be protected by: • appending legally required information and return address details (for misdelivered email) to business email (e.g. as a disclaimer) • warning users that the contents of email messages may be legally and contractually binding and that the use of email may be monitored.	SOGP – NC2.1 **UA1.1**	Evidence of legal notices and warnings approved by HR, Security and Legal teams in line with data protection policies.
1.8	The organisation must prohibit: • automatic email diversion to external to Police.uk email addresses. (If this is absolutely necessary then it must be subject to governance with an exception process in place and reviewed at least every six months to	SOGP – NC2.1 **UA1.1**	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from

Reference	Minimum requirement	Control reference	Compliance Metric
	prevent permanent diverts. Automatic replies is always a better option) • unauthorised private encryption of email or attachments. • the opening of attachments from unknown or untrusted sources.		defined security architecture. Based on Threat and risk assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence that the controls have been tested.
1.9	Personal use of business email must be clearly labelled as personal and subject to the terms of a user agreement.	SOGP – NC2.1 **UA1.1**	Evidence of an acceptable use policy for email. Approved by HR, Security and Legal teams, in line with data protection policies.
1.10	Users must be educated in how to protect the confidentiality and integrity of email messages (e.g. checking for external recipients, checking full email history for confidential information when forwarding, Care when replying to all in an email with multiple to or cc lists, checking attachments are correct before sending etc.).	SOGP – NC2.1 **UA1.1**	Evidence of eLearning or training materials delivered to users. Metrics showing uptake of eLearning materials and evidence of process to deal

Reference	Minimum requirement	Control reference	Compliance Metric
			with lack of completion.
2. Collaboration Platforms and import / export to external systems			
2.1	The use of collaboration platforms must be signed off by an appropriate business manager usually the Information Asset Owner (IAO.) • The use of collaboration platforms or import / export of data must be supported by lawful business needs. • Data privacy impact assessments (DPIA) must be undertaken where Personally Identifiable Information (PII) or other sensitive data is affected.	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of a formal change control process including business representatives (IAOs.) Documented business needs DPIAs conducted and signed off by appropriate authorities.
2.2	There must be documented standards/procedures for collaboration platforms, which include: • configuring their security settings • providing assurance over the content handled by collaboration platforms • improving the security of technical infrastructure supporting collaboration platforms (e.g. managed internally or provided as part of a managed service) • protecting conferencing services (e.g. teleconferencing, videoconferencing and online web-based conferencing) against unauthorised access.	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based on Threat and risk assessments. Evidence that identified risks have been mitigated with technical and

Reference	Minimum requirement	Control reference	Compliance Metric
	• Logging of collaboration activity for auditing and investigation purposes. • Retention of logs must be in line with the Police Information and Records Management: Code of Practice.		procedural security controls. Evidence of tested configurations. Evidence of monitoring of logs.
2.3	The security of collaboration platforms must be improved by: • only permitting the acquisition and use of approved platforms • assessing the information risks of each platform being acquired or in use • adding, updating and deleting user profiles (e.g. following recruitment of new staff or changes to their job role) • making users aware of how to use these platforms securely (e.g. through an acceptable use policy for employees or a code of conduct for external users). • Application of the NCSC Pattern: Safely Importing Data	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence of training and awareness to users.

Reference	Minimum requirement	Control reference	Compliance Metric
2.4	Collaboration platforms must be configured to operate securely by: • requiring authentication before users are granted access to platforms • disabling unauthorised features (e.g. message transcripts, externally facing APIs or user self-registration) • protecting the integrity of messages (e.g. by the use of digital signatures) • logging specified security-related events (e.g. to check for unauthorised activity, investigate potential breaches and maintain records for regulatory purposes).	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based on Threat and risk assessments. Evidence that identified risks have been mitigated with technical and procedural security controls.
2.5	Assurance must be provided over the integrity and confidentiality of content handled by collaboration platforms by: • using content management techniques (e.g. information classification, data validation, timestamping and content filtering) • appointing one or more content managers to maintain and monitor content	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and

Reference	Minimum requirement	Control reference	Compliance Metric
	• scanning content, including attachments or uploaded content, to detect malicious activity or accidental leakage of information.		business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence of scanning logs and remediation.
2.6	The security of collaboration platform infrastructure must be improved by: • employing a standard configuration for each platform • hardening collaboration platform servers (e.g. by locking down the operating system and application) • configuring firewalls to block the use of unauthorised collaboration platforms (e.g. by blocking known ports).	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls.

Reference	Minimum requirement	Control reference	Compliance Metric
			Evidence of configuration documentation detailing hardening that has been implemented.
2.7	Conferencing services (e.g. teleconferencing, videoconferencing and online web-based conferencing) must be protected against unauthorised access by: • requiring authentication before users are granted access to a conference • providing a unique password for each new conference session (i.e. not repeating the same password for consecutive conference sessions) • maintaining a record of who joins and leaves a conference session • ensuring hardware (e.g. screens and cameras), software (e.g. presentation, screen sharing and remote takeover applications) and network connections are disabled or closed once a conference session has ended.	SOGP – UA1.2 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence that conferencing logs are being reviewed and acted upon.

Reference	Minimum requirement	Control reference	Compliance Metric
3. Voice Communication Services			
3.1	Voice communication services must be reviewed and subject to sign-off by an appropriate business manager or network administrator.	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based on Threat and risk assessments. Evidence of a formal change control process including business representatives.
3.2	There must be documented standards/procedures for voice communication services and underlying technical infrastructure, which include: • use of the organisation's voice communication services • registration and authentication of users with access to voice communication services • general network controls for voice communication services (e.g. deploying monitoring tools, providing resilience and redundancy, installing firewalls and preventing the use of unauthorised devices)	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks

Reference	Minimum requirement	Control reference	Compliance Metric
	• technology-specific controls (e.g. separating voice traffic from general network traffic, hardening devices, identifying vulnerabilities, encrypting sensitive voice traffic, and monitoring voice-related event logs) • protection of voicemail systems against unauthorised access (e.g. using password protection).		have been mitigated with technical and procedural security controls. Evidence that logs are being monitored for abnormal activity.
3.3	Network security controls for voice communication services must be applied, which include: • monitoring bandwidth using tools that are capable of recognising voice traffic • deploying network components to provide resilience and redundancy • installing firewalls that can filter voice traffic • restricting traffic sent over voice communication networks to authorised software and devices (e.g. IP phones, IP PBXs and virtual telephone applications).	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence that monitoring is taking place.

Reference	Minimum requirement	Control reference	Compliance Metric
3.4	Technology-specific controls must be applied, which include: • separating voice traffic using virtual local area networks (VLANs) • hardening voice communication devices (e.g. IP phones, routers and IP PBXs) • scanning voice communication networks for vulnerabilities (e.g. open network ports or non-secured administration consoles) • encrypting voice network traffic • analysing voice-related event log files.	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence that penetration tests have taken place and remediation actions are in place.
3.5	Access to voicemail must be restricted to authorised users by using a password/passphrase, PIN or equivalent of sufficient complexity.	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of an access control policy including details of the requirements for voicemail, based on the outputs from the SbD

Reference	Minimum requirement	Control reference	Compliance Metric
			(Secure-by-design) process, for technical and procedural risk mitigation. Evidence of penetration testing.
3.6	The administrative functions and technical infrastructure associated with voice communication services must be protected by: • restricting administrative access to a limited number of authorised individuals • segregating administrative roles (e.g. creation of new lines, implementation of call forwarding and provision of voicemail access) • monitoring the activity of administrative accounts.	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Evidence of threat modelling and business impact assessments. Evidence that identified risks have been mitigated with technical and procedural security controls. Evidence that penetration testing has taken place.

Reference	Minimum requirement	Control reference	Compliance Metric
3.7	Changes to the configuration of settings for voice communication services (e.g. extension number changes, voicemail password resets and call redirection) must be performed by a minimum number of authorised, competent individuals.	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of a formal change control process including business representatives.
3.8	A method of reviewing voice communication services must be established, which includes: • monitoring use of voice communication services to determine adequate capacity and operator workloads/staffing requirements • inspecting bills/invoices for voice communication services to identify unusual patterns (e.g. security breaches, suspicious behaviour or fraud). • Keeping logs of all voice communications for auditing and investigation purposes. • Retention of logs must be in line with the Police Information and Records Management: Code of Practice. • Retention of Voicemails in line with Police Information and Records Management: Code of Practice	SOGP – NC1.4 NIST CSF - PR.AC.7	Evidence of voice communication lifecycle management that identifies the requirements to manage the monitoring and cost of the service, this can be integrated in to current processes, or new processes created if current processes are deemed not appropriate on review.

4. Other Electronic Communications Services

This section deals with general requirements for any other electronic communications services that might be used that don’t fall into the categories of collaboration, email and voice communications.

Reference	Minimum requirement	Control reference	Compliance Metric
4.1	Communications must be protected while at rest and in transit using encryption.	SOGP – IM1.2.5	Evidence of threat modelling and

Reference	Minimum requirement	Control reference	Compliance Metric
	See also: Cryptography standard	and IM1.2.6 NIST CSF - PR.AC.7	business impact assessments. Evidence that systems have undergone penetration tests as part of regular IT Health checks and remediation plans have been documented and implemented.
4.2	A log of communications must be stored to allow auditing and investigation. Logs and audit data must be retained in line with POLICE INFORMATION AND RECORDS MANAGEMENT: CODE OF PRACTICE guidance.	SOGP – SE1.1 NIST CSF - PR.AC.7	Evidence that logs are being stored and are accessible for investigation purposes. Evidence that processes and procedures are in place to recover information from logs.
4.3	Use of other communications services must be reviewed and approved by an appropriate business manager or supervisor.	SOGP – AC1 NIST CSF - PR.AC.7	Evidence of SbD (Secure-by-design) process starting at project initiation and incorporating design blueprints and architectural principles, from defined security architecture. Based

Reference	Minimum requirement	Control reference	Compliance Metric
			on Threat and risk assessments. Evidence of a formal change control process including business representatives.
4.4	Guidance, processes and procedures must be in place to ensure electronic communications are used in line with data protection policies.	SOGP – SG1.1	Evidence of procedural and standards documentation. Where risks are identified documented evidence of risk mitigations.
4.5	Mechanisms must be in place to ensure the authenticity of electronic communications and prevent spoofing, hijacking or "man in the middle" threats.	SOGP – AC1 NIST CSF - PR.AC.7	Evidence of an access control policy including details of the requirements for voicemail, based on the outputs from the SbD (Secure-by-design) process, for technical and procedural risk mitigation.
4.6	Use of any electronic communications systems must be limited to those who have been authorised.	SOGP – AC1	Evidence of an access control policy including details of the

Reference	Minimum requirement	Control reference	Compliance Metric
		NIST CSF - PR.AC.7	requirements for voicemail, based on the outputs from the SbD (Secure-by-design) process, for technical and procedural risk mitigation.
4.7	Identity and access management must be in place to prevent unauthorised use of electronic communications.	SOGP – AC1 NIST CSF - PR.AC.7	Evidence of an access control policy including details of the requirements for voicemail, based on the outputs from the SbD (Secure-by-design) process, for technical and procedural risk mitigation.

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.

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

(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
0.1	PDS Cyber	Initial version	18/12/23
0.2	PDS Cyber	Updates following peer review	09/02/24
1.1	PDS Cyber	Annual review	06/01/25

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	23/05/24
1.1	NCPSB	National Cyber Policy & Standards Board	27/03/25

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
NCSC Pattern – Safely importing data	Web Page	07/2018
Set up government email services securely - GOV.UK (www.gov.uk)	Web Page	04/2024
Email security standards MTA-STS and TLS-RPT - UK Government Security	Web Page	04/2024
Police Information and Records Management: Code of Practice	Web Page	Published 20 July 2023