CYBER STANDARDS DOCUMENT

NCSP Security Management

ABSTRACT:

This standard describes the requirements to implement and maintain an effective cyber security management system, as required by the National Community Security Policy Framework.

Implementation of this standard will help members mature their cyber resilience through the application of adequate management controls and oversight.

ISSUED	August 2025
PLANNED REVIEW DATE	August 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 Standard describes the requirements to fulfil the National Community Security Policy (NCSP) Security Management Policy statement. By implementing this standard, members of the policing Community of Trust will be able to demonstrate an effective governance framework, and a clear commitment to information security and risk management.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

Security Management

- *Develop a comprehensive, approved information security policy, and reinforce it through other security-related local policies, such as an acceptable use policy, (each of which should be supported by more detailed standards, controls, and procedures) and communicate them to all individuals with access to policing's information and systems.*
- *Establish a specialist information security function(s), led by a sufficiently senior manager (e.g. a Chief Information Security Officer or equivalent), which is assigned adequate authority and resources to run information security-related projects; promote information security throughout policing (nationally or locally); and manage the implications of relevant laws, regulations and contracts. Define the roles and responsibilities of the wider security workforce, including operational security responsibilities.*
- *Security management reporting should be in place to enable the organisational leadership to take informed risk management decisions.*

Audience

This standard is aimed at:

- Member Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs), Information Security Officers (ISOs), and information security practitioners.
- Third parties who act as service providers or suppliers to members.
- Auditors providing cyber and information assurance services to members.

Scope

This standard applies to any member of the policing Community of Trust. It is also applicable to third parties to the policing Community of Trust.

Requirements

This section details the minimum requirements to implement an effective cyber security management structure to assure policing systems and information.

Reference	Minimum requirement	Control reference	Compliance Metric
1. Develop the Security Policy Framework	Members of the policing Community of Trust must adopt and ensure adherence to the NCSP. Ensure that appropriate policy, procedure, or standards that cover all the NCSP statements are in place and are adhered to. Any local risk-based decisions to deviate shall be subject to risk governance and be documented and reviewed commensurate to risk level. See the **National Information Security Risk Management Framework** for more information. All documents must have a regular review and approval cycle, with updates communicated to the organisation where required.	**NIST CSF:** ID.GV-1 **NIST CSF 2:** GV.PO-01, GV.PO-02 **ISO 27002:2022:** 5.1 **ISF SOGP:** SM1.1, SM1.2, SM2.1, SM2.2, SM2.3, SG1.1	*Current, maintained policies, distributed and easily accessible to all personnel, including visitors and contractors.* *Organisational resource, responsibility, governance and process for managing the creation, review, and changes to policy and procedures.* *Alignment of policy and procedure to the NCSP statements.*
2. Define Senior Information Security Leadership Roles & Responsibilities	Appoint a suitably senior role as force SIRO (or equivalent) to provide executive level accountability for information risks. • Implement the College of Policing SIRO role profile. • Ensure appropriate and adequate training is provided.	**NIST:** ID.GV-2, ID.GV-3, PR.AT-1, PR.AT-5 **NIST CSF 2:** GV.RR-01, GV.RR-02, GV.RR-03, GV.RR-04,	*Named SIRO (or equivalent role) in organisation.* *SIRO (or similar) responsibilities and activity within organisation aligns to College of Policing APP and Handbook.*

Reference	Minimum requirement	Control reference	Compliance Metric
	The SIRO must provide Senior leadership commitment to the NCSP and promote its associated standards for implementation and adherence throughout the organisation. This will include ensuring that adequate resources are available to deliver and manage the information security programme. Ensuring that a suitable information security management training development plan is in place and operating across the organisation. The SIRO chairs / has oversight of organisation's information risk governance board (or similarly named organisational management-level governance group). **See also:** • Security Governance Standard • People Security Management Standard • Cyber Incident Management Standard • College of Policing Information Management Authorised Professional Practice (APP) • College of Policing SIRO Handbook • National Information Security Risk Management Framework	GV.OC-02, GV.OC-03, PR.AT-01, PR.AT-02 **ISO 27002:2022:** 5.2, 5.4, 5.24, 5.25, 5.26, 5.27, 5.31, 5.36, 6.3, 6.4 **ISF SOGP:** SM2.1, SM2.2, SM2.3, SM2.4, SM2.5, SM2.6, SM2.7, SG1.2	*Records of board meeting minutes.* *Training records held against personnel records. Details of training curriculum.* *Organisation represented at regional SIRO meetings / National SIRO conference events and Boards.*

Reference	Minimum requirement	Control reference	Compliance Metric
3. Establish Information Asset Owners	Appoint IAOs for organisational information assets. IAOs may be supplemented with Platform Asset Owners (PAOs), who hold the responsibility for risks associated with the underlying platform(s). • Implement the College of Policing role profile. • Ensure appropriate and adequate training is provided. • Provide management reporting regime to the SIRO. The organisation's information, physical devices and systems must be inventoried. Refer to the **Physical Asset Management Standard** for further information. The Information Asset Register must formally register and record the link between the organisation's Information Assets and designated IAOs. **See also:** • National Information Security Risk Management Framework • Physical Asset Management Standard • Information Management Standard • College of Policing Information Management APP	**NIST:** ID.AM-1, PR.AT-2, PR.DS-3 **NIST CSF 2:** GV.RM-06, ID.AM-02, ID.AM-04, ID.AM-05, ID.AM-07 **ISO 27002:2022** 5.2, 5.9, 5.10, 5.31, 5.32, 5.33, 5.36, 8.19 **ISF SOGP:** AM1.2	*Job Description and Role Profile available.* *IAO (or similar) responsibilities and activity within organisation aligns to College of Policing APP and IAO Handbook.* *Training records held against personnel records. Details of training curriculum.* *Information Asset Register created and maintained, including regular review cycle for all assets.* *Information Assets formally registered and recorded against IAOs.* *Management reports, meeting minutes, or other evidence of information governance flows between IAOs and SIRO.*

Reference	Minimum requirement	Control reference	Compliance Metric
4. Establish Specialist Information Security Function(s)	Appoint Suitably Qualified Experienced Professional/s (e.g., ISO), who will be responsible for the implementation and day-to-day running of the information security function. Define and implement a role profile or job description detailing the required responsibilities to: • Provide adequate authority to run information security-related projects. • Lead security specific roles (e.g., ITSO, Security Operations staff, and other IT security professionals). • Ensure the responsibility for compliance with laws and regulations affecting information security. • Prioritise information security controls to ensure that they address organisational risk needs. • Ensure information security obligations associated with legislation, regulations, contracts, industry standards and organisational policies are met. • Ensure that the compliance requirements of the National Policing Community Security Policy and other national policing requirements are met. • Deliver management reporting upwards (to SIRO/equivalent and via external reporting frameworks).	**NIST:** ID.GV-2, ID.GV-3, PR.AT-1, PR.AT-5 **NIST CSF 2:** GV.RR-02, GV.RR-03, PR.AT-01, PR.AT-02 **ISO 27002:2022:** 5.2, 5.3, 5.5, 5.6, 6.4, 6.8, 7.1, 7.2, 7.3, 7.4, 7.7, 7.8, 7.9 **ISF SOGP:** SM1.1, SM1.4, SM2.2, SM2.3, SM2.5, SM2.6	*Role(s) identified within organisation structure.* *Job Description and Role Profile available, supported by appropriate Professional Development Plan.* *Maintained Security Assessment for Policing (SyAP) evidence.* *Timely responses to compliance requests.* *There is documented responsibility within the organisation for defining and implementing the Information Security strategy.* *Security roles within the organisation operate within a clear structure for governance, reporting, and escalation. Conflicts of interest are minimised, and individuals are positioned to provide transparent*

Reference	Minimum requirement	Control reference	Compliance Metric
	• Provide expert advice in response to information security incidents. • Promote a culture of information security awareness, with appropriate senior management support, that allows for decision making to be risk-based, informed by the National Community Security Policy and its associated Standards. • Undertake cyber risk assessments and make recommendations for risk management controls. • Promote information security throughout policing (nationally or locally). **See also:** • Security Governance Standard • People Security Management Standard • Cyber Incident Management Standard • Physical & Environmental Management Standard • Business Continuity Standard • College of Policing Information Management APP • National Information Security Risk Management Framework		*reporting and escalation.* *Laws, regulations, and best practice are documented within responsibilities to remove ambiguity.* *Board minutes, showing attendance, actions, decisions, and updates.* *Details of security awareness campaigns (e.g., posters, Intranet, emails, and training events).*

Reference	Minimum requirement	Control reference	Compliance Metric
5. Establish an Information Risk Governance forum	In support of the **National Information Security Risk Management Framework**, establish a management forum chaired by the SIRO to ensure regular management reviews of the performance of cyber risk management. This forum shall provide direction and oversight on behalf of the senior leadership and overall organisational risk management framework. The forum will help ensure that security activities are properly performed unilaterally to reduce information risk within agreed risk appetite. The forum can review progress against the cyber security programme, arbitrate risk escalations, consider security incident trends, instigate organisational security initiatives and audits. **See also:** • National Police Information Security Risk Management Framework	**NIST CSF** ID.GV-4, ID.RM-1 **NIST CSF 2:** GV.RM-03, GV.RM-04 **ISF SOGP:** IR1.1, SG1.2, AS1.3, AS1.4	*Terms of reference which define the structure, purpose, and scope of the forum(s).* *An approved set of metrics should be used as indicators of security maturity. These indicators should be reviewed during management forums to provide insights into information security and risk within the organisation.* *Meeting minutes showing routinely scheduled forums with updates, reports, actions, and decisions.* *Retention of meeting records, including agenda, papers and reports.*

Reference	Minimum requirement	Control reference	Compliance Metric
6. Define the Roles & Responsibilities of the Wider Security Functions within the Organisation	Identify roles responsible for broader security activities, such as an IT Security Officer (ITSO), System Auditors, Security Operations staff, and Crypto Custodians. These activities may be fulfilled by existing roles subject to holding the necessary knowledge, skills, and experience (see *Section 7*). The responsibilities of the wider security function will cover attendance at IT governance boards/groups. For example, Security Working Groups, and Cyber Incident Response Teams.	**NIST:** DE.DP-1, ID.GV-2, PR.AT-1, PR.AT-2, PR.AT-5 **NIST CSF 2:** GV.RR-02, GV.OC-02, PR.AT-01, PR.AT-02 **ISO 27002:2022:** 5.2, 5.3, 5.5, 5.6, 8.16 **ISF SOGP:** SM2.3	*Roles identified within organisation structure.* *The number of roles responsible for the wider security function should be assessed in the context of the organisation's size, requirements, and sourcing model.* *Job Description and Role Profile available, supported by appropriate Professional Development Plan.* *Similar to the aforementioned roles, the responsibilities of the designated roles will should also be assessed in the context of the organisation.* *Meeting minutes detailing attendance and topics, relevant to security.*

Reference	Minimum requirement	Control reference	Compliance Metric
7. Information Security – Specific Training	Roles responsible for cyber security activities shall be suitably qualified and experienced according to the activities they are responsible for. This includes the roles such as Information Security Manager, ISO, ITSO, System Administrators, Security Operations staff, and Crypto Custodians. Individuals shall undertake continuous professional development to maintain their skills and competency. **See also:** • People Security Management Standard	**NIST:** ID.GV-3, PR.AT-1, PR.AT-2, PR.AT-5 **NIST CSF 2:** GV.OC-03, PR.AT-01, PR.AT-02 **ISO 27002:2022** 5.10, 5.26, 5.27, 5.31, 5.33, 5.36, 6.8, **ISF SOGP:** SM1.2, SM1.4, SM2.1	*Role profile or job description that requires a minimum level of knowledge, skills, and experience.* *Requirements for individuals to maintain professional certifications/ qualification where it is deemed necessary by the organisation.* *Records of Continuing Professional Development (CPD).* *Evidence of learning development pathways and training needs analysis.*

Reference	Minimum requirement	Control reference	Compliance Metric
8. Third-Party Management	Policing has a requirement to ensure information risks are identified and managed effectively throughout all stages of any relationship with external suppliers and third-party organisations. For a detailed set of requirements, controls, and metrics, see the **Third-Party Assurance for Policing (TPAP) Standard**	**NIST:** ID.BE.1, ID.BE.2 **ISO 27002:2022** 5.19, 5.20, 5.21, 5.22, 5.31, 5.32, 8.33,	*Categorisation of suppliers which is based on the risks posed to the organisation through accidental, or adversarial third-party compromise.* *Cyber risk assessment of suppliers and third parties.* *Register of suppliers & third parties. Regular reviews of suppliers and third parties.*
9. Project Management	All projects must follow a formal project management process that addresses the security requirements of the organisation. Projects must be run in a systematic and structured manner to allow security requirements—such as Secure-by-Design—to be implemented consistently. **See also:** • System Development Standard • Secure By Design Guideline	**ISO 27001: 2022** 5.8, 8.25 **ISF SOGP** SM3.1	*Policy or procedure setting out the requirements for security within projects.* *The application of recognised frameworks for project delivery.* *The alignment to Secure-by-Design requirements.*

Reference	Minimum requirement	Control reference	Compliance Metric
10. Cyber Insurance	There must be a documented policy or approach that covers the organisation's decision to purchase cyber insurance. As a starting point, this procedure must cover the business drivers for holding cyber insurance, such as using insurance to treat certain information risks, the potential impacts resulting from a cyber incident, the increasing frequency and cost of attacks, and the potential impact of regulatory fines. The business benefits of holding cyber insurance must also be established within this procedure. This will ensure that the organisation understands which of its risks are insurable, what the required level of coverage is, and what specialised services can be obtained from providers. It must also state what the policy terms mean in the context of the organisation. For example, premiums and excesses for budgeting purposes, indemnity limits, coverage, and claim conditions. Suitable methods of obtaining the correct level of cyber insurance must be documented. Details of an organisation's cyber insurance coverage must be stored securely, communicated to relevant personnel—but kept under a strict need-to-know policy. The policy must be reviewed regularly and following any significant business change to ensure that coverage remains valid.	**NIST:** ID.RM-01 **NIST CSF 2:** GV.RM-04 **ISF SOGP** SG2.4, IR2.6.5, SC1.4.6, SR1.3.1	*A documented decision on whether to purchase cyber insurance.* *A documented position of what the insurance policy must cover.* *How the risk resulting from a cyberattack is managed without cyber insurance (e.g. the impacts are documented and formally accepted).* *Details of how the procedure is communicated and stored securely, without the disclosure of information that may make the organisation a more attractive target to threat actors.*

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
1.1	PDS Cyber Specialist	Annual review. Minor amendments	04/07/2024
1.2	PDS Cyber Specialist	Annual Review. Minor amendments. Addition of NIST CSF 2.0 references.	06/07/2025

Approvals

Version	Name	Role	Date
1.1	NCPSB	National Cyber Policy & Standards Board	26/09/24
1.2	NCPSB	National Cyber Policy & Standards Board	31/07/25

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 & v2.0	04/2018
CSA Cloud Controls Matrix	v4	01/2021
College of Policing – college.police.uk	Web Page	04/2025
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
National Community Security Policy	1.4	09/2024