CYBER STANDARD DOCUMENT

SECURITY MANAGEMENT

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

Implementation of this standard will help members to ensure that adequate management controls and oversight is in place to mature their cyber resilience.

ISSUED	*October 2023*
PLANNED REVIEW DATE	*October 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	Matt Roff	Initial version	13/07/23
0.2	Matt Roff	Draft Update	28/07/23
0.3	Matt Roff	Update following consultation with PDS Cyber Standards Manager	14/08/23
0.4	Matt Roff	Update following consultation with PDS CSM	24/08/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National approving authority	28/09/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

Contents

Document Information 3
Document Location 3
Revision History 3
Approvals 3
Document References 3
Community Security Policy Commitment 5
Introduction 5
Owner 5
Purpose 5
Audience 6
Scope 6
Requirements 6
Communication approach 13
Review Cycle 13
Document Compliance Requirements 14
Equality Impact Assessment 14

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 Policing Community Security Policy (NPCSP) Security Management Policy statement. By implementing this standard, forces 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 (based upon the National Community Security Policy), and reinforce it through other security related 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., an Information Security Officer), 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 individuals employed in one or more Security Operation Centres (SOC), who contribute to an organisation's information security. Security management reporting should be in place to enable the organisational leadership to take informed risk management decisions, support the security-related elements of mergers and acquisitions, and take out cyber insurance, where appropriate.

Audience

This standard is aimed at:

- Member Senior Information Risk Owners (SIROs), Information Security Officers (ISOs), information security practitioners, Information Asset Owners (IAOs.)
- Third parties who act as service providers or suppliers to members.
- Auditors providing 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 Security Policy Framework	Members of the Policing Community of Trust must adopt and ensure adherence to the National Policing Community Security Policy. Ensure that appropriate policy & standards that cover all the NPCSP themes 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	**NIST:** ID.GV.1 **ISO 27001:2022:** 5.01, 6.04, 5.10 **ISO 27001/2:** 5.1.1, 5.1.2, 8.1.3, 18.2.2 **ISF SOGP:**	*Current, maintained policies distributed & easily accessible to all personnel, including visitors and contractors*

	to risk level. See the National Police Information Security Risk Management Framework (NPISRMF) The NPCSP framework policies, controls, standards, procedures ,guidelines and blueprints can be adopted to support this. All documents must have a regular review and approval cycle with updates communicated to the organisation where required.	SM1.1, SM1.2, SM2.1, SM2.2, SM2.3	
2. Define Senior Information Security Leadership Roles & Responsibilities	Appoint a suitably senior role as force Senior Information Risk Owner (or equivalent) to provide executive level accountability for information risks. • Implement the College of Policing role profile. • Ensure appropriate and adequate training is provided. The SIRO provides Senior leadership commitment to the National Cyber Security Policy and promoting 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	**NIST:** ID.GV.2, ID.GV.3, PR.AT.1, PR.AT.5 **ISO 27001:2022:** 5.01, 5.02, 5.03, 5.05, 5.06, 5.31, 5.32, 5.33, 5.35, 5.36, 8.24 **ISO 27001/2:** 6.1.1, 6.1.2, 6.1.3, 6.1.4, 7.2.3 **ISF SOGP:** SM2.1, SM2.2, SM2.3, SM2.4, SM2.5, SM2.6, SM2.7	*Organisation represented at regional SIRO meetings / national SIRO conference events and Boards*

	organisational management-level governance group) **<u>Linked Standards</u>** • Security Governance • People Management • Threat & Incident Management • Business Continuity **<u>See also</u>** • College of Policing Information Management Authorised Professional Practice (APP) • College of Policing Senior Information Risk Owner handbook. • National Police Information Security Risk Management Framework (NPISRMF)		
3. Establish Information Asset Owners	Appoint Information Asset Owners (IAOs) for organisational information assets • 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 Physical Asset Management Standard for further information. **<u>Linked Standards</u>** • Information Risk Assessment • Physical Asset Management • Information Management • Business Continuity	**ISO 27001/2:** 6.1.1, 8.1.1, 8.1.2, 8.1.3, 8.2.3, 12.6.2, 18.1.1, 18.1.2, 18.1.3, 18.1.5, 18.2.2, 18.2.3 **NIST:** ID.AM.1, PR.AT.2, PR.DS.3	*Job Description and Role Profile available* *Information Asset Register created and maintained, including regular review cycle for all assets*

	<u>See also</u> • College of Policing Information Management Authorised Professional Practice (APP)		
4. Establish Specialist Information Security Function(s)	Appoint Suitably Qualified Experienced Professional/s (e.g., ISO) • Define and implement a role profile or job description. • Assigned adequate authority and resources to run information security-related projects. • Responsible for leading security specific roles (e.g., ITSO, SOC staff and other IT security professionals) • To ensure compliance with laws and regulations affecting information security. • Consistently 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). • Provide expert advice in response to information security incidents. • Promotes a culture of information security awareness, with appropriate senior management support, that allows for decision	**NIST:** ID.GV.2, ID.GV.3, PR.AT.1, PR.AT.5 **ISO 27001:2022:** 5.01, 5.02, 5.03, 5.05, 5.06 **ISO 27001/2:** 6.1.1, 6.1.2, 6.1.3, 6.1.4, 7.2.3 **ISF SOGP:** SM1.1, SM2.2, SM2.3, SM2.5, SM2.6	*Role identified within organisation structure.* *Job Description and Role Profile available, supported by appropriate Professional Development Plan* *Maintained SyAp evidence. Timely responses to compliance requests.*

	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) **Linked Standards** • Security Governance • People Management • Threat & Incident Management • Physical & Environmental Management • Business Continuity **See also** • College of Policing Information Management Authorised Professional Practice (APP) • National Police Information Security Risk Management Framework (NPISRMF)		
5. Establish an Information Risk Governance forum	In support of the National Police 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.	**NIST CSF** ID.GV.4 & ID.RM.1 ISF SG1.2	Terms of reference. Meeting minutes. Records of meeting operations including agenda, papers and reports.

	The forum can review progress against the cyber security programme, arbitrate risk escalations, consider security incident trends, instigate organisational security initiatives and audits.		
6. Define Roles & Responsibilities of wider security functions within organisation	Identify roles responsible for broader security activities, such as IT Security Officer (ITSO), System Admins, Security Operations Centre (SOC) staff where applicable, Crypto Custodians etc. These activities may be fulfilled by existing roles subject to holding the necessary skills and competencies (see section 6.) • May include attending IT governance boards/groups, such as IT Security Working Groups, Cyber Incident Response Teams etc. **<u>Linked Standards</u>** • System Development • Application Management • System Access • System Management • Networks & Communications • Technical Security Management • Threat & Incident Management • Physical & Environmental Management • Business Continuity	**NIST:** DE.DP.1, ID.AM.1, ID.GV.2, PR.AT.1, PR.AT.2, PR.AT.5, RS.CO.2 **ISO 27001:2022:** 5.02, 5.03, 5.05, 5.06, 8.16 **ISO 27001/2:** 6.1.1, 6.1.2, 6.1.3, 6.1.4 **ISF SOGP:** SM2.3	*Roles identified within organisation structure.* *Job Description and Role Profile available, supported by appropriate Professional Development Plan*

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 of Information Security Officer (ISO), IT Security Officer (ITSO), System Administrators, Security Operations Centre (SOC) staff where applicable and Crypto Custodians. Individuals shall undertake continuous professional development to maintain their skills and competency. **Linked Standards** • People Management	**NIST:** ID.GV.1, ID.GV.3, PR.AT.1, PR.AT.2, PR.AT.5 **ISO 27001/2:** 8.1.3, 8.2.3, 18.1.1, 18.1.3, 18.1.5, 18.2.2 **ISF SOGP:** SM1.2, SM2.1	*Evidence of learning development pathways and training needs analysis.* *Effective training delivery – evidence will include a reduction in security incidents occurring within the organisation.*
8. Supply Chain Management	Policing has a requirement to ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers and third parties (including organisations in the supply chain). • Ensure that all third parties are examined to fully understand their overall security posture to enable risk owners to take informed decisions during procurement activities. • Third parties should be required to undergo a structured security assessment as part of the tendering process. This should be stated at the beginning of any tendering / procurement activity.	**NIST:** ID.BE.1, ID.BE.2 **ISO 27001/2:** 18.1.1	*Contract terms and conditions. Cyber risk assessment of suppliers and third parties. Register of suppliers & third parties. Regular reviews of suppliers and third parties.*

	• This includes where there is a shared responsibility for risk, cloud services for example. **Linked Standards** • Third Party Management (TPAP)		

Communication approach

This standard will be communicated as follows:

1. Internal peer review by the members of the National Cyber Policy & Standards Working Group which includes PDS and representatives from participating forces.

2. Presentation to the Nation Cyber Policy & Standards Board for approval.

3. Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed with information security officers (ISOs) and Information Management 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.

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.)