CYBER STANDARD DOCUMENT

SECURITY GOVERNANCE

ABSTRACT:
This Standard defines the requirements to implement Security Governance as mandated in the National Community Security Policy.

ISSUED	October 2023
PLANNED REVIEW DATE	July 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	Tim Moorey	Initial version	05/10/22
0.2	Tim Moorey	Template updated following National Policy & Standards Working Group review	06/10/22
0.3	Tim Moorey	Migrated to NPCC PDS template	17/04/23
0.4	Tim Moorey	Minor amends following NCPSWG comments and approval.	07/06/23

Approvals

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

Document References

Document Name	Version	Date
Authorised Professional Practice for Information Assurance - link		16/06/20
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
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 4
Community Security Policy Commitment 6
Introduction 6
Owner 6
Purpose 6
Audience 7
Scope 7
Requirements 7
Information Security Governance Framework 7
Strategy and Programme 8
Communication approach 10
Review Cycle 10
Document Compliance Requirements 10
Equality Impact Assessment 10

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 Governance Policy statement. By implementing this standard forces, and those delivering IT services on behalf of UK policing, will be able to demonstrate an effective governance framework and a clear commitment to information security and risk management.

As part of this, the creation and management of an information security strategy and programme is required.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

Security Governance

- To Establish, maintain, and monitor an information security governance framework, which enables Policing's information assurance governing body to set clear direction for, and demonstrate their commitment to, information security and risk management.
- To ensure that the governing body either directly or through its delegated representatives defines the maximum level of risk or impact that Policing is prepared to accept in any given situation, i.e., risk appetite.
- To Support the information security governance framework by creating an information security strategy and implementing an information security programme.

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.

It applies to all local, national and 3rd party systems that store, process and/or transmit policing data.

It also applies to projects and programmes that are building new systems that will store, process, transmit policing data.

Requirements

This section details the minimum requirements to implement an effective Cyber Security Governance structure to assure Policing systems and information.

Reference	Minimum requirement	Control reference	Compliance Metric
1	**Information Security Governance Framework**		
1.1	Members shall identify and communicate their place in the Community of Trust.	NIST CSF ID.BE.2	Records to evidence requirements being met. PCAF assessments.
1.2	A cyber security policy should be in place which is owned by a senior leader. The policy must be regularly reviewed considering organisational and regulatory requirements and changes. The policy must be communicated across all areas of the organisation with regular reminders to all personnel.	NIST CSF ID.GV.1 ID.GV.2 ID.GV.3	Cyber security policy in place owned by senior officer. Regular reviews. Records of communication & reminders.
1.3	A governance framework should be in place describing the overall governance structure inclusive of cyber security roles and responsibilities aligned with internal and external	NIST CSF ID.GV.2 ISO 27001:2022	Cyber security policy in place owned by senior officer.

Reference	Minimum requirement	Control reference	Compliance Metric
	roles (The National Community Security Policy Framework serves this purpose at a National Level and can be referenced by Forces). This should be supported by a strategy and delivery programme.	5.01	Regular reviews. PCAF review.
2	**Strategy and Programme**		
2.1	A cyber security vision shall be in place which includes missions, objectives, and activities to deliver them. A process shall be in place to set, review and prioritise these on a regular basis. The cyber security vision will be communicated across all areas of the organisation.	NIST CSF ID.BE.3	Records to evidence requirements being met.
2.2	A senior role must be assigned the mission and resources to coordinate, develop, implement, and maintain the organisation wide cyber security program.	NIST CSF ID.BE.2	Senior role assigned. Role description includes responsibilities.
2.3	Cyber and information security documentation shall be regularly reviewed and updated to ensure it meets the needs of the organisation and effectively meets the strategic vision and objectives.	NIST CSF ID.BE.3	Records to evidence requirements being met.
2.4	The cyber security policy shall include guidance for privacy and civil liberties. A programme of improvements shall take account of legal and National requirements or changes and address compliance gaps. Senior management should be appraised regularly so that they understand requirements and impacts.	NIST CSF ID.GV.3 ID.DV.1 ISO 27001 A.5.1.1	Records to evidence requirements being met.
2.5	Processes should include appropriate contact and escalation with National Policing bodies with regards to compliance issues and security events.	NIST CSF ID.BE.2 ISO 27001	Records to evidence requirements being met.
2.6	The status and performance of the Cyber security programme shall be assessed and reported to the responsible Senior Leader on a regular basis.	NIST CSF ID.BE.3 ISF SG1.2	Meeting minutes. Report records.

3	**Risk Management**		
3.1	The cyber security programme shall be focussed upon managing and reviewing cyber risks and supporting the National Information Risk Management Framework.	NIST CSF ID.GV.4 ISF SG1.3	Programme in place and reviewed. Risk register or similar with evidence of risk management practices.
3.2	The management of cyber risks will consider National Policing and Force objectives.	NIST CSF ID.RM.1 -3	Records to evidence requirements being met.
3.3	Cyber risk shall be considered alongside other organisational risks as part of risk management during operations, projects and change initiatives.	NIST CSF ID.RM.1 -3	Records to evidence requirements being met.
3.4	In line with the National Information Risk Framework, risk management processes must be in place. Risk appetite shall be communicated appropriately to enable effective risk management. A process shall be in place to review and handle exceptions or accepting risks above the agreed risk appetite. This should include risk balance cases and risk treatment plans with defined timed, objectives.	NIST CSF ID.RM.2 ISF SG1.3	Records to evidence requirements being met.
3.5	The National Community Security Policy applies and needs to be supported by local policies, standards or procedures which must be regularly reviewed and have defined responsibilities supported by processes, resources, and metrics.	NIST CSF ID.RM.1 ISF SG1.2	Cyber security policy in place owned by senior officer. Regular reviews. Evidence of supporting processes.
3.6	The information risk governance structure aligned to the National Information Risk Management Framework shall be in place for reporting and owning cyber risks.	NIST CSF ID.GV.4 & ID.RM.1	Records to evidence requirements being met.
3.7	There shall be a clear approach to consistently identify, assess, record and manage cyber risks across the organisation. This can be achieved through effective communication and the use of a risk management tool across the organisation.	NIST CSF ID.GV.4 & ID.RM.1	Records to evidence requirements being met. These will include threat & vulnerability and business impact assessments.
3.8	The performance of cyber risk management shall be reported and monitored by senior management on a regular basis.	NIST CSF ID.GV.4 & ID.RM.1 ISF SG1.2	Meeting minutes. Report records.

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 NCPSB 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