CYBER STANDARDS DOCUMENT

NCSP Cyber Procurement Standard

ABSTRACT:

This Standard specifies the minimum requirements regarding cyber procurement processes and actions. It aims to provide members of the policing community with clear direction to manage procurement associated with any potential new suppliers / stakeholders entering into a new contract.

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 for Cyber procurement processes.

Introduction

This standard specifies the minimum requirements regarding cyber procurement processes and actions. It aims to provide members of the policing community of trust and third parties working for policing with clear direction to manage cyber procurement.

This standard also strives to support the National Policing Cyber Security Strategy published in June 2024 to meet its five strategic objectives:

- Manage cyber security risk
- Protect against cyber attacks
- Minimise the impact of cyber security incidents
- Develop the right cyber security skills knowledge and culture
- Measurements

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to outline the expectations and requirements for potential new suppliers from a cybersecurity perspective. To ensure that any new supplier adheres to high standards of cybersecurity, risk management, and compliance to protect both organisational data and the wider digital ecosystem. This process also ensures that third-party suppliers align with the organisation's commitment to cybersecurity and privacy.

In addition, the requirements stated in this standard are mapped across the following industry standard frameworks and acts:

- National Cyber Security Centre - How to assess and gain confidence in your supply chain... - NCSC.GOV.UK
- CIS Controls - CIS Critical Security Control 15: Service Provider Management
- NIST Cyber Security Framework v1.1 - NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)
- Information Security Forum (ISF) Statement of Good Practice (SoGP) - Securing the Supply Chain: Preventing your suppliers' vulnerabilities from becoming your own - Information Security Forum
- Procurement Act 2023 - https://www.gov.uk/government/publications/the-procurement-bill-summary-guide-to-the-provisions/the-procurement-bill-a-summary-guide-to-the-provisions

This standard helps members of the community of trust to comply with the National Community Security Policy (NCSP) Cyber Procurement Standard leading to:

- Establish a comprehensive and approved Cyber procurement framework (including understanding what needs to be protected and why; know who your suppliers are and build an understanding of what their security looks like; understand the security risk posed by your supply chain and build security considerations into your contracting processes and raise awareness of security within your supply chain. Encourage an organisation wide culture of reporting security within your supply chain and build trust with suppliers.

Audience

Members of the Policing Community of Trust must read and adopt this standard.

More specifically the standard is targeted at, those who are involved in the procurement or commercial contracts of new suppliers, either on behalf of national policing or at a local force level. The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of threat and incident management within policing:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Auditors providing assurance services to PDS or policing.

Any person who accesses or processes national policing systems with third parties, information or local force systems should be aware of the requirement to report actual supply chain cyber risks as described in this standard.

Finally, policing's reliance on any other external stakeholders acting as service providers or developing products or services for PDS or policing, should also be made aware of and comply with the content of this standard, in relation to their work on policing systems and data.

Scope

1. The requirements of this standard must form part of third-party supplier contractual obligations where Policing information is processed or stored on behalf of any member of the policing community of trust.
2. This standard applies wherever policing information is processed or stored, National policing IT systems, applications, or service implementations.
3. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.
4. The requirements of this standard can be considered as part of any agreements with third parties who are not suppliers, who have access to Policing information. Policing has a legal obligation to share data in certain situations where there will be no contract nor will there be any such agreement, i.e. data sharing with an accused's solicitor.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
Responsibilities of contracting authorities (members of the policing community of trust.)			
CPS 1.0	All suppliers to go through the Third Party Assurance Process (TPAP) and be onboarded via an appropriate Tier. A business risk profile should be in place for contracts that handle, process or dispose of policing information assets. This informs the overall risk appetite for supplier selection. Risk assessments and assurance must be completed by the contracting authority e.g. the force, not by the third party supplier. Where a force system is intended to connect to a national system, national assurance must be undertaken by PDS. Where an existing Force system intends to connect to a national system, that connection shall be dependent upon national assurance by PDS . This should entail risks being assessed using a cyber supply chain risk assessment process that covers the following areas	ISO 27001:2022 5.19 and ISF SOGP SC 1	Assessment that includes the National Community Security Policy and all associated standards.' All suppliers to go through the PDS Third Party Assurance Process (TPAP). Key Performance Indicators (KPIs) established for ongoing performance management throughout contract duration. Records of supplier assessments and risk reviews.

Reference	Minimum requirement	Control reference	Compliance Metric
	(aligned to the NCSP headings): • Security Governance • Information Risk Assessment • Security Management • System Development • People Management • Information Management • Physical Asset Management • Application Management • System Access • System Management • Networks and Communications • Third Party Management • Technical Security Management • Threat and Incident Management • Physical & Environmental Management • Business Continuity • Information Assurance		
CPS 1.1	Ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers (including organisations in the supply chain)	SF SOGP SC1.1 ISO 27001 15.1.1	Local process in place to identify, manage, review and escalate risks to Information Asset Owner. Risk register reflects identified risks
CPS 1.2	Identify and employ only those external suppliers that adequately meet security requirements.	ISF SOGP SC1.2	Local supplier assurance process in place. Risk profile for business requirement for contracts.

Reference	Minimum requirement	Control reference	Compliance Metric
	SIRO engagement where suppliers are used that do not meet security requirements and present risks outside of appetite.		Escalation process to SIRO for suppliers that are outside of risk appetite. Adequate security controls in place to meet risk appetite.
CPS 1.3	Aligned to the contract risk profile, define security requirements based upon the Policing National Cyber Policies & Standards for products and services provided by external suppliers and specify how they will be met.	ISF SOGP SC1.3	Local supplier assurance process in place. Risk profile for business requirement for contracts. Security controls aligned to NCSP defined to meet risk appetite.
CPS 1.4	Review supplier responses against security requirements to provide assurance that external suppliers are meeting security requirements. Seek documentary evidence from suppliers to support their responses.	ISF SOGP SC1.4 ISO 27001 15.1.1	Records of third party reviews against requirements including supplier provided evidence. Records of decisions re third parties. Risk register reflects identified / managed risks.
CPS 1.5	Ensure that cloud services (As A Service) meet cloud security principles and controls, and that information risks are managed in cloud environments.	ISF SOGP SC2.1 NCSC Cloud Security Principles.	Records of third party reviews against requirements. Schedule of regular reviews with suppliers against KPIs.

Reference	Minimum requirement	Control reference	Compliance Metric
		Cloud Security Alliance Cloud Controls Matrix.	Records of decisions re third parties. Risk register reflects identified / managed risks.
CPS 1.7	Address weak or insufficient cloud security controls that are outside of risk appetite to ensure that cloud services are securely managed in a heterogeneous, multi-cloud environment.	ISF SOGP SC2.2	Risk treatment plan with owners and timescales to resolution within appetite. Risk register reflects identified / managed risks. Schedule of regular reviews with suppliers against KPIs.
CPS 1.8	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	NIST CSF ID.AM.6	Records including contract statements / clauses.
CPS 2.0	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	NIST CSF ID.GV.2	Records including contract statements / clauses Schedule of regular reviews with suppliers against KPIs.
CPS 2.1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. Third parties will often not be fully compliant with every requirement, even after consultation with them. The contract service manager needs to consult with the Information Asset Owner (IAO) to decide whether the non-compliances are within risk appetite and can be managed	NIST CSF ID.SC.1	TPAP supplier assurance process in place, Records of decisions re third parties. Risk register reflects identified / managed risks including a schedule of regular reviews with suppliers against KPIs.

Reference	Minimum requirement	Control reference	Compliance Metric
	as risk cases or not. These risk cases may need to be presented to the Senior Information Risk Owner (SIRO) as required to consider whether the supplier fails the assessment.		
CPS 2.2	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed in line with the business risk profile associated with the contract. Third parties should be assessed in context as not all questions may be relevant for every service. Individual services to be performed may have particular requirements and third parties nominally of one rating may have additional requirements placed upon them. This should be done in consultation with the assurance manager for the system, service manager or person who has the best understanding of the risk environment for the service. For example, addition of an in person audit or a Police Assured Secure Facilities (PASF) audit may be required.	NIST CSF ID.SC.2 ISO 27001 15.1.2, 15.1.3	Risk profile for business requirement for contracts. Prioritised cyber security requirements. TPAP supplier assurance process in place, Records of decisions
CPS 2.3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet	NIST CSF ID.SC.3 ISO 27001 15.1.2, 15.1.3	Risk profile for business requirement for contracts.

Reference	Minimum requirement	Control reference	Compliance Metric
	the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.		Prioritised cyber security requirements. Records including contract statements / clauses.
CPS 2.4	Upon selection, contracts shall incorporate agreed measurable security requirements or key performance indicators to ensure continuous monitoring and review.	NIST CSF ID.SC.4 ISO 27001 15.2.1, 15.2.2	Key Performance Indicators / Metrics and reviews in contracts
CPS 2.5	Security points of contact shall be established with the contracted third party to enable regular dialogue to support reviews, performance monitoring and escalation of issues.	NIST CSF ID.AM.6 ISO 27001 15.1.2	Records including contract statements / clauses.
CPS 2.6	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.		TPAP supplier assurance process in place (including PASF where this is required) Contractual statement Records of decisions re third parties
CPS 2.7	Contracts should include a requirement of the third party to inform the contracting authority of any security event, incident or breach that relates to the contract regardless of whether it has a material effect.	NIST CSF PR.AT.3 NIST CSF ID.GV.2 ISO 27001 15.1.1	Records including contract statements / clauses. Records of notifications.
Responsibilities of contracted body or supplier			

Reference	Minimum requirement	Control reference	Compliance Metric
CPS 3.0	Third-party stakeholders (suppliers, customers, partners) understand their roles and responsibilities.	NIST CSF PR.AT.3	Records including contract statements / clauses.
CPS 3.1	Third parties and suppliers must inform the contracting authority of any security event, incident or breach that relates to the contract regardless of whether it has a material effect.	NIST CSF PR.AT.3 NIST CSF ID.GV.2 ISO 27001 15.1.1	Records including contract statements / clauses. Records of notifications.
CPS 3.2	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.		Contractual clause in place. Records of audits, tests and evaluations.
CPS 3.3	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	NIST CSF ID.AM.6	Records including contract statements / clauses.
CPS 3.4	Cybersecurity roles and responsibilities are coordinated and aligned with the contracting authority in order that regular performance reviews can be conducted.	NIST CSF ID.GV.2	Records including contract statements / clauses Schedule of regular reviews with suppliers against KPIs.
CPS 3.5	The third party shall have an information security governance regime in place including a board level accountable owner for cyber security risk.	NIST CSF ID.GV.2	Records including contract statements / clauses

Reference	Minimum requirement	Control reference	Compliance Metric
CPS 3.6	Ensure that cloud services (As A Service) meet cloud security principles and controls, and that information risks are managed in cloud environments.	ISF SOGP SC2.1 NCSC Cloud Security Principles. Cloud Security Alliance Cloud Controls Matrix.	Evidence against contracting authority requirements. Schedule of regular reviews with suppliers against KPIs.
CPS 3.7	The third party addresses weak or insufficient cloud security controls that are outside of risk appetite to ensure that cloud services are securely managed in a heterogeneous, multi-cloud environment.	ISF SOGP SC2.2	Risk treatment plan with owners and timescales to resolution within appetite. Risk register reflects identified / managed risks. Schedule of regular reviews with suppliers against KPIs.

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 issue) 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 including peer review	11/03/25
1.0	PDS Cyber	Incorporate changes from NCPSWG	04/06/25

Approvals

Version	Name	Role	Date
1.0	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	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021