NATIONAL POLICING COMMUNITY SECURITY POLICY FRAMEWORK

ABSTRACT:
This framework provides all national policing and its partners with a clear guide of how information security policies and standards work in national policing, the objectives of the framework, whom the framework and its supporting policy and principles apply to, whom has accountability for information security and risk and how policies will be governed.

APPENDIX A: Members

APPENDIX B: Policy & Standards Governance model visual

APPENDIX C: Glossary

ISSUED	September 2024
PLANNED REVIEW DATE	August 2025
DISTRIBUTION	Community Security Policy Framework Members

CONTENTS

INTRODUCTION

National policing will maintain public trust by securing data and by applying a consistent, proportional approach to technology risk across policing.

The National Policing Digital Strategy 2030 is built upon the 2025 Policing Vision to provide the foundations for policing to deliver the National Digital Strategic objectives and the NPCC Cyber Security Strategy. In the future we will exchange more data and information with partners, adopt new connected technologies and move to cloud-based infrastructures. The move to a more open ecosystem cannot be at the expense of information security.

This framework defines the holistic approach to information and technology risks by aligning to Government Security standards, guidance from the National Cyber Security Centre (NCSC) and industry standards. The National Policing Community Security Policy Framework supports a proportionate baseline standard of cyber security for national policing to deliver its operational and strategic objectives.

As the cyber threat landscape facing the UK Police forces continues to evolve, so must the means by which forces maintain their security posture. The purpose of the National Policing Community Security Policy Framework is to provide the structure for information security for national policing, suppliers, and partners to carry out their services securely.

Cyber security is achieved through the consistent delivery of internationally recognised controls. To effectively realise these control objectives, policing must maintain clear definitions on how they are achieved in both a local and national context. Rather than continuing to work in isolation across forces, policing will move towards a common set of cyber security policies, standards, processes, procedures, patterns, and guidelines.[1]

The National Policing Community Security Policy Framework, this document, will be referred to as the '**Framework**' throughout this document.

The scope of the Framework applies to both this document and the supporting National Policing Information Security Policy and National Policing Information Security Principles that underpin the Framework.

Membership of the established 'Community of Trust' requires alignment to this Framework and its underlying policy and principles.

---

[1] NPCC National Policing Cyber Security Strategy. Strategic Priority 3: Operational Consistency

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

PURPOSE

This Framework lays out how information security will be managed and governed for national policing. To achieve this, it defines:

- Who this framework and its supporting principles and policy applies to.
- The objectives of this Framework in the context of information security.
- Who is accountable for information security and the risk relating to information security within policing.
- What the Framework applies to (Scope).
- How information security is governed.
- Compliance with the Framework.
- Policy exception.

AUDIENCE

This document is intended for all in scope member organisations listed under Annex A, and any suppliers and partners that have access to, store and/or process police information.

This includes all personnel from the organisations defined above.

These member organisations and their suppliers and partners form the 'Community of Trust', which is the foundation on which policing's use of digital services is built.

OBJECTIVES

This Framework sets out Policing commitment to ensuring that adequate information security controls operate effectively on our information (whether held electronically or in hard copy). The Framework and its supporting policy and principles also set out what 'in scope' organisations and personnel should do to maintain adequate controls on policing information. In doing so, this Framework supports the policing strategic aims and objectives and should enable employees throughout our organisations to identify their roles and responsibilities in handling policing information.

The Framework will provide the means to demonstrate that a proportionate level of assurance to the National Police Chiefs Council (NPCC), Digital, Data & Technology Coordination Committee (DDaTCC), Police Information Assurance Board (PIAB), National Senior Information Risk Officer (NSIRO), National

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

4

System Information Asset Owners (NIAO), Local Senior Information Risk Owners (SIRO), College of Policing, relevant HMG organisations and other members and individuals of the National Policing Community, that risks to national policing information are being managed.

Compliance with this Framework will assure members of the community that all forces, relevant member organisations and individuals adhere to a minimum baseline of common security assurance, legal, statutory, and regulatory standards, ensuring the core information security principles (see Knowledge Hub) are followed and applied to an adequate level, providing assurance that other members of the community are protecting policing information assets. Adherence to the Framework will form the basis for compliance with Government National Cyber Security Strategy.

SCOPE

All national police information, systems, services, infrastructure, technologies, personnel, and premises, including all entities that can access, process and store police information are in scope of this Framework.

Organisations, agencies, and functions included in the scope of this Framework are listed in Annex A. This is not an exhaustive list; it is provided for ease of reference. Other entities, as described below, will also fall within scope of this Framework, but may not be listed.

Suppliers and partners that have access to, store and/or process police information are also in scope of this Framework.

FRAMEWORK

The National Policing Community Security Policy Framework is made up of several documents, with each level of documentation contributing to the management of information security and risk across policing.

The key Framework documentation is explained below.

Framework
This document. Provides a clear guide of how policies and standards work in national policing, what the objectives are, who the policy and principles apply to, defines accountability, explains how policy will be governed, and the exception process.

Principles
Provide a statement of commitment from PIAB and a set of guiding principles that policing will strive to achieve. They represent the 'What' we need to do to be secure. They do not tell you

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

5

'How', this is achieved through the policy and other more detailed supporting documentation, such as standards and guidelines.

They are intended to set direction and should be easily understood by all stakeholders.

Policy

Provides confirmation of management intent, in support of the principles and are approved by PIAB. Policy defines how the principles are achieved, but still at a level that can be understood by all stakeholders.

Policy will be clear, concise and in language that can be understood by all.

Standards

Provide minimum requirements regarding processes, actions, and configurations.

Guidelines

Provide recommended practices that are based on industry standards and help augment standards when greater discretion is permissible.

Control Objectives

Statements describing what is to be achieved as a result of the organisation implementing a control.

Controls

Technical, administrative or physical safeguards.

Baselines

Technical in nature and specify the required configuration settings for a defined technology platform, e.g. blueprints.

Procedures

Step-by-step instructions for implementing policies, standards, and controls.

GOVERNANCE

The National Police Chiefs Council (NPCC) delegates the ownership of Information Risk Management to the National Senior Information Risk Owner (NSIRO). The NPCC Information Assurance Lead provides direction and guidance to the Police Information Assurance Board (PIAB), which includes National System IAO and Force / Constabulary Senior Information Risk Owners.

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

6

The Police Information Assurance Board (PIAB) is responsible for provisioning national Information Assurance policy, implementing this Framework and acting as the regulatory authority.

The National Cyber Policy & Standards Board (NCPSB) is responsible for the validation of this Framework and the supporting Information Security Policy and Principles, prior to subsequent sign-off by PIAB and to review and approve the supporting Standards and Control Objectives.

The National Standards Assurance Board will publish all PIAB approved Policies and NCPSB approved Standards.

All Framework member forces, agencies and organisations ensure that adequate competent resources are assigned to Information Assurance (IA) activities including:

- Applying baseline security controls to protect against and detect cyber security events.
- Information risk management activities, including production and review of force system Information Risk Management and Assurance Information Security Policy compliance.
- Developing & maintaining security, education and awareness across all personnel.
- Timely completion of baseline compliance Information Assurance returns.
- Support for compliance audits by independent professional bodies, e.g. HMICFRS, and/or agents of the PIAB.
- Timely security incident investigation including, reporting through published Information Security Incident Processes and in accordance with current policies and standards.

There are two National Police Chiefs Council (NPCC) portfolios which have responsibility for Information Assurance, Data Protection (DP) and Freedom of Information (FoI) compliance.

- The **Information Assurance portfolio** is responsible for ensuring that the necessary measures are taken to protect the confidentiality, integrity, and availability of all Police Service information systems.
- The **DP and FoI portfolio** is responsible for ensuring that police information and processing complies with the principles contained in the Data Protection and Freedom of Information legislation.

See Annex B for detailed illustration of the governance process.

COMPLIANCE

Compliance and alignment to the Framework and its supporting policy and principles provides the baseline for the 'Community of Trust'. Policing must defend as one against identified threats and work based on a common assessment of Information Security Risk. Policing must pro-actively defend critical networks,

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

7

systems and applications in a coordinated manner and continuously baseline the cyber risk management position of each force and their digital services.

- Forces, agencies and organisations are required to demonstrate compliance with the Framework and its supporting policy and principles. Compliance provides assurance to PIAB, relevant HMG organisations and other community members that risks to community information is being managed to a level acceptable to the wider Framework community.
- Demonstrable compliance is provided through the Police Cyber Assurance Framework including:
  - o Continuous local Assurance through local Force Senior Information Risk Owner to the Police Digital Service Cyber Services, acting on behalf of PIAB.
  - o Continuous Evidence from force/system Information Assurance returns that are aligned to the NIST Cyber Security Framework.
  - o Information Assurance Independent audits, undertaken by PDS Cyber Services, and/or suitable assured auditors and/or agents of PIAB.

EXCEPTION PROCESS

On occasions where policy cannot be adhered to, an exception process is required. For national policing that exception process follows the form of Information Risk Management as described in the National Information Risk Management Framework.

When policy cannot be complied with, this will likely represent a risk to policing, resulting in the need to follow risk identification, quantification, and management processes.

Governance processes are in place for the management of these risks, and it is important that these processes are followed to ensure senior management are aware and in control of the information risks to which policing is exposed at any given time.

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

8

APPENDICES

ANNEX A - MEMBERS

Members of the 'Community of Trust' and so bound by this Framework and its supporting principles and policy, include those forces and agencies constituted under:

- The Police and Justice Act 2006;
- Police Act 1996;
- Police Act (NI) 2003;
- The Police and Fire Reform (Scotland) Act 2012.

And:

- National Police Chiefs Council (NPCC) and National Policing Co-ordinating Committees and Portfolios
- National Counter Terrorism Policing Head Quarters (NCTPHQ)
- British Transport Police (BTP)
- States of Jersey Police
- Guernsey Police
- Isle of Man Constabulary
- Police Service of Northern Ireland (PSNI)
- Ministry of Defence Police (MDP)
- National Crime Agency (NCA)
- Police Service of Scotland (PSoS), (branded as "Police Scotland")
- Scottish Police Authority (SPA)
- MoD Service Police Crime Bureau
- Civil Nuclear Constabulary (CNC)
- National College of Policing
- Home Office – PPPT
- Police Digital Service (PDS)

Suppliers and partners that have access to, store and/or process police information, are also in scope of this Framework, however, will likely be mandated through contract which will reference compliance to National Policing Policy and Standards.

Note: This list represents the current known mandated organisations, this list may be updated from time to time, to reflect the addition or removal of organisations. Updates to this list will not require a full refresh and approval of the Framework, only agreement from the impacted parties.

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

9

ANNEX B – POLICY & STANDARDS GOVERNANCE MODEL – VISUAL

Information Security Policy & Standards governance structure will provide direction, authorisation and visibility of national level cyber security principles, policy, standards, and control objectives, which will enable UK police forces, National System owners and other member organisations to work to a clear set of policy and standards, enhancing the security of UK policing and national systems. *Figure 1* provides a visual illustration of how the governance bodies operate.
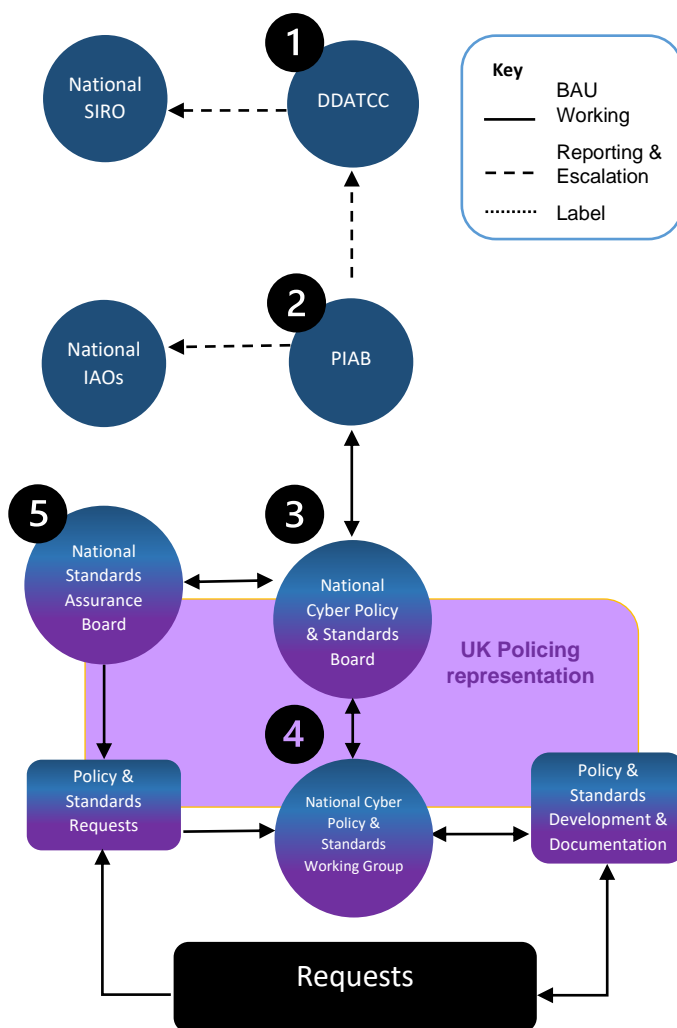

Figure 1

1	**Digital, Data & Technology Coordination Committee** chaired by the National SIRO, with senior representation from across policing. Will be informed of security frameworks, principles and policies, to which security standards will be aligned.
2	**Police Information Assurance Board (PIAB)** will review and approve security frameworks, principles and policies, validated by the NCPSB.
3	**National Cyber Policy & Standards Board (NCPSB)** chaired by a Senior Officer. Representatives include the PDS Cyber Services Leadership Team, National System Auditors, Force Auditors and Force representation. The remit of this group is to validate national policing security frameworks, principles & policy for subsequent sign-off by PIAB and to review and approve national policing security standards and control objectives.
4	**National Cyber Policy & Standards Working Group** chaired by the Cyber Policy & Standards Manager, will be made up of representatives from across PDS and community members. The remit of this group is to validate security policy & standard requests, identify the necessary resources with appropriate knowledge to develop and document the required policies, standards, control objectives, guidelines, controls, measures, procedures and baseline configurations. The Group will review and validate standards and control objectives, prior to sign-off by the National CP&S Board. The Group will review and approve guidelines, controls, measures, procedures and baseline configurations.
5	**National Standards Assurance Board** chaired by the National Standards Lead. Representatives from across policing, including legal and data representation. The remit of this group is to review, assess and approve publication of standards and related documentation to the Knowledge Hub for consumption by UK Police Forces and supporting organisations.

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

10

ANNEX C – GLOSSARY

Risks in information security typically arise due to the presence of **threats** and **vulnerabilities** to assets that process, store, hold, protect, or control access to **information** which gives rise to **incidents**.

Assets in this context are typically all personnel, equipment, systems, or infrastructure.

Information is the data set(s) that National Police forces want to protect (See National Policing Risk Appetite v2.2).

Incidents are unwanted events that result in a loss of **confidentiality** (e.g., a data breach), **integrity** (e.g., corruption of data) or **availability** (e.g., system failure). Threats are what cause incidents to occur and may be malicious (e.g., insider threat, national state, terrorism), accidental (e.g., a key stroke error) or an act of God (e.g., a flooding, earthquake).

The following table (Table 1) provides full titles in relation to any abbreviations that may have been used in the document.

Table 1

BTP	British Transport Police
CISO	Chief Information Security Officer
CNC	Civil Nuclear Constabulary
CSP	Community Security Policy
DDaTCC	Digital Data and Technology Coordination Committee
HMICFRS	His Majesty's Inspectorate of Constabulary and Fire & Rescue Services
IA	Information Assurance
IAO	Information Asset Owner
ISO	Information Security Officer
MDP	Ministry of Defence Police
NCA	National Crime Agency
NCPSB	National Cyber Policy & Standards Board
NCSC	National Cyber Security Centre
NCTPHQ	National Counter Terrorism Policing Head Quarters
NIAO	National System Information Asset Owner
NPCC	National Police Chiefs Council

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

11

NPIRMT	National Police Information Risk Management Team
NSAB	National Standards Assurance Board
NSGB	National Standards Governance Board
NSIRO	National Senior Information Risk Owner
PASF	Police Approved Secure Facilities Assessment
PIAB	Police Information Assurance Board
PIAG	Police Information Assurance Group
PIAF	Police Information Assurance Forum
PPPT	Police & Public Protection Team
PSNI	Police Service of Northern Ireland
SIRO	Senior Information Risk Owner
SLT	Senior Leadership Team
SPA	Scottish Police Authority

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

12

THE LEGAL BASIS

REVIEW

The Framework is 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 Framework continues to meet the objectives and strategies of the police service.

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

13

DOCUMENT INFORMATION

Document Location:

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
V0.1	Chief Cyber Architect (PDS)	Chief Cyber Architect (PDS)	Jan 21
V1.0	National Cyber Policy & Standards Board	National Cyber Policy & Standards Board	Sep 22
V1.3	National Cyber Policy & Standards Board	National Cyber Policy & Standards Board	Sep 23
V1.4	National Cyber Policy & Standards Board	National Cyber Policy & Standards Board	Sept 2024

Approvals

Version	Name	Role	Date
V1.0	Police Information Assurance Board	Police Information Assurance Board	23/09/22
V1.3	Police Information Assurance Board	Police Information Assurance Board	12/10/23
V1.4	Police Information Assurance Board	Police Information Assurance Board	01/10/24

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

14

Document References

Document Name	Version	Date
Government Functional Standard GovS 007: Security	2.0	13/09/2021
Information Security Management ISO27001	2022	2022
National Policing Community Security Policy	5.7	13/05/2019
NIST Cyber Security Framework	1.1	2018
National Policing Information Risk Appetite	2.2	Sep 2019
National Cyber Security Centre – NCSC.GOV.UK	Website	Nov 2021
National Policing Cyber Strategy	2024	Jun 2024

VERSION: 1.4
DATE: 21/08/24
REFERENCE: PDS-CSP-FRA

COPYRIGHT: Police Digital Service
DOCUMENT SIZE: 15-Page Document
CLASSIFICATION: OFFICIAL

15