POLICY DOCUMENT

# NATIONAL POLICING COMMUNITY SECURITY PRINCIPLES

**ABSTRACT**:
This document provides all National Policing and its partners with a clear set of information security principles, which are the foundation to all information security activity.

| | |
|---|---|
| **ISSUED** | September 2022 |
| **PLANNED REVIEW DATE** | August 2023 |
| **DISTRIBUTION** | Community Security Policy Framework Members |

**POLICY VALIDITY STATEMENT**
This policy is due for review on the date shown above. After this date, the policy may become invalid.

Framework 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 |
|---|---|---|---|
| V0.1 | Chowdhury Rahman | First draft | 25/11/21 |
| V0.2 | Dean Noble | Updated and restructured after initial feedback | 31/08/22 |
| V1.0 | Tim Moorey | Updated version following review at NCPSB | 22/09/22 |
| V1.2 | Tim Moorey | Cosmetic changes. Ported to NPCC PDS template. Content unchanged. | 09/02/23 |

Reviewed by

| Version | Name | Role | Date |
|---|---|---|---|
| V0.1 | Jason Corbishley | National CISO | Dec 21 |
| V0.1 | Dean Noble | Chief Cyber Architect (PDS) | Jan 22 |
| V1.0 | National Cyber Policy & Standards Board | National Cyber Policy & Standards Board | Sept 22 |

Approvals

| Version | Name | Role | Date |
|---|---|---|---|
| V1.0 | Police Information Assurance Board | Police Information Assurance Board | 23/09/22 |
| | | | |

## Document References

| Document Name | Version | Date |
|---|---|---|
| Government Functional Standard GovS 007: Security | 2.0 | 13/09/21 |

## Contents

## Introduction

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support and prioritise the way in which National Policing decides which ideas, initiatives and/or opportunities are to be progressed (and warrant investment) and those that are not.

These principles are a fundamental part of the National Policing Community Security Policy Framework and provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of information security capabilities can be assembled. The primary focus of these principles is to provide the starting point for, setting the policy, standards and control objectives, which support the Community Security Policy Framework.

The audience, scope, objectives, and governance for these principles are defined by the National Policing Community Security Policy Framework, which can be found on Knowledge Hub.

For clarity these principles are approved by the Police Information Assurance Board (PIAB) and apply to all members of the 'Community of Trust' as defined by the National Policing Community Security Policy Framework, and any suppliers and partners that have access to, store and/or process Police information, to provide services to Policing.

## Principles Structure

The principles described within this document will be structured in the following way:

**Name:** Clear, precise and easy to remember.

**Statement:** Generally, one or two sentences in length. Clearly tells the reader what the principle is.

**Rationale:** Explanation of why the principle is important and how it will benefit the National Policing and Law Enforcement Organisations.

**Implications:** Usually in the form of a list to describe what is required to successfully carry out the principle and how it could potentially impact Policing and those who supply to them.

**Principles**

PRINCIPLE 1: Accountability

**Statement:** National Policing is accountable for how it complies with the legislation and regulations governing the protection of the information assets it collects, processes, stores and transmits. National Policing must have appropriate measures and records in place to be able to demonstrate its compliance.

**Rationale:** Clear accountability provided through a top-down information security and risk management structure and mechanism for coordinating security and risk activity and supporting information security

governance will significantly improve policing's ability to have a clear view of its strengths and weaknesses and to manage its controls effectively and proportionally. This also enables auditability, which provides assurance to the community of trust.

**Implications:**

- Information asset and risk owners must be identified promptly and maintained to enable effective decision making.
- Information asset and risk owners should be adequately trained and competent to carry out their responsibilities in relation to information security and risk.
- Well defined and appropriate measures and the ability to collect accurate and timely management information to report against those measures will be key to effective decision making.
- For Policing to defend as one, members must seek to collate their measures and records, to enable a national view, to enable those with accountability to make informed decisions that benefit all of policing.

PRINCIPLE 2: Governance

**Statement:** National Policing will establish and maintain an information security and risk governance structure, with commitment demonstrated by Policing's governing bodies.

**Rationale:** Robust governance supported by Policing's governing bodies will ensure effective management of information security and risk. Policing will benefit from a good understanding of its risk exposure and the ability to effect mitigation through effective oversight.

**Implications:**

- Senior stakeholders from the National Policing Information Assurance and Technical communities will need to demonstrate commitment to the governance processes.
- Information security and risk control data, both locally and nationally, will be key to the effectiveness of the governance.
- Governance processes will be needed to identify, log and manage (mitigate, track and report) information risks, controls to address, and their effectiveness.

- A coherent set of policies, standards, and controls to manage risks to its information assets, facilitating control and direction of National Policing's approach to security will be required.
- Clearly defined roles and responsibilities for both accountable individuals and governance committees are essential.

### PRINCIPLE 3: Risk Based Security

**Statement:** The implementation of policy, standards, and controls for National Policing must be set at the appropriate level of risk appetite.

**Rationale:** Designing controls to mitigate inherent risks to within a defined risk appetite, rather than following a prescriptive control manual, with a one size fits all approach, will ensure more cost effective and useable security solutions.

**Implications:**

- Adopting a risk-based approach will require the involvement of key stakeholders from the National Policing Information Assurance and Technical communities, throughout the lifecycle of Policing systems.
- Controls defined and implemented will be commensurate with the level of risk being addressed, and the appetite for risk, set by the risk owners.
- Threat levels and resultant risk levels will need to be continuously monitored and prompt action taken to remediate increases in risk, outside of appetite.
- Security investment will be based upon levels of risk exposure, providing clearer return on investment.

### PRINCIPLE 4: Confidentiality

**Statement:** National Policing must ensure the information assets, with which it is entrusted are only accessed by those with the appropriate authority and need to do so, and necessary and proportionate controls are in place to prevent unauthorised access or misuse.

**Rationale:** Policing information needs to be protected from unauthorised access. Policing data is subject to both legal and regulatory requirements for its protection. Protecting this data from unauthorised access, will significantly reduce Policing information risk.

**Implications:**

- People, process, physical and technological controls will need to be designed, documented, and implemented for both national and local systems, to ensure confidentiality.
- Regular testing should be conducted to ensure confidentiality is maintained.
- Nationally agreed policy, standards and controls will be needed to help members achieve consistency of confidentiality across Policing systems, contributing to the community of trust.

PRINCIPLE 5: Integrity

**Statement:** National Policing must ensure the information assets with which it is entrusted, can only be modified by those with the appropriate authority and need to do so, and that suitable controls are in place to prevent unauthorised or accidental modification.

**Rationale:** Integrity provides the assurance that Policing data is accurate and reliable. Without integrity, the value of the data and outputs from that data cannot be trusted.

**Implications:**

- People, process, physical and technological controls will need to be designed, documented, and implemented for both national and local systems, to ensure integrity.
- Regular testing should be conducted to ensure integrity is maintained.
- Nationally agreed policy, standards and controls will be needed to help members achieve consistency of integrity across Policing systems, contributing to the community of trust.

PRINCIPLE 6: Availability

**Statement:** National Policing must ensure appropriate controls are in place to maintain the resilience of policing operations.

**Rationale:** System resilience is critical to ensure the continued availability of authorised access to Policing data through, and beyond, severe disruptions to its critical processes and the IT systems which support them, to ensure Policing and its partners can continue to deliver Policing operations.

**Implications:**

- People, process, physical and technological controls will need to be designed, documented, and implemented for both national and local systems, to ensure availability requirements are met.
- Regular testing should be conducted to ensure required levels of availability are maintained.
- Nationally agreed policy, standards and controls will be needed to help members achieve consistency of availability across Policing systems, contributing to the community of trust.

PRINCIPLE 7: Detection

**Statement:** National Policing must have the ability to identify the occurrence of confidentiality, integrity, or availability events promptly and accurately.

**Rationale:** Timely detection of accidental or malicious events in Policing information systems is critical to the ability to respond to those events. Failure to detect the event can and will lead to increased impact on policing information systems and therefore Policing's ability to carry out its operations.

**Implications:**

- An organisation wide culture of reporting suspected or actual security events or breaches.
- A robust detection capability requires significant investment in people, process, and technology.
- Continuous monitoring requires 24 by 7 coverage.
- Regular testing should be conducted to ensure event detection capability is maintained.

PRINCIPLE 8: Response

**Statement:** National Policing must have appropriate plans in place to act, in the event of a detected security incident, increasing the ability to contain the impact in a timely manner.

**Rationale:** Without effective and well tested incident response plans, Policing increases the time that adversaries can disrupt Policing operations or the time that internal errors persist in the Policing environment, increasing the impact on Policing operations.

**Implications:**

- Comprehensive and well tested incident response plans must be in place for information security events, both nationally and locally.
- Incident response plans should take into consideration supply chains on which Policing operations are dependent.
- Availability of accountable individuals for the management of local and national information security incidents is essential.

### PRINCIPLE 9: Recovery

**Statement:** National Policing must ensure appropriate plans are in place to recover any capabilities or services that are impaired due to a security incident.

**Rationale:** Following a security incident, Policing systems or services must be restored promptly to minimum recovery objectives, to allow Policing operations to continue, and vulnerabilities remediated to prevent similar incidents from reoccurring.

**Implications:**

- Business Continuity plans should be in place and regularly tested for both local and national systems.
- Disaster Recovery plans should be in place and regularly tested for both local and national systems.
- Business Continuity and Disaster Recovery plans should incorporate supply chain dependencies.

### PRINCIPLE 10: Secure by Design

**Statement:** The security of our information assets should never be an afterthought; security should be built in from the ground up. National systems will be assured against this principle.

**Rationale:** By building security into each phase of the lifecycle of a Policing system, from concept to decommissioning, ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the Policing community.

**Implications:**

- All new national systems will be built and assured following a secure by design methodology.
- The development of local systems should follow secure by design principles.
- Information Asset and Risk Owners will need to be engaged throughout the system development lifecycle.

PRINCIPLE 11: Culture

**Statement:** The first line of cyber defence for any organisation is its people. National Policing must develop and embed a security focused culture, through continual education and training of its population in best practices, to both protect themselves and the systems they develop and use, from cyber threats.

**Rationale:** Inadequately trained and educated personnel across Policing, increases the risk of employee action or inaction, resulting in a security breach, impacting the confidentiality, integrity or availability of Policing systems and information. A well-educated and trained Policing population will result in reduced information risk.

**Implications:**

- All personnel will participate in fundamental information security awareness and training activities, aligned to their respective roles.
- All personnel can easily report security weaknesses, suspected incidents or breaches.
- Senior Information Risk Owners (SIROs) and Information Security Officers (ISOs) should participate in training specialist for their roles.
- Information Asset and Risk owners should participate in advanced information risk training.

PRINCIPLE 12: Third Party Risk

**Statement:** National Policing is often dependent upon non-policing organisations to support policing operations. National Policing must ensure that National Policing principles, policy, and standards, are adhered to by the suppliers and partners that collect, process, transmit and store information assets on their behalf.

**Rationale:** Weaknesses in the security controls of our suppliers, partners, and their downstream suppliers, will eventually surface as incidents for Policing when those weaknesses are exploited. Identification and management of those weaknesses to prevent exploitation will be beneficial to Policing in reducing this risk.

**Implications:**

- Policing will need robust and consistent third party risk management processes and procedures.
- Policing will need a clear understanding of how their information is processed, stored and transmitted by third party suppliers and their supply chains.

**Review Cycle**

These principles 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 principles continue to meet the objectives and strategies of the police service.