POLICY DOCUMENT

NATIONAL POLICING COMMUNITY SECURITY POLICY

ABSTRACT:
This Policy provides confirmation of management intent, in support of the Community Security Principles. This Policy will define how the principles are to be achieved, at a high level. Detail to support this Policy will be in the form of standards, control objectives and other supporting documentation.

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.

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	Chowdhury Rahman	Initial Draft	01/03/2022
0.2	Chowdhury Rahman	Amends after feedback	03/03/2022
0.3	Dean Noble	Aligned to Framework and Principles	05/09/2022
1.0	Tim Moorey	Amended to reflect discussions at NCPSB	22/09/22
1.2	Tim Moorey	Cosmetic changes. Ported to NPCC PDS template. Content unchanged. PIAB approval 23/09/22 unaffected.	09/02/23

Approvals

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

Document References

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

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 policy in conjunction with the National Policing Community Security Policy Framework and the National Policing Community Security Principles sets out National Policing requirements for the establishment, implementation, maintenance, and continual improvement of appropriate information security controls. The controls will continue to be improved and aligned to any changes in National Policing strategy, operating environment, risk profile, laws and regulations, and in response to incidents or emerging threats.

Introduction

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

The Community Security Policy (CSP) is an integral part of the Community Security Policy Framework and combined with Community Security Principles and the supporting standards, control objectives and other supporting documentation will help policing maintain public trust in its management of information assets.

This Policy should be read in conjunction with the National Policing Community Security Policy (CSP) Framework, and Community Security Principles with which this policy is aligned.

The audience, scope, objectives, governance and exception process for this policy are defined by the National Policing Community Security Policy Framework, which can be found in Knowledge Hub.

For clarity this policy has been approved by the Police Information Assurance Board (PIAB) and applies 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.

This policy has taken into consideration and is aligned with industry best practice, which includes ISO/IEC 27002:2022, CIS Controls v8 (Center for Information Security), NIST Cyber Security Framework, CSA Cloud Controls Matrix v4 (Cloud Security Alliance) and NCSC 10 Steps to Cyber Security.

Purpose

The purpose of this policy is to:

- Establish a community wide information security and risk programme, which takes into account the internal and external issues relevant to its purpose and effectiveness and those that affect the community's ability to achieve successful policing outcomes.
- Establish, implement, and maintain appropriate controls to enable the delivery of National Policing governance, risk, and compliance requirements. Controls can be administrative, physical, or technological, the scope of which shall be our people, processes, and technology in the context of our operational, legal and regulatory environments.
- Establish authority, accountability, and competence for managing information security and risk.
- Protect information assets from risks associated with the theft, loss, misuse, damage, or abuse whether intentional or unintentional.
- Preserve the following attributes of policing information assets:
    - Confidentiality - Access to information shall be limited to those with appropriate authority.
    - Integrity – Information assets shall be complete and accurate, and technology assets shall operate correctly, according to specification.
    - Availability – Information assets shall be available to the right person, at the time, when it is needed.
- Assess the output of controls to monitor their effectiveness, performance and for reporting, maturity, continual improvement and to inform management decisions.
- Ensure on-going operational, legal, and regulatory compliance.

Policy Statements

The following policy statements are written to enable achievement of the National Policing Information Security Principles (see document list). The standards, control objectives and other supporting documentation developed to support this policy will be published separately and will contain appropriate guidance. It is the responsibility of all community members and other in scope organisations to ensure that they are familiar with and adhere to this policy.

Security Governance

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. The governing body either directly or through its delegated representatives should also define the maximum level of risk or impact that Policing is prepared to accept in any given situation, i.e. risk appetite.

Support the information security governance framework by creating an information security strategy and implementing an information security programme.

Information Risk Assessment

Conduct regular and continuous information risk assessments for target environments such as critical operational policing environments, processes, and applications (including those under development), and supporting technical infrastructure in a rigorous, consistent manner, using a systematic, structured methodology.

Adopt an information risk assessment methodology that includes important activities, which cover scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation, risk treatment and risk reviews. Information risks should form part of organisational risks management as appropriate.

Security Management

Develop a comprehensive, approved information security policy (this 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. a Chief 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.

People Management

Embed information security into each stage of the employment lifecycle (including personnel vetting, induction, employment contracts, ongoing management, and termination), assigning ownership of information (including responsibility for its protection) to capable individuals and obtaining confirmation of their understanding and acceptance. Enable individuals working in remote environments to protect critical and sensitive information they handle against loss, theft, and cyber-attack.

Maintain a comprehensive, ongoing security education, training, and awareness programme (SETA), to promote and embed expected security behaviour in all individuals who have access to the organisation's

information and systems.

Information Management

Establish an information classification scheme, which applies to all formats of information, supported by information handling guidelines. Protect information against corruption, loss, and unauthorised disclosure in line with its classification throughout all stages of the information lifecycle (create, process, transmit, store, and dispose) and in information transfer agreements.

Note: Policing is aligned to the Government Security Classification Scheme. Further details can be found here - Government Security Classifications - GOV.UK (www.gov.uk).

Assign responsibility for managing information privacy across Policing, both locally and nationally to a sufficiently senior manager (e.g. a Data Protection Officer), which should be supported by conducting data protection impact assessments and protecting personally identifiable information (i.e. information that can be used to identify an individual person).

Physical Asset Management

Protect physical assets, including endpoint devices (e.g. workstations, laptops and servers); office equipment (e.g. network printers and multifunction devices); and specialist devices and equipment (e.g. heating, ventilation and air conditioning (HVAC) systems, radio equipment and IoT devices) throughout their lifecycle, addressing the information security requirements for their acquisition (e.g. purchase or lease), configuration, maintenance and disposal.

Protect mobile devices (including tablets and smartphones), the applications they run and the information they handle against loss, theft and unauthorised disclosure by: configuring security settings; restricting access; installing security software; and managing devices centrally through an Enterprise Mobility Management (EMM) solution.

System Development

Establish a structured system development methodology that; incorporates a secure by design methodology; applies to all types of business system (including related technical infrastructure); is supported by a formal project management process; establishes specialised, segregated development environments; and involves a quality assurance process.

Develop applications in accordance with a robust system development lifecycle, which includes applying industry good practice and incorporating information security during each stage of the lifecycle (secure by design); requirements gathering; design; acquisition (including purchase, lease and open-sourced); build; testing; implementation; and decommission.

Application Management

Incorporate security controls into applications (including specialised controls for web applications) to protect the confidentiality and integrity of information when it is input to, processed by, and output from these applications.

Develop critical End User Developed Applications (EUDA), such as spreadsheets, Power BI, etc, in accordance with an approved development methodology, recording them in an inventory, and protect them by configuring security settings in vendor software; validating input; implementing access controls; restricting user access to powerful functionality; and managing changes diligently.

System Access

Restrict access to applications, mobile devices, systems and networks to authorised individuals and services (entities) for specific lawful business purposes, as defined in a formal access control standard and supported by an Identity and Access Management (IAM) system. Ensure individuals are only granted access privileges in line with their role; authenticated using access control mechanisms (e.g. password, token or biometric); and subject to a rigorous sign-on process before being provided with approved levels of access.

Protect applications that provide external user access by performing business impact assessments to determine information security requirements, and implementing security arrangements that are supported by agreed, approved contracts.

Ensure additional robust controls to limit privileged access to systems, networks or data.

Ensure 3rd party access is strictly controlled.

System Management

Design and build systems, including web servers and virtual instances (including containers), to operate securely and cope with current and predicted workloads. Configure them in a consistent, accurate manner to protect them (and the information they process and store) against malfunction, cyber-attack, unauthorised disclosure, corruption, and loss.

Manage the security of systems by performing regular backups of essential information and software, applying a rigorous change management process, managing capacity requirements, and monitoring performance against agreed service agreements.

Networks and Communications

Design physical, wireless and voice networks to be reliable and resilient; prevent unauthorised access; encrypt connections; and detect suspicious traffic. Configure network devices (including routers, firewalls, switches, and wireless access points) to segregate networks into domains, to function as required and to prevent unauthorised or incorrect updates.

Protect electronic communication systems (e.g. email, collaboration platforms and voice communication platforms) by setting policy for their use; configuring security settings; and hardening the supporting technical infrastructure.

Third Party Management

Identify and manage information risk in relationships with external suppliers and third parties throughout the supply chain (including suppliers of hardware and software; outsourcing specialists; and cloud service providers).

Implement a third party security management framework that includes security-related steering groups, standards, processes, and registers.

Embed information security requirements into both the procurement process and formal third party contracts, obtaining assurance that they are met.

Establish and enforce a comprehensive, documented security management approach for the acquisition, development, and use of cloud services, communicated to all individuals who may purchase, develop, configure, or use cloud services. Create and implement a set of fundamental cloud security controls, tailored to the needs of the policing, that includes network security, access management, data protection, secure configuration, and security monitoring.

Technical Security Management

Build a sound technical security infrastructure, applying security architecture principles and integrating technical security solutions, which include malware protection and intrusion detection.

Deploy approved cryptographic solutions (e.g. using encryption, public key infrastructure and digital signatures) in a consistent manner across the organisation to help protect the confidentiality of information; determine if critical information has been altered; provide strong authentication; and support non-repudiation.

Threat and Incident Management

Manage threats and vulnerabilities associated with applications, systems and networks by scanning for technical vulnerabilities; maintaining up-to-date patch levels across hardware, operating systems and applications; performing continuous security event monitoring; acting on threat intelligence; and protecting information against targeted cyber-attack.

Establish a comprehensive and approved information security incident management framework (including a designated incident response team; access to cyber incident investigators and forensics experts; threat-related information; and technical investigation tools), which is supported by a process for the identification, response, recovery, and post incident review of information security incidents.

Encourage an organisation wide culture of reporting of suspect or actual security events.

Physical and Environmental Management

Protect critical facilities and services, in line with a specialised physical risk assessment, against targeted cyber-attacks; unauthorised physical access; accidental damage; loss of power; fire; and other environmental or natural hazards. Physically protect all environments against unauthorised physical access.

Appoint local security coordinators in forces and national policing organisations throughout Policing, who are responsible for: maintaining a security profile (containing important details about service users, information, applications, equipment, technology, and locations); promoting information security; and managing information risk.

Encourage personnel to report physical security weaknesses or breaches promptly.

Business Continuity

Develop a Policing-wide business continuity strategy and programme, which is supported by a resilient technical infrastructure and an effective crisis management capability.

Develop, maintain, and regularly test business continuity plans and arrangements (sometimes including disaster recovery plans) for critical operational processes and applications throughout Policing.

Information Assurance

Implement a consistent and structured information security assurance programme, supported by comprehensive security testing (using a range of attack types), penetration tests, and regular security and risk compliance monitoring. To provide specific audiences, including representatives from executive management, Policing operations, and IT, with an accurate, comprehensive, and coherent view of information risk across the organisation.

Conduct thorough, independent, and regular audits of the security status of target environments (e.g. critical operational environments, processes, applications, and supporting technical infrastructure).

Review Cycle

This Policy 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 policy continues to meet the objectives and strategies of the police service.