NPCC National Police Chiefs' Council

POLICE DIGITAL SERVICE

CYBER STANDARD DOCUMENT

TECHNICAL SECURITY MANAGEMENT

ABSTRACT:
This Standard specifies the minimum requirements regarding technical security management. It describes the requirements to enable members of the community of trust to build and operate an effective technical security infrastructure, applying security architecture principles and integrating technical security solutions, such as malware protection, intrusion detection and cryptography.

ISSUED	January 2024
PLANNED REVIEW DATE	January 2025
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	Phil Penn	Initial version	07/07/23
0.2	Phil Penn	Updated following internal peer reviews	13/12/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for Cyber standards	25/01/24

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
National Policing Community Security Policy	1.3	09/2023

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 the design, building and managing sound technical security infrastructures protecting policing systems and data.

Introduction

In today's dynamic and interconnected digital policing landscape, establishing a robust technical security infrastructure is critical to safeguarding sensitive information and ensuring the confidentiality, integrity and availability of policing information assets.

This document provides the requirements to design, implement and maintain a sound technical security framework, incorporating security architecture principles and integrated solutions such as malware protection, intrusion detection, and approved cryptographic solutions, including Public Key Infrastructure (PKI).

It should be read in conjunction with the suite of the National Community Security Policy (NCSP) standards, guidelines and blueprints. Application should be considered in the context of local and national policing risk appetites.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

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.

Audience

Members of the Policing Community of Trust.

More specifically the standard is targeted at, architects, developers, and security experts tasked with designing and building solutions, applications and services that will process or store policing information assets.

The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of the use of technology 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.

Finally, Policing's reliance on third parties means that suppliers 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. This standard applies to all networks, cloud environments, applications and systems that process, store or access policing data or information assets. This includes but is not limited to, desktops, laptops & mobiles.

2. In addition, devices or systems that are not owned by members are expected to have the required technical controls in place wherever the systems are connected to national policing systems.
3. This standard applies to all production and non-production environments, including network, cloud and application environments.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1.0	**Build a sound technical security infrastructure**		
1.1	When designing or improving security infrastructure, ensure that the National Cyber Security Architecture Principles are applied including; 1. Security fundamentals 2. Security by design 3. Segregation and segmentation 4. Virtualisation 5. Application security 6. Protective monitoring 7. Automation and orchestration 8. Defend as one **See Also** • Cyber Security Architectural Principles	**ISO 27001:2022** 8.27	Project governance and designs include and make reference to the application of the principles. Decisions and exceptions are documented.
1.2	Ensure that there are easy to understand designs and documentation to ensure accurate decision making and implementation of technical security controls that must also be adaptive for interoperability and continuous improvement.	**NIST** DE.AE-1, **ISO27001:22** 8.27	Technical architecture design evidenced within High level and low level designs backed up with comprehensive supporting documentation

Reference	Minimum requirement	Control reference	Compliance Metric
1.3	Ensure that the security infrastructure supports the risk profile of the organisation and system in accordance with the National policing Information Security Risk Management Framework. **<u>See also</u>** • National Information Security Risk Management Framework (NISRMF) • NCSC Cyber Risk Management Framework • NCSC Risk Management Doc • NIST Risk Management Framework.	**NIST** ID.GV-4	Internal risk assessments and application of the NISRMF. Application of local risk management policies / frameworks. Regular management reviews of associated risks.
2.0	**Malware protection**		
2.1	An understanding of malware protection must be established and implemented within technical designs. • Anti-virus, Endpoint Detection and Response (EDR) tools should be included in design plans to demonstrate that device protection is applied to protect against malware. • AV, EDR should be configured with alerting in place • Management access should be restricted to privileged users.	**NIST** PR.AT-1, DE.AE-4, DE.CM-4, DE.CM-5 **CIS v8.1** 10.1,10.2,10.4,10.6,10.7 **ISO27001 :2022** 8.07 **ISO27001 :2013** A.12.2.1	Malware protection must be evidenced within designs Evidence of logging and monitoring of malware detection A comprehensive incident response plan to demonstrate action in the event of a malware attack Evidence of regular Penetration tests/ITHC to test the identify performance and reporting i.e.

Reference	Minimum requirement	Control reference	Compliance Metric
	- Consider using PDS National Management Centre malware portal for malware submission. See Thru (https://mas.nmc.police.uk/)		testing malicious weblinks and files in a sandbox environment or approved test files such as EICAR/WICAR
2.2	Malware that is detected must be contained, removed and analysed within a defined timescale. - Laptops, desktops, mobile devices and servers protection AV (Anti-Virus) or EDR (Endpoint detection and response) software installed to ensure adequate protection is provided against malware attacks - AV /EDR software should be monitored and configured to contain/quarantine and clean the device if malware has been identified. - Monitoring should be configured for review and examination by the Administrator to manually clean the identified malware. - Anti malware protection should have signature database regularly updated to ensure known malware is identified - A heuristic approach is good practice to include with anti-malware software to identify potential malware threats.	**NIST** RS.AN-1, DE.DP-4, DE.CM-4, DE.CM-5 **CIS v8.1** 10.2 10.3 10.4 10.5 10.6 10.7 **ISO27001:22** 8.07 **ISO27001 :2013** A.12.2.1	Regular reporting of detection and quarantine files identify regular patterns of IoC (Indicators of Compromise) Regular reviews and reporting of AV/EDR consoles to identify updates. Audit regular configuration changes with change management approval

Reference	Minimum requirement	Control reference	Compliance Metric
2.3	It is important as part of an overall defence approach to ensure that all authorised users are vigilant to threats. As part of an organisational cyber security education and awareness programme the following behavioural objectives should be met for all users of any IT service, system or application; • Aware of threats to IT systems • Identifies potential or actual malicious activity such as malware • Adheres to acceptable use policies and standards of behaviour • Reports suspected or actual incidents as required by the local security incident management procedures **See also** • People management standard • Threat & Incident management standard	**NIST** DE.CM-3, PR.AT-1, PR.AT-2, PR.AT-5, RS.CO-1, PR.IP-11 **ISO27001:2022** 6.03 **ISO27001:2013** 7.2.2	Acceptable Use policies in place for systems and services. Incident reporting and management procedures in place and tested. All personnel cyber education & awareness programme in place. Includes specific training / awareness to recognise and report malware threats. Records of reported suspected or actual malware.
3.0	**Protective monitoring & intrusion detection**		
3.1	Establish a baseline of network operations and expected data flows for systems and users. At the very least, critical and sensitive systems and data flows must be identified.	**NIST** DE.AE-1, ID.AM-3, ID.BE-4, ID.BE-5	Evidence baselines within information asset register, data flow maps and technical designs and documentation

Reference	Minimum requirement	Control reference	Compliance Metric
3.2	Apply protective monitoring for onsite and cloud environments with a defined timescale to react to suspected and active attacks. • Effective protective monitoring for cloud and onsite environments can be provided by a 24/7 operational Security Operations Centre (SOC) to enable effective monitoring. • Protective monitoring use cases must be used to define what is monitored within an environment. Example of use cases include; detecting compromised accounts, monitoring system changes, compliance with security policies, and threat hunting cloud applications • Detecting unusual behaviour on privilege accounts reporting and alerting should be provided to enable real time event management. • SIEM security event and incident management and SOAR Security orchestration and automated response. • IDS (intrusion detection system) and IPS (Intrusion prevention system) • Retention of protective monitoring logs 12 months /365 days	**NIST**,DE.AE-2,DE.AE-3, DE.AE-4, DE.CM-1,DE.CM-6, DE.CM-7 **ISO27001:2022** 12.2.1 **CIS v8.1** 13.1 13.1 13.3 13.7 13.8	Identify known and unknown threats such as detecting command and control and AV signatures, identify Indicators of compromise (IOC) such as threat trends. Endeavour to understand Automation with known threats. Regular reporting and reviews of threats. Establish roles and responsibilities of SME/management of Data and network analysts to identify and investigate threats. Regular reviewing of functionality and assets to include review of use cases for any changes of network implementation of new applications/hardware Protective monitoring works seamlessly with incident response plans.

Reference	Minimum requirement	Control reference	Compliance Metric
	See also • Threat & Incident management standard		Review log ingestions and retention identify hot/cold storage.
3.3	Ensure that all systems and assets are synchronised to a trusted, accurate time source. • Configure at least two synchronized time sources.	**NIST** PR.PT-1 **CIS v8.1** 8.4 **ISO27001:2022** 8.17 **ISO27001:2013** 12.4.4	Two synchronised time sources in use. All assets and security monitoring systems have synchronised time.
4.0	**Cryptographic solutions**		
4.1	• To ensure that integrity is applied public and private keys must be used. • When encrypting a private message use recipient's public key, to decrypt use private key. • To digitally sign a message, use a private key.	**NIST** PR.AC-4, DE.CM-7,, PR.DS-1, PR.DS-2 **CIS v8.1** 1,3.63.11,16.1 **ISO27001:2022** 8.24, **ISO27001:2013** 10.1 10.1.1 14.2.5,	Evidence of documentation , data flows , email policies Audit email traffic proxies Applying cryptography i.e. Public and private keys in messages email ensures that the sender is verified and

Reference	Minimum requirement	Control reference	Compliance Metric
	- To verify the sender's message, use the senders' public key,		therefore provide non-repudiation
4.2	Security of a PKI Public key infrastructure protection controls are required to ensure confidentiality, integrity and availability. This includes; - Ensuring secure storage of Private keys with controlled access. - ensuring that cryptographic keys are available to avoid any disruption in services and can be recovered in the event of an emergency.		Validation of configuration by independent review such as an IT health check. Verification and testing of key backup mechanisms.
4.3	To provide confidentiality to Cryptographic keys they must be stored securely with strong access controls to protect against unauthorised disclosure, theft, loss and corruption minimising the risk of an attack exposing critical or sensitive information. - Storage of Keys should be stored within approved digital vaults and Hardware Security Modules (HSM)on secure hardened devices. - Access to Keys should have strong access controls and multi-factor authentication (MFA). - Monitoring and access requests approved by a change management process.	**ISO27001:2022** 8.24 **ISO27001:2013** 18.1.5 10.1.2 10.1.1	The following should be audited and evidenced. Generation of keys using an HSM, random generator on a secure TPM. Keys should be encrypted with a strong algorithm Signing 2049-BIT RSA Hashing SHA -256. Evidence of secure key storage such as Azure key vault and apply strong access controls RBAC ,

Reference	Minimum requirement	Control reference	Compliance Metric
	- Key access control should be implemented between two authorised individuals', to ensure confidentiality is maintained. Two-person rule.		assign at least one approver with MFA enforced. Evidence of restricted access to Keys such as Private links , firewall and Virtual networks. Access requests to keys must be audited through change management approval.
4.4	Availability of PKI is critical to ensure that encryption services are operational and cryptographic keys can always be recovered during an emergency. - Regular backups of cryptographic keys including testing recovery.	**ISO27001:2022** 8.24 **ISO27001:2013** 18.1.5 10.1.2 10.1.1	Regular backups of Key vault. Monitoring of key vault with alerting in place.

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 Nation Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed within IT and information security 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 reporting.

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.

Document Compliance Requirements

(Adapt according to Force or PDS needs.)

Equality Impact Assessment

(Adapt according to Force or PDS needs.)

Appendix A – Terms and Abbreviations

Based upon National Institute of Standards & Technology (NIST) and National Cyber Security Centre

Term	Abbreviation	Brief explanation
Alert		A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.
Anomalies		Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.
Attack		Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Attacker		Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.
Anti-virus	AV	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
Data Loss Prevention	DLP	A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.
Distributed Denial of Service	DDOS	When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. Distributed uses numerous hosts to perform the attack.

Term	Abbreviation	Brief explanation
Endpoint Detection & Response	EDR	Endpoint Detection and Response (EDR) is an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response.
European Institute for Computer Anti-Virus Research	EICAR / WICAR	The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO) to test the response of computer antivirus (AV) programs.
Event		Any observable occurrence in a network or information system.
Exploit		May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.
Forensics		The practice of gathering, retaining, and analysing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
(Cyber) Incident		A breach of the security rules for a system or service - most commonly; Attempts to gain unauthorised access to a system and/or to data. Unauthorised use of systems for the processing or storing of data. Changes to a systems firmware, software or hardware without the system owners consent. Malicious disruption and/or denial of service.
Hardware Security Module	HSM	A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs.
Impact		The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Term	Abbreviation	Brief explanation
Intelligence		Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.
IoC (Indicator of Compromise)		(IOCs) serve as forensic evidence of potential intrusions on a host system or network. These artifacts enable information security (InfoSec) professionals and system administrators to detect intrusion attempts or other malicious activities. Security researchers use IOCs to better analyse a particular malware's techniques and behaviours. IOCs also provides actionable threat intelligence that can be shared within the community to further improve an organization's incident response and remediation strategies.
Intrusion Detection System	IDS	A security service that monitors and analyses network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
Intrusion Prevention System	IPS	A system that monitors the events occurring in a computer system or network, analysing them for signs of possible incidents, and attempting to stop detected possible incidents.
Malware		Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.
Multi Factor Authentication	MFA	An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Term	Abbreviation	Brief explanation
MITRE Attack	MITRE ATT&CK	MITRE ATT&CK ® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Adversarial Tactics, Techniques, and Common Knowledge
Phishing		Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Public Key Infrastructure	PKI	Public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption , The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.
Roles Based Access Controls	**RBAC**	Role-based access control is a policy-neutral access control mechanism defined around roles and privileges.
Security information and event management	**SIEM**	Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.
Security orchestration, automation and response	**SOAR**	Security orchestration, automation and response (SOAR) is a group of cyber security technologies that allow organizations to respond to some incidents automatically. It collects inputs monitored by the SOC such as alerts from the SIEM system and supports with incident response activities.
Security Operation centre	**SOC**	Security Operation centre is a team of security analysts that monitor and detect any malicious activity within systems over a 24/7 period, if any malicious activity is detected action is taken to eliminate the threat and report accordingly.

Term	Abbreviation	Brief explanation
Threat		Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Hunting		**T**hreat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find any malicious actors in your environment that may have slipped past your initial endpoint security defences.
Trusted Platform Module	TPM	A dedicated microcontroller designed to secure hardware through integrated cryptographic keys. The term can also refer to a chip conforming to the standard ISO/IEC 11889.
Vulnerability		A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.