National Police Chiefs' Council

POLICE DIGITAL SERVICE

CYBER STANDARD DOCUMENT

CYBER THREAT AND INCIDENT MANAGEMENT

ABSTRACT:

This Standard specifies the minimum requirements regarding cyber threat and incident processes and actions. It aims to provide PDS (Police Digital Service) and policing with clear direction to manage threat, vulnerabilities and incidents associated with cyber-attacks and cyber incidents.

ISSUED	December 2023
PLANNED REVIEW DATE	October 2024
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	PDS Cyber	Initial version	20/06/23
0.2	PDS Cyber	Updated for review	20/06/23
0.3	PDS Cyber	Updated following NCPSWG comments. Inclusion of Appendix A for terms	11/09/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for approving Cyber standards	30/11/23

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 standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out national policing requirements.

Introduction

This standard specifies the minimum requirements regarding cyber threat and incident processes and actions. It aims to provide policing, PDS (Police Digital Service) and third parties working for policing with clear direction to manage the threat, vulnerabilities and incidents associated with cyber-attacks and cyber incidents.

The Information Security Forum (ISF) Standard of Good Practice for Information Security 2022 (SoGP) defines threat and incident management as the ability to:

Manage threats and vulnerabilities associated with business applications, systems, and networks and to establish a comprehensive and approved information security incident management framework, which is supported by a process for the identification, response, recovery, and post-implementation review of information security incidents.

Examples as to how this can be achieved include:

- Continuous security event monitoring
- Acting on threat intelligence
- Having a dedicated Incident Response Team

These examples and other related actions are the focus of this document and are detailed throughout.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to establish formal requirements, which detail Threat Intelligence, Cyber Attack Prevention, Security Incident Management Framework and Security Incident Management Process that should be applied within each police force and PDS.

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

- ISO 27002:2022
- CIS Controls
- NIST Cyber Security Framework
- Information Security Forum (ISF) Statement of Good Practice (SoGP)

This standard alongside the Vulnerability Management Standard, helps members of the community of trust to comply with the National Community Security Policy (NCSP) Threat and Incident Management Policy heading;

- 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.

Audience

Members of the Policing Community of Trust.

More specifically the standard is targeted at, those who are needed to respond to or are involved in the response and recovery measures of a cyber incident or cyber-attack, 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, information or local force systems should be aware of the requirement to report actual or suspected security incidents as described in this standard.

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 wherever policing information is processed or stored, National policing IT systems, applications, or service implementations.

2. 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.

3. The requirements of this standard should 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.

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.

Requirements

This section details the minimum requirements for threat intelligence, cyber-attack response, security incident management framework and process to protect policing from the loss of confidentiality, integrity or availability of the data or loss of availability of the systems and services it relies upon to meet policing outcomes.

Reference	*Minimum requirement*	*Control reference*	*Compliance Metric*
1.0 Threat Intelligence	Each policing community member, PDS, Partner and 3rd party supplier should have a threat intelligence capability established which can effectively create, process, and manage threat intelligence. Threat intelligence utilised and created by policing should be: • relevant • insightful • contextual • actionable	SoGP SG1.2, IR2.3, SM2.2, TM1.3, TM1.4, TM1.5 ISO 27001:2022 Annex A 5.7 NIST ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4	NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested Artefacts produced by this requirement might include defined processes, a list of sources, threat assessments, reports
1.1	**Process.** The threat intelligence capability should be supported by a documented intelligence cycle, which includes: • a prioritised set of requirements to direct the production of threat intelligence. • identified information sources. • collection of relevant information from selected sources • processing information to prepare it for analysis. • conducting analysis of information to produce threat intelligence. • communicating threat intelligence clearly and concisely • using threat intelligence to inform decisions related to information risk.		Records of communicating threat intelligence, decisions, actions, reviews.

Reference	*Minimum requirement*	*Control reference*	*Compliance Metric*
	- taking action to implement the decisions made. - reviewing and improving the threat intelligence capability.		
1.2	Information relating to potential risks and/or adversarial attacks should be collected from both internal and external sources: *Internal*: - event logs from infrastructure and a security information and event management (SIEM) system - alerts from security solutions - dedicated teams that perform information security-related activities *External:* - trusted threat information providers or advisors - government agencies or similar - publicly available information		Evidence of log /alert collections, analysis, reports. List of sources, trusted advisors, agencies worked with.
1.3	The prioritised set of requirements should provide requirements-driven threat intelligence. This should: - provide an early warning system to identify threats that are likely to target the organisation. - determine the motivation, capabilities and commitment of identified threats and the extent to which the organisation is at risk of a targeted attack. - identify threat events likely to be used to attack the organisation. - demonstrate how information, gathered during reconnaissance, could be used by attackers.		Threat assessments, early warning reports Threat assessment reports, vulnerability

Reference	*Minimum requirement*	*Control reference*	*Compliance Metric*
	• determine the prevalence of threat events used at different stages of the cyber-attack chain. • identify technical vulnerabilities in operating systems, applications, and other software, which could be exploited to perform attacks on the organisation. • identifies the techniques used by attackers to maintain control of compromised systems and conceal their activity.		assessments, analysis of tactics, techniques and procedures.
1.4	**Technology.** The intelligence cycle should be supported by: • analytical tools, such as threat intelligence platforms (TIPs), to support the production and analysis of threat intelligence. • collaboration and the sharing of information with approved partners		Suite of tools / sources / partners
1.5	**Decision Making.** There should be 3 layers of threat intelligence across policing: • Strategic Threat Intelligence: high level information about the threat landscape • Tactical Threat Intelligence: intelligence on tools, techniques, and attack methodologies • Operational Threat Intelligence: intelligence on specific attacks and indicators		Defined process including documented decision making.

2.0 Cyber Attack Response	Each policing community member, PDS, Partner & 3rd party Supplier should ensure that there are documented standards, processes and procedures to respond to sophisticated, targeted cyber-attacks at each stage of the cyber-attack kill chain. * These will include National Cyber standards and procedures. These standards should consider all tactics under the MITRE ATT&CK Framework including: • Reconnaissance, typically using informative security controls (e.g., threat intelligence and an insider threat programme) • Initial Access Controls, typically using a combination of preventative and detective security controls such as strong multi-factor authentication, and encryption at all stages of the information lifecycle. • Maintaining control, typically using security controls such as strict audit of user accounts, and scanning systems and networks for anomalies • Identifying potentially compromised information, typically using security controls such as continuous monitoring and Data Loss Prevention (DLP) • Exploitation of information, typically performing threat intelligence, enhanced due diligence measures, and monitoring online activity for details about stolen material.	SoGP TM1.5 ISO27001: 2022 CISv8.1 1.1-1.5, 2.1-2.4, 3.1-3.14, 4.1-4.12, 5.1-5.5, 6.1.-6.8, 7.1-7.7, 9.1-9.7, 10.1-10.7, 12.1-12.8, 13.1-13.10, 14.1-14.9 NIST ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, ID.SC, PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.PT, RS.IM	NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested Documented, agreed, implemented standards, procedures and processes. Evidence of 3rd party supply standards & procedures.

2.1	**Process**. To understand the risks and impact associated with cyber-attacks, there should be a thorough review of potential attacks highlighting any vulnerabilities associated with: • people (e.g., successful social engineering attempts and potential insider threats) • processes (e.g., a weakness in any one process that a threat actor could exploit as part of the attack) • technologies (e.g., an unpatched operating system vulnerability or vulnerable legacy system). To achieve this: • systems, third-parties, software, and information systems should be inventoried, and risk assessed. • models of governance developed including organisational cybersecurity policies. • identity, credential, and authorised devices are documented. • all users should be informed and trained. • vulnerability management plan developed and maintained. • a baseline of network operations and expected data flows for users and systems should be established and managed. • the network, the physical environment and personnel activity should be monitored to detect potential cybersecurity events. ***-see Appendix A Terms and Abbreviations**		Documented processes and supporting records.

3.0 Security Incident Management Framework	**People.** Each policing community member, PDS, Partner & 3rd party supplier should have an established Cyber Incident Management Framework which is made up of specialist teams (or individuals) who: • Have defined and documented roles and responsibilities with sufficient skills or experience in managing incidents. • Have the authority to make critical business decisions and escalate as required. • Can communicate successfully with key stakeholders both internally and externally.	SoGP TM2.1, TM2.2, TM2.3, TM2.4 ISO27001: 2022 5.24, 5.26, 5.29 ISO27001/2 12.4.1, 16.1.1, 16.1.4, 16.1.5 CISv8.1 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7 NIST RS.IM.1, RS.IM.2, RS.OP.1, RS.RP.1	NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested Documented, approved cyber incident management framework. Records of reviews, approvals and invocations.
3.1	**Technology**. The framework should also have documented and detailed processes/ procedures which specify: • The dedicated technology tooling (SIEM) and incident analysis resources used to handle incidents quickly and effectively. • Details about how Cyber Security incidents should be recorded and maintained.		Documented, approved processes and procedures. Associated records including previous incidents and outcomes.
3.2	**Knowledge**. Information required to assist with the management of incidents should be documented and easily accessible to the specialised teams in place and look to include: • Contact details for all internal and external stakeholders, agencies, and partners. • Access to relevant security-related event logs, for example those produced by devices,		Contact register. Inventory / record of knowledge assets.

	applications, security products and systems. - Access to BAU cyber incident management process and Incident Response Plan. - Detail of an agreed escalation process internally within the force and externally for all Partners. - Threat intelligence and the results of threat analysis - Technical details of 3rd party vendors used across the estate.		Inventory of 3rd party suppliers.
3.3	**Control.** Legal and regulatory requirements should be identified and met during the incident response to include: - Security related laws and regulations relevant to the incident - Incident reporting timescales (e.g., Notifying the Information Commissioner's Office within 72 hours of a data breach being identified) - Any specific compliance requirements - Collection of forensic electronic evidence		Registry of legal & regulatory requirements. Forensic readiness policy / plan.

4.0 Security Incident Management Process **4.1**	Each policing community member, PDS, Partner and 3rd party supplier should ensure that Cyber security incidents are identified, responded to, recovered from, and followed up using an approved cyber security incident management process. **Incident Response Plan.** All policing community members must have a documented Cyber Incident Response Plan. This plan must describe incident response procedures including: • Roles & Responsibilities • Contacts & Escalation Process • Definition & Categorisation of an Incident • Training & Exercising • Overview of Existing Tools & Processes used in Prevention of a Cyber Incident • Incident Communication Plan • Major Incident Declaration Plans • Incident Reporting • Incident Plan Activation • Triage & Impact Assessment Process • Incident Analysis Process • Containment & Eradication Procedure • Remediation & Recovery Process • Post Incident Review Template & Process • Any Links out to Relevant Documentation or Interfaces to other Processes • The Incident Response Plan must be reviewed and updated annually as a minimum requirement or as	ISF TM2.2, TM2.3, TM2.4 ISO27001/2 16.1.1, 16.1.2, 16.1.6 CIS v8.1 7.2, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8 NIST DE.AE.1, DE.AE.2, DE.AE.4, ID.GV.2, PR.IP.1, PR.IP.10, RC.CO.3, RC.IM.1, RC.RP.1, rS.AN.2, RS.AN.4, RS.CO.1, RS.CO.2, RS.CO.3, RS.CO.4, RS.CO.5, RS.IM.1, RS.IM.2, RS.MI.1, RS.MI.2, RS.MI.3, RS.RP.1	NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested Documented, approved, maintained incident response plan.

	a result of testing / invocations.		
4.2	**Recording an Incident.** All cyber security incidents should be recorded in a log or ITSM system. As a minimum they should: - Be categorised and classified and given a reference. - Contain a description of the incident and the impact. - Contain all actions taken during the incident and any evidence gathered. - Include a start and end date and time. - Include a resolution reason.		Records of incidents and actions taken.
4.3	**Collaborative Working**. When responding to a cyber incident, policing community members and NMC should support this with collaborative actions including: - Sharing logs from relevant security or IT products, systems, and applications to complete analysis. - Sharing findings analysis and investigations - NMC Incident Response will respond to and acknowledge all force queries within 30 minutes. - NMC Incident Response will provide recommendations of actions to take, to policing community members, on their investigative findings.		Records of collaborative working internally and externally.
4.4	**War Gaming / Red Teaming**. Regular cyber security exercises should be performed to test the strength and validity of the Incident Response Plan, decision making capabilities		

	and aid continuous improvement. This as a minimum requirement, should be carried out annually. There should be multiple exercises built to cover different cyber incident scenarios such as: • DDoS • Malware • Ransomware • Phishing/ Smishing • Data Breach The Incident Response Plan must be reviewed and updated as a result of exercises.		Records of designing and undertaking exercises. Findings & learning outcomes.
4.5	**Communications.** All forces and systems must have a robust communications plan for reporting cyber incidents, both internally & externally. All incidents involving police data or systems that have been considered cyber related by the Information Security Officer must be reported to the NMC for visibility. Reviews of all information related incidents should be undertaken including trending. This will help ascertain the effectiveness of security controls as well as feedback into risk assessments. Communications should be: • Tested regularly to ensure they are fit for purpose. • Have a contingency plan in place to move to secondary methods if the primary methods are affected by a cyber incident.		Documented communication plans. Records of testing and reviews. Management reviews of incident reports. Incident trending and reviews against risks and controls. Records of regular communications across organisation. Management reviews of incident reports.

4.6	Forces and organisations should encourage the internal reporting of all non-cyber events, incidents, breaches or near misses that affect policing information. Examples include physical security, failures to follow policy, theft or damage. **Post Incident Reviews.** Following the recovery of a critical cyber incident a debrief or PIR must be completed by both PDS and the affected force or system owner: • To complete root cause analysis to identify the cause of the incident • Perform any forensic investigations if required from the event. • Record and track all actions raised follow up to ensure all are implemented. • To review existing processes and procedures to determine their capabilities and if they were fit for purpose during the incident. Any agreed changes to processes following this should be tested and documented. • Document the PIR in a report. • Recommend that a bi-annual aggregate review of all PIR's in the preceding 6 to 12 months be undertaken to identify any trends or developments. • Management reviews of incidents should help ascertain the effectiveness of security controls as well as feedback into risk assessments.		Records of previous incidents and outcomes. PIR reports Defined schedule of reviews of all incidents including trends and risk reviews.

5.0 Emergency Fixes	**Recommendations**. NMC (PDS) will provide recommendations to forces for any remediations and emergency fixes in response to a cyber incident. Forces and systems should have documented procedures for applying emergency fixes to business applications and technical infrastructure (including software and end points).	ISF TM 2.3	NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested

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 Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy 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.
Breach		An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.
Data Breach		A breach leading to loss of data.
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
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 analyzing 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.
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.
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.

Term	Abbreviation	Brief explanation
Kill-Chain		Developed by Lockheed Martin, **the Cyber Kill Chain®** framework is part of the **Intelligence Driven Defense®** model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective. The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.
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.
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.
Post Incident Review	PIR	A Post Incident Review is a document that is created after a cybersecurity incident has occurred: it is an in-depth analysis of what happened, how it happened, and what steps can be taken to prevent similar incidents from happening in the future.
Ransomware		Malicious software that makes data or systems unusable until the victim makes a payment.
Reconnaissance		A process of gathering information about the target organization. For an attacker, the first step of hacking involves collecting crucial information regarding the target so the attacker can then utilize this information to exploit and penetrate the target networks.
Recover		Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Term	Abbreviation	Brief explanation
Respond		Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
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.
Smishing		Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.
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.
Triage		Triage is an incident response technique for identifying and prioritizing your response to cyber threats. It helps you analyze threat alerts to determine the most harmful or impactful ones and prioritize them over others to prevent damage to your system.
Tactics, Techniques and Procedures	TTP	The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
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.

Term	Abbreviation	Brief explanation
War gaming / Red Teaming		A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.