CYBER STANDARD DOCUMENT

VULNERABILITY MANAGEMENT

ABSTRACT:
This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running IT services and managing vulnerabilities within PDS & policing systems.

ISSUED	November 2023
PLANNED REVIEW DATE	November 2024
DISTRIBUTION	Community Security Policy Framework Members

STANDARD VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, the standard 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	Ginu Mammen	Initial version	09/11/22
0.2	Ginu Mammen	Internal review updates	25/11/22
0.3	Ginu Mammen	Updated and circulated to PDS SMEs	16/12/22
0.4	Sonia Lombardo	Rebranded to NPCC PDS template	02/02/22
0.5	Ginu Mammen & Tim Moorey	Updated following NCPSWG comments	27/04/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for 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
NCSC CAF Guidance, B4.d. Vulnerability Management	3.1	04/2022

10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
Vulnerability management - NCSC.GOV.UK	Web Page	09/2016
Cyber Essentials technical requirements (v3.1)	V3.1	04/2023

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.

Introduction

Vulnerabilities are defects that weaken systems. All modern software contains vulnerabilities; either software defects that require patches or configuration issues that require administrative activity to resolve. These vulnerabilities must be addressed in a timely manner, to avoid disruption to organisation's operation and to preserve the confidentiality, integrity and availability of data and systems.

Vulnerability management is the continuing process that helps organisations identify, assess, prioritise, and minimise vulnerabilities in their system. Ultimately, the goal of vulnerability management is to reduce the risks posed by vulnerabilities by using techniques such as patching, hardening, and configuration management. This helps to ensure security while limiting risks that could potentially be exploited by malicious users.

This standard is aligned with the NCSC's vulnerability management guidance.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running IT services and managing vulnerabilities within PDS & policing systems. This standard sets out the requirement to identify and address technical vulnerabilities in a timely and effective manner to reduce exposure to the risk of them being exploited, thereby reducing the risk of serious security breaches.

Audience

This standard is aimed at:

- Staff across PDS & policing to any person who builds & implements or maintains IT systems, either on behalf of National policing or at a local Force level,
- IT System managers, administrators and those who have escalated privileges to provide administrative functions.
- Information & cyber risk practitioners and managers.
- Information Asset Owners (IAOs) and Senior Information Risk Owners (SIROs.)
- Suppliers acting as IT service providers or developing products or services for PDS or policing.
- Auditors providing assurance services to PDS or policing.

Scope

1. This standard is to cover systems handling data within the OFFICIAL tier including OFFICAL-SENSITIVE special handling caveat of the Government Security Classification Policy (GSCP). National and local policing IT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

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.

Requirements

The requirements to deliver effective vulnerability management are described in the table below:

Reference	Minimum requirement	Control reference	Compliance Metric
1	The organisation, business procedures, information processing facilities and systems that affect information security need to be controlled. Properly controlled change management is essential in most environments to ensure that changes are appropriate, effective, properly authorised and carried out in such a manner as to minimise the opportunity for either malicious or accidental compromise.	NIST CSF DE.CM.1 & DE.CM.2 & DE.DM.3 CIS 18 Controls 7.1.	Validation of process and documented evidence of risk assessed changes.
2	Management of Technical Vulnerabilities - Information regarding the technical vulnerabilities of information systems being used must be obtained in a timely fashion, so that the exposure to such vulnerabilities is evaluated and appropriate measures taken to address the associated risk.	NIST CSF ID.RA.1 & ID.RA.2 & ID.RA.3 & PR.IP.12 ISO 27001:2022 8.08 CIS 18 controls – 7.2	Maintained IT threat & risk assessment. Effective, accurate register of IT assets Documented evidence of vulnerability threat feeds and reviews.
3	Ensure that all information technology assets are continuously assessed and monitored for known vulnerabilities. Technology assets include all networks, servers, endpoint devices and peripherals. This also includes infrastructure, platform & software as a service (IaaS, PaaS & SaaS) infrastructures. **<u>Linked Standards</u>** • Physical Asset Management	NIST CSF DE.CM.8 ISO 27001:2022 8.08	Effective, accurate register of IT assets Records of scans across IT assets Records of ITHCs

Reference	Minimum requirement	Control reference	Compliance Metric
4	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. The process should describe the expected times to respond to and fix vulnerabilities.	CIS 18 Controls – 16.2 NIST CSFRS.AN.5	Reporting process, who is responsible for handling vulnerability reports, a process for intake, assignment, remediation, remediation testing, and a vulnerability tracking system. Records of time to respond and time to fix. Operational Level Agreements for remediation.
5	Perform Root Cause Analysis on Security Vulnerabilities	CIS 18 Controls – 16.3 NIST CSF RS.AN.5	Root Cause Analysis Process in the organisation, assess whether the root cause analysis process was followed in last 12 months.
6	Establish and Maintain a Severity Rating System and Process for Vulnerabilities (See further information section)	NIST CSF ID.RA.1 CIS 18 Controls – 16.6	The enterprise has a severity rating system and process for prioritising the order vulnerabilities are fixed
7	Newly identified vulnerabilities are mitigated across affected assets across the whole estate or documented as accepted risks. The patch management process should include conditions for temporary exceptions from patches being applied (See further information section)	NIST CSF RS.MI.3	IAO/SIRO receives and reviews monthly. vulnerability reports to ensure all. vulnerabilities are mitigated within. expected timeframes or risk accepted and documented.

Reference	Minimum requirement	Control reference	Compliance Metric
8	Handling unsupported / obsolete systems or applications: Establish a clear management plan and timeline for the decommissioning, replacement or upgrade of obsolete systems. All risks should be recorded on the system / project risk register. **See also** • National Information Security Risk Management Framework		Technical debt or similar register. Management plan to address.

Further information

Requirement 6: Vulnerability scoring

All vulnerabilities detected by scanning tools are assigned a severity level based on the Common Vulnerability Scoring System ("CVSS") Base Score Metrics: Critical, High, Medium, Low, or Informational. It is recommended to form a 'vulnerability triage group', consisting of staff with knowledge of cyber security risk, business risk and IT estate management. The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity. The Common Vulnerability Scoring System (CVSS) assigns numeric scores to vulnerabilities and attempts to assist in the process of vulnerability triage. It can be a useful tool if used correctly, but the triage group must ensure that they:

- Do not select an arbitrary score above which vulnerabilities must be fixed, ignoring all issues below that level.
- Do not take CVSS scores in isolation without considering organisation specific mitigations or priorities.

The establishment of standard timelines for vulnerability management is critical in ensuring that identified vulnerabilities are addressed promptly, reducing the risk of potential cyberattacks. The table below describes the vulnerability management remediation targets drawn from the Cyber Essentials technical requirements (v3.1) to help inform remediation efforts can be prioritised based on the severity and complexity of the identified vulnerabilities. Regarding systems which hold bulk personal data refer to point 8 of the NCSC Protecting bulk personal data guidance.

Category	CVSS Score	Vulnerability remediation target
Critical	**9.0 – 10**	**14 days**
High	**7.0 – 8.9**	**14 days**
Medium	**4.0 – 6.9**	**30 days**
Low	**1.0 – 3.9**	**30 days**

Table 1 - Vulnerability management remediation target times

Prioritise the correction of vulnerabilities based on the impact, severity and exploit complexity of a vulnerability. The decision to fix or leave an issue identified is, at root, a business decision and every organisation has their own risk appetite, refer to the National policing risk appetite guidance.

Requirement 7: Handling exceptions

Exceptions occur where it is not possible to deploy patches or updates in accordance with the timescales described in this standard. Exception requests must be handled by a local process including approval from IAO/SIRO. The process to review exceptions may be part of an IT change advisory board (CAB) for example.

Requests for exceptions should consider;

- The reason for the request,
- Risk to the enterprise of not following the standard,
- Specific mitigations that will not be implemented,
- Technical and other difficulties in applying patches,
- Mitigating factors,
- Risk management plan and
- Date of review

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.

This standard should be socialised with IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with your Force SIRO / 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 standard 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.)