CYBER STANDARDS DOCUMENT

APPLICATION MANAGEMENT

ABSTRACT:

This Standard is intended to guide the reader through the process of securely managing business applications both internally developed and externally sourced, regardless of whether locally installed or cloud based. Centred around stocktaking, documenting and actively managing those applications, this standard should enable the visibility of all business utilised applications, ensuring all are appropriately assessed for risk, appropriately licensed and managed in such a way as to not introduce cyber security risk going forward.

ISSUED	December 2023
PLANNED REVIEW DATE	November 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	Rick Martindale	Initial version	14/08/2023
0.2	Rick Martindale	Initial feedback applied	20/10/23

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	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 for application management.

Introduction

The Application Management standard is intended to minimise the risk of unsanctioned and poorly managed applications processing and potentially leaking sensitive information or compromising corporate systems. Additionally cost control and standardised ways of working will be introduced thereby reducing "Shadow IT".

The intention is to introduce security controls into and around applications to protect the confidentiality, availability and integrity of information processed by these applications. The premise behind these controls is to take stock of existing applications, record their existence, purpose, owner and condition in an asset inventory, and maintain this going forward for all business applications. Through this inventory, they can be protected by ensuring their configuration is secure, necessary additional controls are in place and any internally developed applications are following a secure development methodology.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to:

- Ensure business applications are protected against unauthorised access, invalid connections and unauthorised disclosure of sensitive information.
- Reduce the risks associated with web applications.
- Ensure the integrity of critical information stored in or processed by business applications is protected.
- Ensure End User Developed Applications (EUDA) function correctly, meet security requirements and are developed in a standard way.
- Assure the accuracy of information processed by critical spreadsheets and protect that information from disclosure to unauthorised individuals.
- Assure the accuracy of information processed by critical databases and protect that information from disclosure to unauthorised individuals.

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

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.

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

- International Security Form Standard of Good Practice (ISF SoGP)
- ISO 27002:2002
- CIS Controls
- NIST Cyber Security Framework

This standard should be considered alongside the System Development standard when developing applications.

Audience

This standard is aimed at:

- Those who procure, build, implement and manage IT applications for and on behalf of UK policing. This includes those within PDS, national policing and local forces
- The end-user community that have administrative privileges which allow them to install applications on End User Devices (EUDs) and servers (virtual and physical) or that produce EUDAs (End-User Developed Applications, e.g., complex macro enabled spreadsheets, Power Platform (including Power BI, Power Automate, Power Apps) Applications, visual programming etc.).
- Member Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs), Information Security Officers (ISOs), Data Protection Officers (DPO), information security practitioners
- Information & Cyber risk practitioners and managers.
- Suppliers acting as service providers or developing products or services for members of the policing community of trust who may have access to policing information assets.
- Auditors providing assurance services to PDS or policing.

Scope

In Scope

- New and existing applications.
- Prospective application purchases or application subscriptions.
- Locally installed applications.
- Cloud-based applications.
- End-User Developed Applications.
- Information assets associated to business applications.

Out of Scope

- Applications utilised entirely by third parties that do not interact with PDS or Policing data.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1.1 Risk Evaluation	Every effort should be made to acquire, lease or deploy robust, reliable software and software components (including open-source software.) A process should be in place to manage the acquisition of software applications that from the outset, considers security requirements and identification of any security deficiencies. This means, at a very minimum, a risk assessment should be run against any purchase, lease or onboarding of any applications, taking into consideration the assessment output to make an informed decision before moving forward. **Linked Standards** • Information Security Risk Management guidance • System Development Standard (for bespoke new applications)	ISF SoGP IR2.5 & SD2.3, ISO 27002:2013 13.2.4, NIST CSF ID.RA.5 & PR.DS.6, CIS v8 15.4 & 16.5	Software aquisition process Engagement with Information Security Officer (ISO) or equivilent. Record of review held on the asset register or audit of an approved application list and optionally a blacklisted application list.
1.2 Business Application Management	A register of all business applications, their associated data and application owners should be held. • This can be as simple as a manually maintained spreadsheet of all business applications, however, this can quickly become a big management overhead and risky in terms of application discovery. • Microsoft Intune has the capability of managing applications, but there are many other alternatives	ISF SoGP BA1.1 & SM2.6, ISO27002:2022 5.9 & 8.26, ISO 27002:2013 8.1.1 & 8.1.2 & 14.1.2, NIST CSF ID.AM.1 & ID.AM.2 & PR.DS.3,	Evidence of an actively maintained asset register with dynamic discovery in place will ensure compliance. Active scanning of endpoints (both user and system) will allow for

Reference	Minimum requirement	Control reference	Compliance Metric
	available in the software market that perform similarly. • The asset register should contain information relating to the application being managed such as the name, the version number, the vendor, the business owner, the license and support status and conditions as well as the license renewal date if applicable. Additionally, the register entry for an application should refer to the sensitivity of the data processed or accessed by the application and whether or not a DPIA has been carried out.	CIS v8 1.1 & 1.2 & 1.3 & 1.4 & 1.5 & 2.1 & 2.3 & 2.4 & 3.2 & 16.4	auditing of the efficacy of the asset register.
1.3 Business Application Protection	All business applications should be securely architected, hardened to industry standards, connections validated, and access controlled. Some of this will fall out of the risk assessment that should be run before onboarding the application (ref 1.1). Following on from onboarding, configuration according to vendor recommendations and allowing for business need should be followed. **<u>Linked Standards</u>** • Identity and Access Management Standard • System Access Standard.	ISF SoGP BA1.1, ISO 27002:2013 9.4.5 & 14.1.3, NIST CSF PR.DS.6, CIS v8 2.2 & 2.6 & 2.7 & 4.8 & 16.1	Regular vulnerability scans, penetration tests and audit of patch history, additionally vendor recommended configuration and updates should be applied where possible.
1.4 Vulnerability Management	Throughout the life of the application, vulnerabilities within should be identified, rated and remediated (patched) to an appropriate level in a timely manner. **<u>Linked Standards</u>** • Vulnerability Management standard.	ISF SoGP TM1.1, ISO 27002: 2013 12.6.1, NIST CSF ID.RA.2 &	Vulnerability management process Records of vulnerability scanning.

Reference	Minimum requirement	Control reference	Compliance Metric
		PR.IP.12 & DE.CM.8 & RS.AN.5 & RS.MI.3, CIS v8 7.2 & 7.3 & 7.4 & 7.5 & 7.6 & 7.7 & 16.2 & 16.3 & 16.6	Records of remediations
1.5 Acceptable Use	Acceptable use policies should define the organisation's rules on how employees and contractors can use business applications. The conditions of acceptable use will vary from one organisation to another, but must be clearly laid out to remove ambiguity.	ISF SoGP SM1.1 & SM2.6, ISO 27002:2013 8.1.3 & 8.2.3	Acceptable Use Policy exists and calls out the use of business applications specifically. See Local Acceptable Use Policy and Security Management Standard.
1.6 Web Application protection	Appropriate controls (both technical and procedural) should be in place for web applications and web content. Consider applying the NCSC cloud security principles A Web Application Firewall (WAF) should be utilised with a minimum core rule set applied (OWASP core rules are a good start), allowing for OWASP top 10 vulnerabilities and DDoS. Web content should be appropriately categorised for intellectual property rights, and/or appropriate attribution to the source material.	ISF SoGP BA1.2, ISO 27002:2022 8.23, NIST CSF PR.PT.5, CIS v8 4.4 & 9.3 & 13.1	A formal IT Health Check, or at the very minimum an appropriately scoped web application penetration test will confirm the web application protection is sufficient in a proactive manner. Protective monitoring logs and events.

Reference	Minimum requirement	Control reference	Compliance Metric
	Protective monitoring of the web application will apply reactive verification of the web application protection.		
1.7 Information validation	The confidentiality, integrity and availability of information processed by (input, storage, manipulation and output) business applications (including web applications) should be protected by appropriate security controls. Minimum requirements should validate input type and appropriateness, including checks for code injection and malware insertion.	ISF SoGP BA1.3, ISO 27002:2022 8.29, ISO 27002:2013 14.2.8, NIST CSF PD.DS.6	Penetration testing of web applications will test input and output validation.
1.8 EUDA Development	A documented methodology should be adhered to for the development of End User Developed Applications (EUDA) in order to meet defined security requirements. Following industry recommended development practices, such as version control, staged development and testing before rolling into live, change management and end of life processes.	ISF SoGP BA2.1, ISO 27002:2022 5.9, ISO 27002:2013 8.1.1, NIST CSF PR.IP.2	Documented development methodology. Audit of repository of EUDAs.
1.9 Protection of Office Productivity Suite software use	Input validation, access controls and user restrictions to powerful functionality should be applied to critical End User Developed Applications (EUDA) created using office productivity suites including word processing, spreadsheets, lists and presentations. Controls should be considered for automation and business information analysis tools. This is especially important for critical functions. This helps to prevent data breaches or unauthorised disclosures of data.	ISF SoGP BA2.2 & SA1.1 & SA1.2, ISO 27002:2013 9.1.1 & 9.4.1, NIST CSF PR.AC.1 & PR.AC.4 & PR.AC.6 & PR.PT.3, CIS v8 5.6 & 6.8 & 16.10	Audit of access requests for applications. Protective monitoring of critical systems. Code reviews or testing (static or dynamic).

Reference	Minimum requirement	Control reference	Compliance Metric
	Open access to powerful functionality and systems should not be granted, any spreadsheet / document / tool accessing data or services of a powerful or sensitive nature should be uniquely identified, appropriately authorised and have accesses restricted to least privilege. When sharing content: • Make use of document content inspection tools to identify hidden or automated content and remove it to minimise unintended data disclosure. • Consider exporting to portable formats such as PDF to ensure only necessary content is shared. See also Information Transfer guidelines. **Linked Standards** • System Access standard • Identity and Access Management standard • Information Management standard • Robotic Process Automation guidance		

Reference	Minimum requirement	Control reference	Compliance Metric
2.0 Protection of Databases	Input validation, access controls and user restrictions to powerful functionality should be applied to critical End User Developed Applications (EUDA) created using database programs. Open access to databases should not be granted, any database being accessed should have each entity accessing that database uniquely identified, appropriately authorised and have accesses restricted to least privilege. **Linked Standards** • System Access standard • Identity and Access Management standard	ISF SoGP BA2.3 & SA1.1 & SA1.2, ISO 27002:2013 9.1.1 & 9.4.1, NIST CSF PR.AC.1 & PR.AC.4 & PR.AC.6 & PR.PT.3, CIS v8 5.6 & 6.8 & 16.10	Audit of access requests for applications. Protective monitoring of critical Databases. Code reviews or testing (static or dynamic).

Communication approach

The Application Management standard 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 National 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 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 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 standard continues to meet the objectives and strategies of PDS and the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

The implementation of this standard should have no impact on equality. In some cases, special applications may well be needed for certain disabilities, however the applications required for those disabilities will pass through the same rigorous review, documentation and inventory management processes.