CYBER STANDARDS DOCUMENT

System Development – Secure by Design (SbD)

ABSTRACT:

This standard outlines the functions within the Secure By Design (SbD) process, aligned to project stages, to ensure a consistent approach to cyber security is achieved throughout a system's development. The purpose of this standard is to define an approach to ensure that all products / solutions are assured in a repeatable, structured and consistent way. This will enable security controls to be designed into solutions at an early stage, ensuring the secure delivery of solutions across policing, whilst identifying and managing risk to within risk appetite.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

ISSUED	February 2025
PLANNED REVIEW DATE	January 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT

This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

Handling Instructions

This document has been marked as OFFICIAL, with the following handling instructions applied:

- Distribution must be in-line with the *Communication Approach* Section set out within this document, and not shared wider than the PDS community, police forces and associated bodies. Further distribution requires prior and explicit documented approval from the Author(s), or the National Cyber Policy & Standards Working Group (NCPSWG).
- If you have received this document by mistake, you must securely dispose of this document and inform the Author(s) and/or NCPSWG email: nationalcpswg@pds.police.uk
- Where there is a need to distribute this document through email, you must use approved email routes e.g. police.uk, gov.uk, PNN, or CJSM.

Where there is a requirement to print this document, it must be stored in a physically secure environment with physical (and technological) access limited to those with permission to access i.e. distribution list and/or those with approval as per above. The printed document must be securely disposed of – for more information on this please contact the Author(s), or NCPSWG.

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 Secure by Design (SbD).

Introduction

This standard describes the requirements to fulfil the National Community Security Policy (NCSP) System Development Policy Statement. It also describes a Secure by Design (SbD) methodology as referred to in the National Community Security Principles.

The National Community Security Principle 10: Secure by Design

Statement: The security of our information assets should never be an afterthought; security should be built in from the ground up. National systems will be assured against this principle.

Rationale: By building security into each phase of the lifecycle of a policing system, from concept to decommissioning, this ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the policing community.

Implications:

- All new national systems will be built and assured following a secure by design methodology.
- The development of local systems should follow secure by design principles.
- Information Asset and Risk Owners will need to be engaged throughout the system development lifecycle.

Security by Design (or Secure by Design), often abbreviated as “SbD”, is an industry term for a range of security practices built on one fundamental idea — that security should be built into a product/solution by design, instead of being added on later by third-party products and services.

SbD as a methodology, has been selected to ensure that a repeatable, structured and consistent approach to the secure delivery of solutions across policing is achieved, as well as ensuring that risk is within risk appetite.

SbD is most effective if it is operated through each stage of project lifecycles; to ensure this, it should be mandated in change governance requirements.

Design documentation developed within the project lifecycle will be assessed and approved by the appropriate governance bodies within the force, organisation and/or national policing. Security Assurance will be based on documented standards and control objectives with all stages of the assurance process peer reviewed, including additional internal review processes, where required.

Building security into each stage of the lifecycle of a policing system, from concept to decommissioning, ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the policing community.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

System Development

- Establish a structured system development methodology that; incorporates an SBD 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.

The purpose of this standard is to define an approach to develop the maturity of assurance, ensuring that all products / solutions are assured in a repeatable, structured and consistent way. This will enable security controls to be designed into solutions at an early stage, ensuring the secure delivery of solutions across policing, whilst identifying and managing risk to within risk appetite.

This methodology should be mapped into the project lifecycle of the force or organisation it is to be used in. It is important that the Project Management Office (PMO) and third-party suppliers involved in a project are fully aware of the inputs and outputs required to progress through the project lifecycle.

The intention of this document is to provide a structured approach that can be adapted for use for all projects.

The process will:

- Provide a robust methodology by which assurance of any product / solution can be achieved.
- Allow national policing and force assurers to identify and understand security risk early in the project and support effective decision making to reduce risk.
- Ensure appropriate security controls are designed and not added.
- Give consistent and repeatable deliverables, to ensure risk is managed effectively and efficiently.
- Provide evidence for compliance and audit activities such as completion of the Security Assessment for Policing (SyAP) / Third Party Assurance for Policing (TPAP), internal and external audits.

- Increase the maturity of assurance.

Audience

Policing Community of Trust – specifically, but not limited to, Senior Information Risk Owners (SIRO), Information Security Officers (ISO), Project Management Office (PMO) and Information Asset Owners (IAO).

This standard is aimed at:

- Information Asset Owners (IAOs), Platform Asset Owners (PAOs), and Senior Information Risk Owners (SIROs).
- Project Management Office (PMO) and business change leads.
- Architects, system designers and engineers.
- Information & Cyber risk practitioners and managers.
- Staff across PDS and policing who are responsible for the selection, development or deployment of IT systems or applications either on behalf of national policing or at a local force level.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors providing assurance services to PDS or policing.

Scope

1. The principles and methodology of this standard are the foundation for National policing IT systems, applications, or service implementations. The requirements will be applied to new and existing installations.
2. This standard is applicable to any infrastructure, system, application, or IT solution that processes or stores policing information assets.
3. 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

This section details the minimum requirements to implement an effective Cyber Security System Development regime to assure policing systems and information. Coverage includes all the inputs and outputs to ensure a robust and consistent approach is taken to manage risk and assure products and services across the organisation. Several stakeholders will be required to be identified and engaged throughout this process to enable effective contribution and appropriate assignment of input and outputs at each stage.

The outputs defined may be produced by a number of stakeholders depending on the roles and governance structure of the organisation; this needs to be mapped out and responsibilities made clear. The organisation should consider producing a RACI Matrix to clearly define those responsible, accountable, informed or consulted as part of the process.

When applying this to a project, consideration should be given from the outset, on the scope of the project, ensuring it is fully understood by all stakeholders, including defining what deliverables are required. This should then be included within the project plan.

Reference	Minimum requirement	Control reference	Compliance Metric
1	**Feasibility, Appraise & Select, Define**		
1.1	Projects need to meet pre-defined information security requirements such as those described in the NCSP and associated standards, guidelines and blueprints.	**ISF SOGP:** SD1.2 SD1.4 SD2.1 SD2.5 **ISO 27002:** 5.8	Artefacts describing security requirements
1.2	Conduct Threat profiling to ensure that both generic and project specific risks are identified. Refer to the OWASP and Sector specific sources such as National Cyber Threat assessments, NMC threat assessments.	**NIST CSF (2.0):** ID.RA-1 ID.RA-2 **CIS (v8.1):** 16.1	Threat assessment process in place and assessments documented. Risks identified
1.3	A Business Impact Assessment (BIA) is undertaken to assess the risks associated with the initiative.	**ISO 27002:** 5.8	Business Impact Assessment

Reference	Minimum requirement	Control reference	Compliance Metric
	The BIA then informs decisions relating to the security requirements.		conducted and accepted by Project and Information Asset Owner
1.4	System development processes need to ensure that security requirements are defined adequately, agreed security controls are developed, and security requirements are met.	**NIST CSF (2.0):** ID.AM-08 **ISF SOGP:** SD1.2 SD1.4 SD2.1 SD2.5	Security Schedule in Contracts. Documented processes and procedures. Post implementation reviews.
1.5	Information security requirements need to be treated as part of business requirements and fully considered and approved.	**ISF SOGP:** SD1.2 SD1.4 SD2.1 SD2.5 **ISO 27002:** 5.8	Project artefacts
2	**Deliver**		
2.1	Systems are to be based on sound design principles that have security functionality built in from the outset whilst allowing for controls to be incorporated easily (System Development Life Cycle SDLC)	**NIST CSF (2.0):** ID.AM-08 **ISO 27002:** 8.25 **ISF SOGP:** SD2.2 **CIS (v8.1):** 16.1	Documented design principles, policy and processes. Post implementation reviews.
2.2	Ensure that system development activities take place under managed change control in a segregated secure environment to minimise disruption to operational / business activity.	**NIST CSF (2.0):** PR.IR-01 **ISO 27002:** 8.32	Technical architecture diagrams. Documented processes and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
2.3	Software and software components acquired from external suppliers or open sources need to provide the required functionality and not compromise the security of critical or sensitive information and systems.	**NIST CSF (2.0):** PR.DS-01 DE.CM-09 **ISF SOGP:** SD1.4 **CIS (v8.1):** 16.4 16.5	Documented processes and procedures. Evidence of testing / validation.
2.4	The asset register is updated in accordance with documented governance to reflect new assets, systems, services, software platforms and applications.	**NIST CSF (2.0):** ID.AM-08 ID.AM-02 PR.PS-02	Documented processes and procedures. Current, up to date complete asset register.
2.5	Systems are to be designed to be able to withstand malicious attacks, and to ensure that no security weaknesses are introduced during the build process.	**NIST CSF (2.0):** ID.RA-01	Documented designs and procedures. Vulnerability management plan. Evidence of testing / validation.
2.6	Coding vulnerabilities should be identified and remedied promptly, throughout the creation and updating of the code.	**NIST CSF (2.0):** PR.DS-01 DE.CM-09 **ISO 27002:** 8.4 8.28 8.31 **CIS (v8.1):** 16.9 16.12	Documented processes and procedures. Evidence of testing / validation.
2.7	Systems should function as intended, meet agreed security requirements and ensure the security of information.	**NIST CSF (2.0):** PR.DS-01 DE.CM-09	Documented processes and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
		ISO 27002: 8.26	Evidence of testing / validation. Project artefacts.
2.8	Avoid using real / live Personally Identifiable Information (PII) as test data. Use anonymised, randomised or pseudo anonymised data, and for AI solutions, validated – See NCSP AI standard. A Data Protection Impact Assessment (DPIA) must be completed where PII data is required to be used. Consider also other impact assessments which may be required within your organisation, such as an Equality Impact Assessment and Ethical use of data assessments	**NIST CSF (2.0):** PR.DS-01 PR.DS-02 PR.DS-10 **ISO 27002:** 8.33	Documented processes and procedures. Test data examples. DPIAs. Project artefacts.
2.9	Only security tested, and approved, versions of the system are permitted into the live environment.	**NIST CSF (2.0):** PR.DS-01 DE.CM-09 PR.IR-01 **ISO 27002:** 8.19	Documented processes and procedures. Evidence of testing / validation. Project artefacts.
3	**Operate, Embed & Close**		
3.1	The introduction of new systems or applications is managed in accordance with change management controls in order to minimise the risk of disruption to operational / live environments.	**NIST CSF (2.0):** PR.PS-01 **ISO 27002:** 8.32 **ISF SOGP:** SD3.1 SD4.1 SD4.3	Documented change management processes and procedures. Risk assessments. Minutes / notes from Change Boards.

Reference	Minimum requirement	Control reference	Compliance Metric
3.2	Throughout the lifecycle business assets are formally managed throughout removal, transfers, and disposal. This can be achieved through regular management reviews such as security working groups.	**NIST CSF (2.0):** ID.AM-08 **ISO 27002:** 7.14 **ISF SOGP:** SD4.1 SD4.3	Documented processes and procedures. Records of processes.
3.3	Assets are disposed of according to records management & information security policies.	**NIST CSF (2.0):** ID.AM-08 **ISO 27002:** 7.14 **ISF SOGP:** SD4.1	Documented processes and procedures. Asset certificates of destruction.

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 National Cyber Policy & Standards Board (NCPSB) for approval.

- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

This standard should be distributed within IT and project 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 / Information Management. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

This standard should be mapped to a project lifecycle and internal governance prior to adoption. Following this, it should be provided to the Information Assurance communities and PMO's and should also be shared with procurement & commercial leads to ensure this is built into procurement activities.

Measurables generated by adopting this standard can also form part of regular cyber management reporting and audit evidencing.

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 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.)

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial draft version	05/03/23
0.2	PDS Cyber	Updated following NCPSWG first review	25/05/23
0.3	PDS Cyber	Re-alignment	11/07/23
1.0	-	-	September 2023
1.1	PDS Cyber	Annual review incorporating minor changes to reflect latest practices, and moving to new Standards template.	05/11/24

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National approving authority	28/09/23
1.1	National Cyber Policy & Standards Board	National approving authority	06/02/25

Document References

Document Name	Version	Date
Government Secure by design	-	05/2024

National Policing Cyber Security Strategy	-	03/2024
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
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
https://www.ncsc.gov.uk/collection/10-steps	Web Page	05/2021