CYBER GUIDELINE DOCUMENT

NCSP Secure By Design (SbD) Guideline V1.0

ABSTRACT:
This document provides detailed guidance to support the National Community Security Policy (NCSP) system development (Secure by Design SbD) standard. Secure by Design 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 risks are managed within risk appetite.

ISSUED	February 2024
PLANNED REVIEW DATE	December 2024
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

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

CONTENTS

COPYRIGHT: Police Digital Services

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 guideline in conjunction with the National Policing Community Security Policy Framework and associated documents supports the National Policing requirements described in the system development standard.

Introduction

This document provides detailed guidance for Secure by Design "SbD" methodology as referred to in the National Community Security Principles and Policy (NCSP).

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, 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), sometimes abbreviated "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.

Secure by Design 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 risks are managed within risk appetite.

COPYRIGHT: Police Digital Services

The Secure by Design (SbD) methodology should be aligned to the project lifecycle and internal governance of the organisation.

This guidance should be read in conjunction with the requirements of the NCSP System Development standard. Guidance is offered for each requirement with examples given. While the examples provided are drawn from the Information Security Forum (ISF) Information Risk Assessment Methodology (IRAM) 2 methodology and US National Institute of Standards & Technology (NIST) cyber security standards, the guidance is designed to be versatile and can be adapted to use alternative risk management strategies.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guidance is to provide practical support to implement the requirements of the NCSP System Development (Secure by Design) core standard. 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 guidance can help members and suppliers of the community of trust demonstrate compliance with the following NCSP policy statements:

System Development

- Establish a structured system development methodology that; incorporates a secure by design 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.

COPYRIGHT: Police Digital Services

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 which process 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:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Those 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 guidance are based on the NCSP System Development (Secure by Design) standard, which applies to new and existing installations.
2. This guidance can be applied to any infrastructure, system, application, or IT solution that processes or stores policing information assets.
3. The security control requirements laid out in this guidance and the related standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.

Guidance details

This guidance should be used in conjunction with NCSP standards as referred throughout. Figure 1 below describes the stages of the Secure by Design process as described in the NCSP System Development standard. The document then provides supporting information to aid the practical application of the process throughout the lifecycle of projects.

COPYRIGHT: Police Digital Services

Figure 1 - Overview of the Secure by Design process from Appendix A of the System Development standard

Project Lifecycle Stages	Description
Policy Concept	The stage name is derived from many government projects started because of a policy decision. It's defined as the stage where the project requestor will work with project management office (PMO) to create a Project Brief, to request project support.
Feasibility	This stage is to begin to understand what is possible, how long it might take and how much it might cost. The project will gather requirements and produce an Outline Business Case and a High-Level Plan during this stage.
Appraise & select	This is the stage where purchasing or building of service(s) and/or product(s) is considered to meet the requirements defined earlier. An Invitation To Tender is produced, if required.
Define	During this stage any Invitation To Tender will be published and the service/product suppliers selected. By the end of this stage, the project will have produced the High-Level Design(s) and a Full Business Case.
Deliver	This is where the solution is built and tested. If this is successful, the project will finalise the production of a Low-Level Design and a draft closure plan.
Operate, Embed & Close	The project operates the solution and embeds it into the business, ironing out any issues and getting it ready to hand over to the business to run.
Operations	The solution will now be in full operational service, the project will have closed and day to day operations will be managed by a Business-As-Usual Team.

COPYRIGHT: Police Digital Services

1. Policy concept

Stakeholder Engagement and Collaboration: Engaging with key stakeholders is critical. Identify and actively involve them from the start to ensure their contributions align with the business and standard's objectives. Their roles, both in providing input (i.e., security requirements, identifying risks) and in handling outputs (i.e., project artefacts), will vary based on their positions within the organisational structure.

Clarifying Roles and Responsibilities: Given the different stakeholders and their potential roles in the process, it is important to clarify responsibilities for each. It is recommended to create a RACI Matrix – specifying who is Responsible, Accountable, Consulted, and Informed for each task or decision. This matrix will ensure clear communication and prevent potential overlaps or gaps in responsibility.

Project Scope and Deliverables: Before commencing any project, a comprehensive understanding of its scope is crucial. All stakeholders should have clarity on the project's boundaries, objectives, and the deliverables expected at its completion. Incorporate this understanding into the project's documentation, ensuring it aligns with the System Development standard.

Assuring Cyber Security in System Development: This guidance, in essence, highlights the need for a robust Cyber Security System Development approach. By following the System Development standard, the aim is to safeguard policing systems and information against potential cyber threats. The standard's requirements are the minimum threshold and continuous improvements should be considered and applied.

2. Feasibility, Appraise & Select, Define

The "Feasibility, Appraise & Select, Define" section offers a comprehensive roadmap for the initial stages of system development, ensuring cyber security considerations are embedded into the project.

This section begins with setting a foundational understanding of security requirements, by categorising and evaluating assets, tools like the IRAM2 Scoping and BIA assistant can be used to support with these activities.

As part of this evaluation, a risk appetite is set by relevant policing owners, determining acceptable risk thresholds for the organisation, thus offering clarity on project expectations. **See the National Information Security Risk Framework.**

The guidance then transitions into threat profiling to understand and categorise potential threats. This section emphasises the significance of a proactive approach to identifying vulnerabilities in both applications and infrastructure.

COPYRIGHT: Police Digital Services

Additionally, the importance of a Business Impact Assessment (BIA) is highlighted, underlining the potential implications of disruptions on the organisation's operations.

As projects evolve, the section highlights the need to integrate security requirements into system development and, crucially, align these requirements including High-Level Designs (HLD) and Low-Level Designs (LLD) and with business objectives. This holistic approach ensures that as projects transition from feasibility to definition, they do so with a robust cybersecurity framework in place.

2.1. Pre-defined Security Requirements

This segment serves as the foundational step, ensuring that the project starts with a clear and robust understanding of the necessary security measures. It underlines the importance of using a structured risk assessment methodology, such as IRAM2, to identify and categorise assets, leading to a comprehensive view of what needs to be protected and to what degree.

Guidance:

Profiling:

The initial stage of profiling involves documenting any apparent attributes of the organisation and the environment being analysed. This includes attributes such as the organisation's history, its roles and responsibilities within the community, the environmental dynamics, and the specific services it delivers.

Example: When assessing a project aiming to deploy an advanced policing surveillance system, profiling would involve understanding the police force's jurisdictional boundaries, the current technological tools in use, and the specific goals of the new surveillance system, such as real-time facial recognition or license (number) plate recognition.

Asset Identification:

Every project should begin by identifying its key assets, both tangible (like servers or physical devices) and information assets (such as proprietary data, personally identifiable information, commercial and financial information or intellectual property).

Example: In the context of a police force deploying a body-worn camera system, the physical assets would include the cameras themselves, and backend database servers. The information assets would include the video footage, which may contain Personally Identifiable Information (PII) requiring the need for robust security controls.

COPYRIGHT: Police Digital Services

Setting a Risk Appetite:

Defining Risk Appetite will help the project determine the level of risk deemed acceptable, and advocate controls and security measures required to be implemented and if there is any governance required i.e., stakeholder approvals for accepting certain risks. This ensures that project parameters are defined early on, offering a clearer scope of controls that need to be implemented to meet the risk appetite and decision-making pathway. **Refer to the National Information Security Risk Assessment Framework (NISRMF) and guidance.**

Example: For a project planning to implement a new digital evidence management system, the risk appetite is likely to be very low (Minimal or Averse) to protect against potential leaks of sensitive investigation details or personal data. This would impose a prioritisation of robust encryption and access control measures, ensuring that only authorised personnel can view the data.

Review Relevant Artefacts Describing Security Requirements

A thorough analysis of artefacts that include security requirements is essential. These requirements determine both the specific security features a system must have, and the expected behaviours, characteristics and constraints the system should support with regards to security.

Example: Specific security requirements might include controls like Multi-Factor Authentication (MFA), Audit Logging, Role-Based Access Control (RBAC), Security Protective Monitoring, or End-to-End Encryption. Meanwhile, requirements that stress system attributes might touch upon include Availability, Scalability, Resilience, and Maintainability – for instance, ensuring that security patches can be applied without causing extended system downtime.

COPYRIGHT: Police Digital Services

2.2. Threat Profiling

This section describes a systematic understanding and categorisation of potential threats. Using a structured approach helps in painting a holistic picture of the threat landscape. Threat Profiling highlights the need for proactive vulnerability assessments to identify potential weaknesses in both applications and infrastructure. Given the dynamic nature of threats, the section also encourages for periodic reviews, ensuring that the system under development remains resilient and responsive to the ever-evolving cybersecurity landscape. **See the NCSP Threat & Incident Management standard.**

Guidance:

Comprehensive Threat Understanding: Adopt a systematic approach to comprehending and categorising threats. Obtaining insights from reliable resources such as the OWASP Top 10 Most Critical Web Application Security Risks and sector-specific sources like National Cyber Threat assessments and National Management Centre (NMC) threat assessments can provide an enriched perspective. Using tools like IRAM2's Threat Profiling can support in documenting a holistic view of security threats, which includes more than the commonly identified threats.

Example: Understanding that threats do not only involve typical malware attacks or phishing attempts, but the wider range of threats, and includes any new CVE's (Common Vulnerabilities and Exposures), latest identified zero-days, insider threats, deliberate exfiltration of classified datasets, or increased activities of orchestrated Distributed Denial-of-Service (DDoS) attacks on policing infrastructure.

Proactive Vulnerability Identification: Rather than reacting to vulnerabilities as they are exploited, try to proactively uncover weaknesses in applications and infrastructures. Methods/tooling such as IRAM2's Vulnerability Assessment process and Penetration testing can be used to achieve this.

Example: Database systems storing sensitive PII including biometric data or witness details must undertake Information Technology Health Checks (ITHC) prior to the go live of a solution, and this should be followed up periodically post go-live, both in accordance with the **Penetration Testing and IT health checks guidance**. Aggregation of data should be considered when assessing data classification of a solution. Implementing proactive controls like intrusion detection systems (IDS) further reinforces the security of data.

Adaptive Threat Monitoring: The threat landscape is constantly changing and increased by evolving attack methodologies and advanced threat actors. Continuous integration of the latest threat intelligence feeds is essential to maintain a secure posture.

Example: Zero-day exploits, advanced persistent threats (APTs), or custom-tailored ransomware may be engineered to infiltrate certain types of servers or infrastructure. Continual threat intelligence gathering, and analysis can help to secure against these cutting-edge cyber-attacks.

COPYRIGHT: Police Digital Services

2.3. Business Impact Assessment (BIA)

A BIA is a critical component of an asset and risk management strategy. It provides a process to understand the potential consequences of unexpected disruptions to critical business operations by analysing the vulnerability of key assets and processes to various threats (as identified in sections above). The BIA is used to gain a holistic perspective on potential vulnerabilities, ensuring proactive measures can be taken to get the required security controls in place. Where Personally Identifiable Information (PII) features, a Data Privacy Impact Assessment (DPIA) will also be completed with consultation with the relevant Data Protection Officer.

Guidance:

After determining the scope (outcome of the "profiling" section above), identifying key assets, and evaluating potential threats, conduct a comprehensive BIA.

For every identified threat**, measure the impact on confidentiality, integrity, and availability** of information assets. Consider both realistic and worst-case scenarios.

- Confidentiality: Determine the impact if unauthorised individuals gain access to sensitive data.
- Integrity: Determine the impact if data is altered maliciously or unintentionally.
- Availability: Determine the potential consequences if data or services become inaccessible.

Where possible **quantify the consequences**: Once potential impacts are determined, translate them into quantifiable measures, such as financial loss or downtime duration.

Determine Business Continuity Requirements: Based on the identified impacts, stipulate the necessary measures to maintain or resume critical functions. This may involve establishing redundant systems, backup data centres, or emergency communications.

Review and Document: Compile a BIA report including Inherent Risk Report (IRR) summarising findings, potential impacts, and recommended protective measures. Ensure that these documents are reviewed and approved by key stakeholders. If possible, utilise tools that can support conducting BIA in a structured way, for example IRAM2's "Scoping and BIA Assistant".

Iterate and Re-assess: Threat landscapes and business operations evolve. Regularly revisit the BIA to ensure its relevance, adjusting for new vulnerabilities, business changes, or emerging threats. Consider use of frameworks like IRAM2's Risk Review cycles for structured re-evaluation.

COPYRIGHT: Police Digital Services

Example: During the BIA consider and discuss a data breach where PII is compromised. The BIA would assess the potential financial penalties, potential impact on public (i.e., loss of PII relating to criminal offences can have significant consequences), regulatory fines, reputational damage, and the cost of associated remedial actions. Recognising the severity of the consequences, the project should prioritise controls like advanced encryption protocols, strict access controls, and regular vulnerability assessments and comply with the required processes such as completing DPIA and keeping this up to date. As new technologies or threats emerge, this BIA would be periodically updated to maintain its relevance.

2.4. System Development Security Requirements

Embed robust security practices into the system development lifecycle and implement the controls defined to address the risks identified in the BIA and Inherent Risk Report (IRR). This can be done by aligning with NCSP standards and guidelines like NIST CSF PR. IP-2 (part of NIST SP 800-53), which highlights the importance of protecting data and information systems by applying relevant security safeguards throughout the development process.

Guidance:

Defining Security Controls: Establish and document the necessary security controls early in the development process. This includes identifying protective measures for data confidentiality, integrity, and availability as per NCSP standards and guidelines for example NIST.

Integrating Security in the Software Development Life-Cycle (SDLC): Incorporate security checkpoints and reviews at each SDLC stage, ensuring that all aspects of development adhere to the NIST framework's best practices.

Implement secure coding practices, regular code audits, and vulnerability assessments to identify and address security weaknesses early.

Risk Management and Mitigation: Regular risk assessments should be conducted in line with NIST guidelines to identify potential security threats and develop appropriate mitigation strategies.

Security of Third-Party Components: Ensure that third-party components and external development partners comply with NIST standards, conducting rigorous security vetting as part of the procurement process. See the **NCSP Third Party Assurance in Policing (TPAP) standard**.

Ongoing Monitoring and Improvement: Engage in continuous monitoring to detect and respond to threats swiftly, following NCSP standards and guidelines regarding incident detection and response.

Embrace a culture of continuous improvement, updating security measures to address emerging threats and technologies.

COPYRIGHT: Police Digital Services

Developer Training and Security Culture: Provide training and resources to development teams regarding secure system development and emerging cybersecurity trends.

Foster a culture where security is a priority at every stage of the development process.

Compliance and Documentation: Ensure all development activities and security measures are well-documented and in compliance with relevant standards and guidelines such as NCSP and OWASP. Regularly review and update documentation to reflect changes in the system and security environment.

Example:

In creating a cloud-based storage solution or an evidence management system, the development team should ensure that secure encryption protocols (as per policing standards) are implemented for both, data at rest and data in transit. They should also integrate other security controls like continuous security monitoring tools and conduct periodic security training for the development team, this will ensure that all aspects of the system's design and implementation are consistently aligned with relevant NCSP and NIST standards.

2.5. Business Requirements Integration

This covers the importance of embedding security within the business requirements. It highlights the need for security to be a core aspect, seamlessly integrated into the system's objectives and operational processes and treating security as an essential, integrated component throughout the system’s design and operational phases, rather than an additional consideration.

Guidance:

Aligning Security with Business Goals and Business Processes: Security practices should be woven into the fabric of the system’s requirements, designs including HLD’s, LLD’s and business objectives. This can be achieved by performing a detailed risk assessment at the beginning and integrating security controls that align with and enhance the business’s operational needs. For example, use of IRAM2 methodology to conduct a thorough risk assessment and aligning the findings with business objectives. Applying NCSP standards and guidelines alongside security Frameworks like NIST SP 800-53 can be used as to implement relevant controls and ensure that security measures are not only comprehensive but also support the business requirements of the system.

Collaboration Across Departments: Adopt a collaborative environment where system architects, developers, IT security teams, and business units work together. This ensures a unified approach to security, with each group understanding and contributing to the security landscape.

COPYRIGHT: Police Digital Services

Ongoing Education and Awareness: Regularly educate and update all staff involved in the system's lifecycle and business processes about the importance of security in its operation. Highlight how each role contributes to the overall security posture.

Example: Development of a system like digital case management application within a police force, where the primary business goal is to streamline case handling while ensuring the confidentiality of sensitive information.

To achieve this, the system's design needs to incorporate robust security controls to safeguard case details, security should be embedded in every business process and designs (HLD and LLD). The following are examples of security controls aligned with business processes:

- Role-based access controls to safeguard case details.
- In the data entry process, procedures are implemented to validate inputs, preventing potential data corruption.
- In the data retrieval process, multi-factor authentication is integrated to ensure that only authorised users can access specific case information.
- The system includes functionalities for regular security audits and real-time monitoring to instantly identify and address any vulnerabilities or security breaches.

This approach shows how security considerations, when integrated into both the business goals and processes of a system development project, can help create a robust, efficient, and secure operational environment.

3. Deliver

This section focuses on the practical aspects of implementing the system requirements and designs. This phase is critical as it bridges the gap between the theoretical security concepts outlined in the planning stages and their actual application in a real-world setting. It covers a wide range of activities like the deployment of the systems, ensuring its ongoing security posture, the management of changes, patches, and updates throughout the systems operational lifecycle.

This is where the security principles and strategies proposed in the earlier stages are implemented, configured, and tested. It involves translating the identified security needs and requirements into tangible, functional system components. Ensuring that the systems are built with robust security from the initial deployment through to regular maintenance and updates when delivered.

Key elements covered in this phase include the adherence to secure development practices, rigorous testing for vulnerabilities, and ensuring the resilience of the system against evolving cyber threats. This

COPYRIGHT: Police Digital Services

can also be applied to challenges of integrating new systems into existing infrastructures, managing the risks associated with these integrations, and ensuring that the system remains secure and functional.

Section 3 is where planning meets practical execution, ensuring that the security measures and controls designed earlier are effectively implemented and sustained over time. It is a critical phase that ensures the long-term success and security of the system in a dynamic and often challenging operational environment.

3.1. Secure Design Principles

In this phase the focus is on the practical implementation of security within the system development process. This section promotes a dynamic approach to security by integrating continuous testing, regular updates based on evolving threats, and incorporating feedback from relevant external sources to ensure that the system is not only secure at this point but remains resilient against future cybersecurity challenges.

Guidance:

Implement Security from the Outset: During system development, prioritise the implementation of security features as defined in the planning phase. This includes integrating security controls right from the initial coding/configuration stages and ensuring that every component of the system adheres to these pre-defined security specifications. This process can be supported by implementing Security Architecture Reviews, which can be used to assess if the system under development is adhering to defined security controls as per relevant security standards (such as ISO, CIS or NIST) at every SDLC stage.

User-Centric Secure Design: Focus on designing systems that naturally guide users towards secure practices. Develop interfaces that not only enhance user experience but also embed security as a fundamental component. Such as clear prompts for strong password creation or intuitive two-factor authentication processes.

Practical Application of Best Practices and Standards: Consistently apply industry-standard security protocols and best practices in a practical context for example, ensure that the system's architecture supports secure communication channels for data transmission and implements robust encryption for sensitive data. Stay updated with the latest developments in cyber security space by referencing resources like NCSC & NMC threat reports or IRAM2's threat horizon reports. This ensures the system is equipped to handle ongoing and emerging security threats.

Continuous Security Testing and Feedback Integration: Implement ongoing security testing methodologies like Static application security testing (SAST) and Dynamic Application Security Testing (DAST) throughout development lifecycle. Additionally, incorporate feedback from external security audits to improve security features frequently.

COPYRIGHT: Police Digital Services

Adaptive Security Architecture: Create a system design that is adaptable to emerging security threats and new vulnerabilities. This flexible approach should be informed by ongoing security reviews and external feedback i.e., NCSC and NMC threat reports. This will ensure that the system remains robust against evolving threats while creating a flexible architecture that can accommodate future security updates and enhancements without requiring a complete overhaul.

Example: In developing an online reporting tool for a police force, secure design principles include embedding strong data encryption from the start, following the relevant guidelines (i.e., NCSC, NIST and ISO). The system's user interface should be created in a way that promotes secure practices, supported by continuous security testing (ITHC). Throughout its development, the team should stay informed about potential threats and emerging risks by consulting appropriate threat reports, ensuring the system's design remains relevant and secure against evolving cyber threats.

The delivery phase of system development is not only about implementing security features but also about maintaining an ongoing commitment to security, backed by relevant strategic insights, standards frameworks, and methodologies.

3.2. Managed Change Control

Managed Change Control addresses the important requirement for controlled and systematic management of changes, this is applicable for both systems under development and systems that are operational. Controlled change management is essential for maintaining the integrity and security of the system during ongoing updates, modifications, or enhancements. This phase highlights the importance of a structured process for change management to minimise risks associated with changes and ensure that any modifications do not compromise the system's security.

Guidance:

Structured Change Management Process: Implement a formal change management process. This should include clear procedures for requesting, reviewing, approving, and implementing changes.

Risk Assessment for Changes: Before any change is applied, conduct a thorough risk assessment to understand the impact on the system’s security, this includes a potential impact on any associated applications, systems and/or environments. This ensures that any modification does not introduce new vulnerabilities.

Stakeholder Involvement: Ensure that all relevant stakeholders, including architecture, development, testing, security, and operations teams, are involved in the change management process. This collaborative approach helps in identifying potential issues early on.

COPYRIGHT: Police Digital Services

Documentation and Tracking: Maintain detailed records of all changes, including the reasons for the change, the risk assessment, and the implementation process. This documentation is crucial for audit trails and future reference.

Testing and Validation: Before the change is implemented it should be tested in a representative test environment. And after implementing the change, regression test the system to validate that the change has not adversely affected the system's functionality or security.

Post-Implementation Review: Conduct a review after each change to assess its impact and effectiveness. This supports in improving the change management process over time.

Example: A system requires an update to include new data fields. Under managed change control, this update will first undergo a risk assessment to ensure it does not impact any other aspect of the system and processes including data integrity or introduce vulnerabilities. Once approved, the change should be documented and deployed, initially in a development environment. It should then progress systematically through the stages of the SDLC: from development to a dedicated testing environment and subsequently to a pre-production environment that mirrors the live setting. This staged approach ensures the update is thoroughly tested for both functionality and security before it is rolled out to the live environment. Finally, a post-implementation review should assess the effectiveness of the update and identify any further improvements needed.

3.3. External Software Components

The management and integration of external software components within system development is essential because software or components acquired from third parties can introduce risks, such as vulnerabilities or compatibility issues, into the system. This section highlights the necessity of thorough vetting, testing, and continuous monitoring of these external elements to ensure they align with the system's security standards and do not compromise the integrity or security of the overall system.

Guidance:

Software assurance Process: Conduct a security assessment for each external product, component, and/or the supplier including open-source products and source code libraries. This should include evaluating the vendor's security practices, analysing the software's historical vulnerabilities, and ensuring compliance with critical security standards. The process aligns with NIST SP 800-53's Supply Chain Risk Management control (SA-12), which highlights inspecting the security risks associated with third-party products and services.

COPYRIGHT: Police Digital Services

Compatibility and Security Testing: Before integration, perform appropriate testing of external components for both compatibility with existing systems and potential security vulnerabilities. This aligns with section "2.2 Managed Control" above and is also recommended by NIST in the "Flaw Remediation control (SI-2)" in NIST SP 800-53, which mandates the timely correction of flaws discovered during security assessments, audits, or reviews.

Monitoring and Updating: Implement a process for ongoing monitoring and timely updating of third-party components and have a system in place for promptly implementing necessary patches or updates to maintain security.

Contractual Agreements and Compliance: Ensure that agreements with third-party vendors includes audit requirements and clauses on compliance with security standards (including data i.e., UK GDPR), regular updates, and disclosure of vulnerabilities.

Documentation and Record Keeping: Maintain detailed documentation regarding all third-party components, including their security features, updates, and any issues encountered.

Example:

When integrating a third-party software into a policing system. A security assessment of the software should be conducted, ensuring it meets policing security standards and is compatible with their existing system. They should test the software in a representative test environment, checking for any potential security vulnerabilities or functional issues. Once integrated, the software should be continuously monitored for updates or emerging vulnerabilities, ensuring it remains secure and functional. This should be complemented by clear documentation and adherence to contractual terms with the vendor for ongoing support and compliance.

3.4. Asset Register Management

Asset Register addresses the important aspect of maintaining an up-to-date and detailed asset register. This involves keeping record of all assets related to the system, including hardware, software, data, and any other resources important to the operation and security of the system. The purpose of this section is to ensure that all assets are accounted for, managed effectively, and protected, thereby contributing to the overall security and efficiency of the system. See the **NCSP Application Management and Physical Asset Management standards**. Further details are provided by NIST in SP 800-53's CM-8 control, which highlights the critical role of accurate and comprehensive asset management in system security and risk management.

COPYRIGHT: Police Digital Services

Guidance:

Comprehensive Asset Documentation: Create and maintain a detailed asset register that includes all components of the system. This register should cover both physical assets (like servers and networking equipment) and intangible assets (such as software applications and data). This register should accurately reflect the current operational environment.

Regular Updates and Verification: The asset register should be regularly updated to reflect new acquisitions, changes, or disposals of assets. Regular verification ensures that the register accurately reflects the current state of assets.

Security Classification and Control: Classify assets based on their criticality and sensitivity in accordance with the UK Government Security Classification Policy. Implement relevant security controls for each asset, as per the relevant classification, to protect against unauthorised access, use, modification, destruction, or theft.

Integration with Risk Management: Link the asset register with the organisation's risk management processes this will help understanding which assets are critical and helps in prioritising risk mitigation efforts and resource allocation.

Access Control and Accountability: Restrict access to the asset register to authorised personnel only. Establish accountability by assigning responsibility for the accuracy and integrity of the asset register.

Example:

The asset register should include detailed listings of all computer systems, communication devices, databases, and software applications used for operations. For instance, the register would document the specifications, location, and security measures of each server storing sensitive case files. Regular audits should be conducted to ensure that all assets are accounted for and that any changes or updates to these assets are accurately reflected. This documentation should be integrated into the agency's broader risk management strategy, ensuring that critical assets, especially those holding confidential information, receive the highest level of security attention and resource allocation.

3.5. Resilient System Design

This is focused on designing systems that are resilient against various types of cyber threats and can maintain functionality even under adverse conditions. Resilient system design is about anticipating potential threats and vulnerabilities and incorporating features and strategies that allow the system to withstand and quickly recover from cyber incidents. This includes implementing redundancy, failover mechanisms, and robust security measures to ensure system availability and integrity.

COPYRIGHT: Police Digital Services

NIST SP 800-53's CP-2 can be followed as this control provides a structured approach to ensuring that systems are designed with contingency and recovery in mind, making them resilient against various disruptions and capable of maintaining critical operations under adverse conditions.

Guidance:

Plan for Threats: Design systems with a mindset that expects security threats. This involves understanding the threat landscape and incorporating features that can mitigate these risks.

Redundancy and Failover: Implement redundant systems and failover mechanisms to ensure system availability and continuity of operations in case of a failure or attack.

Robust Security: Embed comprehensive security measures into the system's design, including strong encryption, secure authentication protocols, and network security controls.

Regular Vulnerability Assessments and Updates: Conduct regular vulnerability assessments to identify and address weaknesses in the system. Ensure that the system is regularly updated to protect against new and emerging threats.

Design for Scalability and Flexibility: Create a system architecture that is scalable and flexible, allowing for quick adaptation and updates in response to evolving security threats.

Example:

Consider a public safety communication network used by emergency services. A resilient design for such a system should include redundant communication channels and data centres to ensure continuous operation during emergencies, even if one channel or centre is compromised. The network should employ end-to-end encryption to secure sensitive communications and have the capability to quickly switch to backup systems in case of a cyberattack. Additionally, the system should be designed to scale up during high-demand situations, such as natural disasters, and adapt to new security protocols as threats evolve.

Follow the **NCSP Business Continuity standard** and use guidelines such as NIST SP 800-53's CP-2 to develop a comprehensive contingency plan that includes redundant communication systems, backup data centres, and protocols for rapid recovery and reestablishment of communications during emergencies. This plan should be tested regularly and updated to adapt to new threats and system changes, ensuring the resilience and reliability of the communication network.

COPYRIGHT: Police Digital Services

3.6. Coding Security

This section highlights the importance of identifying and addressing vulnerabilities within the codebase of a system to prevent potential security breaches and system failures. It encourages secure coding practices, regular code reviews, and the use of automated tools to detect and rectify security flaws.

NIST SP 800-53's SA-11 control can be used for further guidance as this provides a structured framework for integrating security testing and evaluation throughout the software development process, ensuring that code security is a fundamental aspect of system development and maintenance.

Guidance:

Secure Coding Practices: Highlight the use of secure coding standards and guidelines to minimise vulnerabilities. Developers should be trained in secure coding techniques and be aware of common security pitfalls in coding.

Conduct Regular Code Reviews: Implement a process for regular code reviews, involving peers or security experts, to identify and fix potential security issues in the code.

Automated Security Scanning Tools: Employ automated tools, such as static application security testing (SAST) and dynamic application security testing (DAST), to continuously scan the code for vulnerabilities.

Vulnerability Remediation: Establish a process for promptly addressing any identified vulnerabilities and ensuring they are rectified and re-tested before the software is deployed.

Integrate Security into the SDLC: Security should be a consideration at every stage of the software development lifecycle, from initial design to deployment and maintenance.

Example:

Applying secure coding practices is critical. The development team could use SAST tools to scan the code in the development phase, identifying vulnerabilities like buffer overflows or insecure cryptographic practices. Following this, DAST tools could be used in a representative test environment to replicate real-world attacks on the application, discovering issues like session hijacking or insecure server configurations. All findings from these tests, along with the outcomes of manual code reviews, should be accurately documented and addressed. This approach is recommended by NIST SP 800-53's SA-11 control as it ensures that the system's code is tested throughout development phases resulting in safeguarding the system's integrity and reliability.

COPYRIGHT: Police Digital Services

3.7. System Functionality and Security

This section highlights the need for systems to function as per requirements while meeting all agreed security controls and ensuring the security of information. This is fundamental in ensuring that the system's operational performance and security posture are in line and do not negatively impact each other.

This highlights the importance of validating that the system adheres to security protocols to protect against threats and vulnerabilities and at the same time achieves its functional objectives.

Guidance:

Alignment with Functional and Security Objectives: Regularly verify that the system meets its functional requirements without compromising security standards. This includes balancing operational efficiency with robust security measures.

Continuous Testing: Implement a routine of continuous testing of both functional and non-functional requirements of the system including the security aspects. This process should involve identifying and fixing any deviations from expected performance or security breaches.

Maintain Information Security: Prioritise the safeguarding of information within the system. Ensure that data protection measures are in place and effective, aligning with confidentiality, integrity, and availability principles. Keep the system up to date with regular updates and patches, especially those addressing security vulnerabilities, to ensure ongoing protection and optimal performance.

Stakeholder Feedback and Involvement: Engage with stakeholders early, involve end-users in the testing and evaluation process to gather feedback on both the functional and non-functional aspects including security.

Example:

In a system with large database, it is essential that the system not only efficiently processes and retrieves data as required but also ensures the highest level of data security. This should involve routine testing for both operational performance (such as query response times) and security aspects (like access control and data encryption). Regular updates should be applied to address any new vulnerabilities or functional enhancements, and feedback from end users should be gathered to ensure the system continues to meet both its functional and security objectives effectively.

COPYRIGHT: Police Digital Services

3.8. Protecting Test Data

This section focuses on the best practices for managing test data. A careful and responsible approach should be adopted when handling test data. The use of synthetic data and conducting a Data Privacy Impact Assessment (DPIA) where necessary, ensures that system testing is thorough and meets security requirements. **It is essential to consult with local Data Protection Officers or equivalent prior to the use of Personal Data as test data.**

Guidance:

Data for Testing: Use anonymised, randomised, or pseudo-anonymised data in place of actual PII. Anonymisation involves stripping away identifiable information, while pseudo-anonymisation replaces private details with fictitious, yet realistic, replacements. Randomised data, generated to mimic real data patterns, can also be effective for testing purposes.

DPIA when Using Real PII: In rare scenarios where the use of real PII is unavoidable for certain tests, conduct a DPIA and consider legitimate interests as part of the DPIA. This assessment should identify and evaluate privacy risks and determine measures to address these risks effectively.

Robust Protection Measures: If real PII or sensitive data is necessary for testing, implement stringent data protection measures, the security controls should be the same as production environment. This includes deploying encryption techniques, setting strict access controls, protective monitoring, regular patching and continuously monitoring the data usage. This is also recommended by NIST SP 800-53 AC-19 which implies that access to test data should be carefully managed and restricted to authorised personnel and may involve encrypting the test data or ensuring it is used only in secure and controlled environments.

Compliance with Data Protection Laws: Ensure that handling of sensitive data in test environments adheres to relevant privacy laws and regulations (i.e., GDPR). This compliance is crucial to avoid legal and ethical implications.

Data Leak Prevention: NIST Cybersecurity Framework (CSF) control PR.DS-5 provides guidance on measures to prevent data leaks this involves ensuring that test data, especially if it replicates or derives from real user data, is handled in a manner that prevents accidental exposure or leakage.

Integrating Best Test Practices: International Software Testing Qualifications Board (ISTQB) provides guidelines and best practices regarding various aspects of software testing, including the management and use of test data. Adopt ISTQB's recommendations in combination with relevant security controls like PR.DS-5 when creating and managing test data. Ensure that test data is relevant, covers a wide range of scenarios, and is managed effectively to maintain its integrity throughout the testing process.

COPYRIGHT: Police Digital Services

Example:

In a scenario where a police force is developing a new platform that includes public engagement and participation, testing the platform's capabilities requires data that simulates actual public interactions. Instead of using real public data, the development team opts for pseudo-anonymised data, where details are replaced with fictional yet realistic data. This approach allows comprehensive testing without compromising public's privacy. If a particular test requires the use of actual public data, a DPIA is conducted to rigorously assess privacy implications and to establish appropriate safeguards, such as data masking and strict access controls. In this case the test environment should be secured with same level of controls and processes as live environment.

3.9. System Testing and Live Environment Integration

The NCSP Information Assurance standard and best practices as outlined in NIST SP 800-53 SA-11 highlight the importance of deploying only those system versions into the live environment that have undergone thorough testing and received formal approval by all relevant departments including security. This step is critical in ensuring that the systems put into operation are free from known vulnerabilities and meet established security standards. See the **NCSP Information Assurance standard**

Guidance:

Rigorous Security Testing: Before any system version is released into the live environment, it must undergo extensive security testing, this includes vulnerability assessments, penetration testing, and security reviews to identify and remediate any potential security issues. See also penetration testing and IT health checks guidance.

Representative Test Environment: Establish a test environment that is isolated from the production environment but replicates its configuration as closely as possible. This is important to accurately assess how the system version will perform in production, both in terms of functionality and security. As recommended by ISTQB, the test environment setup, management, and maintenance are essential for ensuring that testing is effective, accurate, and reflective of real-world operational conditions.

Remediation of Identified Vulnerabilities: Any vulnerabilities or weaknesses discovered during testing should be remediated in accordance with timescales described in the NCSP vulnerability management standard. The NIST SP 800-53 SA-11 suggests integrating this process within the system development lifecycle to ensure effective and timely resolution of security issues. See the **NCSP Vulnerability Management standard.**

COPYRIGHT: Police Digital Services

Formal Approval Process: Implement a formal approval process for all system versions. This process should involve a review of the security testing results and a sign-off from authorised personnel, confirming that the system version meets all necessary security criteria.

Change Management Integration: Coordinate the deployment of new system versions with the organisation's change management processes. This ensures that all changes are tracked, managed, and communicated effectively.

Continuous Monitoring Post-Deployment: Once deployed, continue to monitor the system version in the live environment for any emerging threats or vulnerabilities, adapting security measures as needed. See the **NCSP Vulnerability Management standard.**

Example:

An agency is developing a new online service platform to handle users' requests and queries. In line with above, the platform must only be deployed in the live environment after thorough security testing and formal approval.

During the development phase, the team follows NIST SP 800-53 SA-11 guidelines by conducting comprehensive security testing. This includes using automated tools like SAST for early detection of vulnerabilities in the code and DAST to assess the application in a running state. Additionally, manual methods such as penetration testing and code reviews are employed to ensure a thorough evaluation of the platform's security. Given that the platform handles sensitive user data, the team implements measures aligned with ISO 27002:2022 Control 8.19. This includes deploying Data Loss Prevention (DLP) technologies to prevent information leakage and ensuring that all data transmissions are encrypted. Before deployment, the platform is rigorously tested in a representative test environment that closely mimics the live environment. This ensures that the platform's performance and security behaviour in the test environment will reflect the production configuration.

After successful security testing and ensuring compliance with relevant standards, the platform undergoes a formal approval process. This includes a review of all testing documentation and a sign-off from relevant stakeholders including the information security officer. Once deployed, the platform is continuously monitored for new vulnerabilities or security breaches. This ongoing observation is in line with the principles of both NIST and ISO standards, ensuring the platform remains secure and functional for use.

This process ensures that the new online service platform is robustly secure, compliant with security standards, and functions effectively, providing a secure and reliable service.

COPYRIGHT: Police Digital Services

4. Operate, Embed & Close

This section addresses the operational aspects of systems post-deployment, ensuring their continuous and secure functioning within the live environment. This covers importance of maintaining the security and performance of systems during their operational phase are addressed including regular monitoring for security threats, implementing updates and patches, and conducting routine maintenance to ensure systems remain secure and functional. It also highlights the integration of new systems into existing business processes and infrastructures ensuring that systems are not only technically working but also aligned with business objectives and user needs.

As systems evolve or as new threats emerge, changes may be required, these changes need to be managed and implemented securely and efficiently, without disrupting business operations using an effective change management process. This includes preparing for and managing security incidents by having plans and processes in place for incident response, data recovery, and business continuity to reduce the impact of any security breaches or system failures.

Finally, Section 4 addresses the end-of-life processes for systems. This includes securely decommissioning systems, ensuring that all sensitive data is properly erased or migrated, and that all components are disposed of or recycled in accordance with relevant policies and environmental regulations.

4.1. Change Management for New Systems

This section underlines change management process specifically for the introduction of new systems or significant updates to existing systems. It highlights the importance of managing these changes carefully to minimise disruption to operational or live environments and to ensure the seamless integration of the new systems or updates. It involves a structured approach to change management, considering the potential impacts on various stakeholders and the overall organisation.

The importance of a structured and strategic approach to change management for new systems is to ensure that changes are implemented smoothly and effectively with minimal disruption to the organisation's operations.

Guidance:

Follow the guidance as detailed in section **3.2 "Managed Change Control".**

4.2. Managing Business Assets Throughout Lifecycle

This section focuses on the comprehensive management of business assets throughout their entire lifecycle and highlights the importance of effectively managing assets from acquisition to disposal, ensuring they are used efficiently and securely while in operation, and securely decommissioned at the end of their life. This includes various aspects such as tracking, maintenance, security, and eventual secure disposal or transfer of assets.

Guidance:

Asset Lifecycle Management: Implement a lifecycle management approach for all assets. This includes planning for procurement, operational use, maintenance, and eventual disposal or transfer. See the **NCSP Physical Asset Management standard.**

Asset Tracking and Inventory: Maintain an accurate and up-to-date inventory of all business assets. This inventory should include details such as asset location, responsible personnel, and the status of the asset throughout its lifecycle while keeping in compliance with relevant GDPR standards like data minimisation.

Regular Maintenance and Security: Ensure regular maintenance of assets to keep them in optimal working condition. Use appropriate security measures including encryption and access control, to protect against data breaches and unauthorised access to protect assets from theft, loss, or misuse. The security measures should include both physical security and cybersecurity controls.

Risk Management and Compliance: Assess and manage risks associated with business assets, including compliance with relevant regulations and standards. Conduct Data Protection Impact Assessments (DPIAs) as part of regular risk management for data assets. This is essential for identifying potential risks to personal data and implementing appropriate mitigations.

Ensure that data collection and processing activities are in strict compliance with relevant regulations like GDPR. This includes ensuring data is processed only for specified and lawful purposes.

Responsible Decommissioning and Disposal: Establish procedures for the responsible decommissioning and disposal of assets. Ensure that sensitive data is securely erased from digital assets, and that physical assets are disposed of in a secure and environmentally responsible manner. See the **NCSP Physical Asset Management standard** which describes the requirements for the secure destruction of data, ensuring that organisations responsibly manage the end-of-life for data in a way that protects sensitive information and complies with legal and regulatory obligations.

COPYRIGHT: Police Digital Services

Example:

A technology department manages a wide range of assets, including hardware, networking equipment, and information assets and should implement a comprehensive asset lifecycle management strategy to ensure efficient and secure management of these assets.

A lifecycle management plan should be developed for each type of IT asset. For server hardware and networking equipment, this includes schedules for upgrades, performance reviews, and eventually phase out plans. For software and information assets, the lifecycle plan should cover version updates, license management, and data archiving or deletion processes. In managing code as an asset, a version control system should be used ensuring that all changes and iterations of software products are tracked and managed efficiently from development to deployment.

An inventory management system should be maintained to track the status, location, and responsible personnel for each asset. The system should be regularly updated to reflect new purchases or changes in asset status. For data assets, they ensure compliance with GDPR principles, particularly focusing on data minimisation.

All physical IT assets should undergo routine maintenance to ensure optimal performance. In terms of information & data assets, regular security audits and updates should be conducted. Robust security controls should be implemented, including firewalls, intrusion detection systems, and data encryption, to protect against breaches and control access. For digital assets like code, continuous integration/continuous deployment (CI/CD) pipelines can be implemented to automate testing and deployment and integrating security checks to identify vulnerabilities early.

DPIAs should be routinely conducted for systems and processes involving sensitive information assets like personal data, to identify and mitigate privacy risks in compliance with relevant standards and guidelines like GDPR.

When IT hardware reaches the end-of-life, a secure decommissioning process must be followed. This includes clearing all sensitive data from storage devices in accordance with the NCSP Physical Asset Management standard before securely disposing of the hardware. For information assets, data must be securely erased or archived, depending on its classification and data retention policy. See the NCSP Information Management standard.

Following relevant standards and guidelines like NIST and GDPR ensures that assets, both physical and digital, are managed effectively throughout their lifecycle, from procurement and operational use to secure decommissioning.

COPYRIGHT: Police Digital Services

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.
- 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 guideline 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 guideline 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.)

COPYRIGHT: Police Digital Services

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Tahir Chowdhory	Initial Version for internal review	09/11/23
0.2	Tahir Chowdhory	Updated following peer review	23/11/23
0.3	Tahir Chowdhory	Updated following team review	12/12/23
0.4	Tahir Chowdhory	Updated following NCSWG comments	16/01/24

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	07/02/2024

COPYRIGHT: Police Digital Services

Document References

Document Name	Version	Date
NPCC National Community Security Policy (NCSP)	v1.3	09/2023
NPCC NCSP System Development standard	v1.0	09/2023
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
NIST Special Publication 800-53 Revision 5	v5	04/2023
IRAM2 SCOPING AND BIA ASSISTANT	v017	07/2017

COPYRIGHT: Police Digital Services