# Secure Development Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. OWASP: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist>
2. SEI CERT: [https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards](https://wiki.sei.cmu.edu/confluence/display/seccode/SEI%2BCERT%2BCoding%2BStandards)
3. NIST 800-218: <https://www.cisa.gov/resources-tools/resources/nist-sp-800-218-secure-software-development-framework-v11-recommendations-mitigating-risk-software>
4. ISO/IEC 17961: <https://www.iso.org/standard/61134.html?browse=tc>
5. ISO/IEC 27001:2022: A.8.25, A.8.26, A.8.28, A.8.29, A.8.31, A.8.33
6. NIST 800-53 rev. 5: AC-20, CM-5(5), IA-5(2), PL-2, SA-3, SA-4, SA-11, SA-15, SA-15(3), SC-8, SC-18, SC-23, SC-39, SI-2, SI-10, SI-11
7. CIS v8: 16.1, 16.2, 16.8, 16.9, 16.10, 16.11, 16.12
8. PCI DSS 4.0: 1.4.2, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.4.3, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 8.2.7, 8.6.2, 11.1.1, 11.6.1
9. AICPA SOC 2 TSC: CC2.1, CC5.2, CC6.1, CC6.7, CC7.1, CC8.1, PI1.1, PI1.3

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Secure Development Policy is to establish a comprehensive framework that ensures the security, integrity, and privacy of software applications developed and maintained by the organization. By integrating security practices throughout the software development life cycle (SDLC), this policy aims to mitigate risks, protect sensitive information, and ensure compliance with relevant laws, regulations, and industry standards. The policy seeks to provide clear guidelines for development teams, ensuring that security and privacy considerations are an integral part of the development process from inception to deployment and maintenance.

## Scope

This policy applies to all software development activities conducted by the organization, including those performed by employees, contractors, and third-party vendors. It encompasses all phases of the SDLC, including planning, design, implementation, testing, deployment, and maintenance. The policy covers the development of web applications, APIs, and other software systems, and is applicable to all environments, including development, staging, production, and test environments. Additionally, this policy mandates the use of secure coding practices, regular code reviews, comprehensive testing, and security measures to protect against common threats and vulnerabilities.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Development Teams**: Groups of individuals responsible for the design, development, and maintenance of software applications.
	2. **Secure Software Development Life Cycle (SDLC)**: A process that integrates security practices into each phase of software development, including planning, design, implementation, testing, deployment, and maintenance.
	3. **Threat Modeling**: A systematic approach to identifying and evaluating potential security threats and vulnerabilities in a system.
	4. **Secure Coding Standards**: Guidelines and best practices for writing code that minimizes security vulnerabilities and protects against common threats.
	5. **Error Handling**: Mechanisms for managing errors in a way that does not expose sensitive information and helps in debugging and maintaining software security.
	6. **Session Management**: Practices that ensure the secure creation, maintenance, and termination of user sessions to prevent unauthorized access.
	7. **Environments**: Distinct settings for different stages of software development, including development, staging, production, and optional test environments, each with tailored access controls and security measures.
	8. **Quality Assurance (QA) Teams**: Groups responsible for testing software to ensure it meets quality, security, and privacy standards before deployment.
	9. **Penetration Testing**: Simulated cyberattacks on a system to identify and fix security vulnerabilities.
	10. **Vulnerability Assessments**: Evaluations to identify weaknesses in a system that could be exploited by attackers.
	11. **Anonymized Data**: Data that has been processed to remove personally identifiable information, making it impossible to trace back to an individual.
	12. **Synthetic Data**: Artificially generated data that mimics real-world data, used for testing purposes without compromising actual user information.
	13. **Code Reviews**: The process of systematically examining code to find and fix vulnerabilities, ensure adherence to coding standards, and improve overall code quality.
	14. **Cross-Site Scripting (XSS)**: A type of security vulnerability where an attacker injects malicious scripts into web pages viewed by others.
	15. **Cross-Site Request Forgery (CSRF)**: An attack that tricks a user into performing actions on a web application without their knowledge or consent.
	16. **SQL Injection**: A code injection technique that exploits vulnerabilities in an application's software by inserting malicious SQL queries.
	17. **Security Headers**: HTTP response headers that enhance the security of web applications by enabling or disabling certain features and protections.
	18. **API (Application Programming Interface)**: A set of rules and tools for building software applications, allowing different programs to communicate with each other.
	19. **Authentication**: The process of verifying the identity of a user or system.
	20. **Authorization**: The process of determining whether a user or system has permission to access a resource.
	21. **Encryption**: The process of converting data into a coded format to prevent unauthorized access.
	22. **Automated Tools**: Software applications used to automatically identify and remediate security vulnerabilities during the development process.
	23. **Security Audits**: Systematic evaluations of software systems to ensure compliance with security policies and standards.
	24. **Security Checkpoints**: Specific stages in the SDLC where security practices and assessments are conducted to identify and mitigate risks.

## Policy

#### Specifications for Security and Privacy in Development

The [responsible party] shall:

* + 1. Incorporate security and privacy requirements from the outset of the development process.
		2. Perform threat modeling to identify potential security risks and mitigation strategies.
		3. Ensure compliance with relevant laws, regulations, and standards related to security and privacy.

#### Secure Software Development Life Cycle (SDLC)

The [responsible party] is required to:

* + 1. Integrate security checkpoints at each phase of the SDLC, including planning, design, implementation, testing, deployment, and maintenance.
		2. Conduct regular security assessments and audits throughout the development process.
		3. Use automated tools to identify and remediate security vulnerabilities early in the development cycle.

#### Secure Coding and Use of Secure Coding Checklists

The [responsible party] shall:

* + 1. Adhere to established secure coding standards such as OWASP, CERT, or SANS.
		2. Utilize secure coding checklists to ensure consistency and completeness in addressing common security issues.
		3. Receive regular training on secure coding practices and emerging security threats.

#### Error Handling

The [responsible party] is required to:

* + 1. Implement error-handling mechanisms that do not expose sensitive information.
		2. Log errors in a manner that aids debugging while protecting confidential data.
		3. Ensure that error messages provide no information that could be exploited by attackers.

#### Protection of Sessions

The [responsible party] shall:

* + 1. Implement secure session management practices, including the use of strong session identifiers.
		2. Ensure sessions are encrypted and that session data is protected from unauthorized access.
		3. Implement mechanisms to prevent session fixation, hijacking, and other session-based attacks.

#### Use of Separate Environments

The [responsible party] shall:

* + 1. Use distinct environments for development, staging, and production to prevent cross-contamination and ensure data integrity.
		2. Optionally use a separate test environment to validate software under different conditions.
		3. Ensure each environment has its own access controls and security measures tailored to its specific use.

#### Software Testing for Quality, Security, and Privacy

The [responsible party] is required to:

* + 1. Conduct testing, including functional, performance, and security tests, before software is deployed.
		2. Include security and privacy criteria in test plans and perform penetration testing and vulnerability assessments.
		3. Ensure testing results are documented and that identified issues are resolved prior to release.

#### Test Data

The [responsible party] shall:

* + 1. Use anonymized or synthetic data in testing environments to protect real user data.
		2. Ensure test data accurately reflects real-world scenarios to validate software functionality and security.
		3. Regularly review and update test data to maintain its relevance and effectiveness.

#### Code Reviews

The [responsible party] is required to:

* + 1. Perform regular code reviews to identify and remediate security vulnerabilities and ensure adherence to coding standards.
		2. Use peer reviews, automated code analysis tools, and security audits to maintain code quality.
		3. Document and track issues identified during code reviews to ensure they are addressed before deployment.

#### Web Application Security

The [responsible party] shall:

* + 1. Implement security measures to protect web applications from common threats such as XSS, CSRF, and SQL injection.
		2. Use security headers and ensure secure communication channels (e.g., HTTPS) are enforced.
		3. Conduct regular security assessments and update web applications to address emerging threats.

#### API Security

The [responsible party] is required to:

* + 1. Implement robust authentication and authorization mechanisms for APIs.
		2. Ensure data transmitted via APIs is encrypted and protected from unauthorized access.
		3. Regularly test APIs for vulnerabilities and ensure they comply with security best practices.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |