|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Secure Coding** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

Government organizations are under constant cyber-attacks that attempt to exploit vulnerabilities within computer systems and thereby threaten the confidentiality, integrity, and availability of information. A large number of vulnerabilities that are successfully exploited are due to software coding weaknesses and coding implementation flaws.

The objective of this coding standard is to ensure that code written is resilient to high-risk threats and to avoid the occurrence of the most common coding errors which create serious vulnerabilities in software. While it is impossible to write code that is completely impervious to all possible attacks, implementing these coding standards throughout information systems will significantly reduce the risk of disclosure, alteration or destruction of information due to software vulnerabilities.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

As per the Information Security Policy, all software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.

The items enumerated in this standard are not an exhaustive list of high-risk attacks and common coding errors but rather a list of the most damaging and pervasive. Therefore, code written must contain mitigating controls not only for the items specifically articulated in the standard below, but also for any medium and high-risk threats that are identified during a system’s life cycle.

* 1. High Risk Vulnerabilities

High risk threats include, but are not limited to:

1. Code Injection
2. Cross-site scripting (XSS)
3. Cross-site request forgery (CSRF)
4. Information leakage and improper error handling
5. Missing Authentication for Critical Function
6. Missing Encryption of Sensitive Data
7. URL Redirection to Untrusted Site ('Open Redirect')
   1. Vulnerability Lists
8. At a minimum, code must eliminate or mitigate the threats identified in the current version of the [Open Web Application Security Project (OWASP) Top 10 Most Critical Application Security Risks (‘OWASP Top 10’)](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) and the [Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors (‘CWE/SANS Top 25’)](http://cwe.mitre.org/top25/) publications (see [Appendix A](#AppendixA))
9. Both OWASP and CWE/SANS periodically reissue their respective lists based on changes in vulnerability and exploitation patterns. Developers are required to independently remain aware of updates to these lists and incorporate any new recommendations.
   1. Secure Libraries and APIs

Use of common security control libraries and common API’s, that have undergone security testing, is required to ensure a consistent approach that minimizes defects and prevents exploitation. When available, publicly available or vendor-supplied libraries or APIs should be used unless there’s a business case developed and exception granted by the [Policy Authority] evelop a custom library.

* 1. Code Review

1. To prevent defects or detect and remove them early, thereby realizing significant cost and schedule benefits to the entity, code must be checked for errors throughout development and during maintenance.
2. Entities must verify that the software assurance model used by the vendor is in line with this standard through vendor assurances, security testing and/or contract requirements.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[Open Web Application Security Project (OWASP) Top 10 Most Critical Application Security Risks (‘OWASP Top 10’)](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project" \t "_blank)

[Open Web Application Security Project (OWASP) Developer Cheat Sheets](https://www.owasp.org/index.php/Cheat_Sheets)

[Open Web Application Security Project (OWASP) Enterprise Security API](https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=Home)

[Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors ‘CWE/SANS Top 25’)](http://cwe.mitre.org/top25/)

[Common Weakness Enumeration (CWE) List](http://cwe.mitre.org/data/index.html)

[Carnegie Mellon Software Engineering Institute CERT Secure Coding Standards](http://www.cert.org/secure-coding/research/secure-coding-standards.cfm?" \t "_blank)

**Appendix A: Coding Resources**

**Open Web Application Security Project (OWASP)**

The OWASP Top 10 is authored by OWASP, an open-source application security community project which aims to raise security awareness of web application security risks. Although OWASP is focused on web application security, the standards and controls presented by this organization are generally also applicable to non-web based information systems.

In addition to the “Top 10” list, OWASP also produces the [Enterprise Security API (ESAPI) library](https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=Home) and [developer cheat sheets](https://www.owasp.org/index.php/Cheat_Sheets). The ESAPI library is an open source, web application security control library designed to mitigate risks to web applications. The ESAPI library provides a framework to implement code to address the risks listed within the OWASP Top Ten project. The cheat sheets provide a concise collection of high value information on specific web application security topics.

Additional information regarding OWASP, the ESAPI library and the Top Ten project is available at <https://www.owasp.org/>.

**Common Weakness Enumeration/SANS**

The CWE/SANS Top 25 Most Dangerous Software Errors publication is the result of collaboration between the SANS Institute, MITRE, and many top software security experts in the US and Europe. The publication is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The MITRE website provides detailed guidance to software programmers for mitigating and avoiding each of the common weaknesses enumerated within the Top 25 list with the [Common Weakness Enumeration (CWE) List](http://cwe.mitre.org/data/index.html).