



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S13-002
IT Standard: Secure Coding	Updated: 9/11/2018
	Issued By: NYS Office of Information Technology Services Owner: Chief Information Security Office

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 for New York State 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 the State's information systems will significantly reduce the risk of disclosure, alteration or destruction of the State's information due to software vulnerabilities.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines.](#)

3.0 Scope

This standard applies to all “State Government” entities as defined in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law (“State Entities”), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. Where a conflict exists between this standard and a State Entity’s standard, the more restrictive standard will take precedence.

This standard covers all systems and applications developed for the SE, regardless of their current system life cycle phase. This includes all test, quality control, production and other ad-hoc systems that exist within or external to the State network. This standard equally applies to SE systems that are developed by third-party entities with or without the participation of State development staff. It is the responsibility of the SE to ensure vendor supplied software, including custom or commercial off the shelf, is built securely.

4.0 Information Statement

As per the [NYS Information Security Policy](#), NYS-P03-002, all software written for or deployed on SE 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 for the SE 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.

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')

At a minimum, SE 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 \('OWASP Top 10'\)](#) and the [Common Weakness Enumeration \(CWE\)/SANS Top 25 Most Dangerous Software Errors \('CWE/SANS Top 25'\)](#) publications (see [Appendix A](#)).

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 into the SE's code any new recommendations.

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, publically available or vendor-supplied libraries or APIs should be used unless there's a business case developed and exception granted by the Information Security Officer (ISO)/designated security representative to develop a custom library.

To prevent defects or detect and remove them early, thereby realizing significant cost and schedule benefits to the SE, code must be checked for errors throughout development and during maintenance.

SEs must verify that the software assurance model used by the vendor is in line with this standard through vendor assurances, SE security testing and/or contract requirements.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards 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, State Entities shall request an exception through the Chief Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S13-002
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

8.0 Revision History

This standard shall be subject to periodic review to ensure relevance.

Date	Description of Change	Reviewer
10/18/2013	Original Standard Release	Thomas Smith, Chief Information Security Officer
10/17/2014	Added reference to NYS Information Security Policy, technical correction of "cluster ISO" reference to "ISO/designated security representative"	Deborah A. Snyder, Acting Chief Information Security Officer
03/10/2017	Updated Scope, contact information and rebranded.	Deborah A. Snyder, Deputy Chief Information Security Officer
09/11/2018	Scheduled review – minor changes to Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer

9.0 Related Documents

[Open Web Application Security Project \(OWASP\) Top 10 Most Critical Application Security Risks \('OWASP Top 10'\)](#)

[Open Web Application Security Project \(OWASP\) Developer Cheat Sheets](#)

[Open Web Application Security Project \(OWASP\) Enterprise Security API](#)

[Common Weakness Enumeration \(CWE\)/SANS Top 25 Most Dangerous Software Errors \('CWE/SANS Top 25'\)](#)

[Common Weakness Enumeration \(CWE\) List](#)

[Carnegie Mellon Software Engineering Institute CERT Secure Coding Standards](#)

[US Department of Homeland Security Build Security In](#)

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](#) and [developer 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](#).