Information Network Security Agency (INSA)

Secure Website Management Standard

Version 1.0

2014 EC

Information Network Security Agency (INSA)

Secure Website Management Standard

Version 1.0

2014 EC

Forward

The growing reliance on the internet creates new opportunities, but also new challenges. Cyber criminals are growing more sophisticated, and they continue to create harmful software and discover new methods for compromising organizational websites. As a matter of fact, organizational websites in our country increasingly become the primary targets of online of adversaries. Therefore, to address this emerging challenges, this secure website management standard has been prepared for maintaining and improving the security of website management. The implementation of the standard requirements should be supported by Critical Mass Cyber Security Requirement and Secure Software Development and Management Standards based on the organization's objectives and security requirements.

Draft national policies, laws, standards, and strategies that enable to ensure the information and computer-based key infrastructures security and oversight their enforcement upon approval is one of the power and duties are given to the Information Network Security Agency (INSA).

Therefore, this standard is issued by Information Network Security Agency (INSA) pursuant to Article 13 of Information Network Security Agency Re-establishment proclamation Execution council of ministers Regulation No.320/2014.

Contents

Terminology and Acronyms

Terminology

The definitions of terminologies that are used in this standard are to be interpreted as described below.

- **Must**: This word means that the requirement is mandatory (an absolute requirement) of the standard.
- **Must Not**: This phrase means that the requirement is an absolute prohibition of the standard.
- **Should:** This word means that the requirement is "HIGHLY RECOMMENDED" to be implemented. There may exist valid reasons in particular circumstances to ignore a particular requirement, but the full implications must be understood and carefully weighed before choosing a different option. There must be a valid justification for ignoring the requirement or choosing a different option.
- **Should not:** This phrase means that the requirement is "NOT RECOMMENDED" to be implemented. There may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any requirement described with this label.
- **May:** This word, or the adjective "OPTIONAL", means that an item is truly optional.

Acronyms

Acronyms	Description
API	Application Programming Interface
CERRT	Cyber Emergency Readiness and Response Team
CI4A	Confidentiality, Integrity, Authentication, Authorization, Availability, and Accountability.
CMCSRS	Critical Mass Cyber Security Requirement Standard
CSS	Cascading Style Sheet
CSS	Cross-site Scripting
DEP	Data Execution Prevention
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INSA	Information Network Security Agency
PDF	Portable Document Format
RSS	Really Simple Syndication
SEO	Search Engine Optimization
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1. Introduction

Organizational websites provide a variety of services to enable organizations to achieve their mission. However, it is inherently vulnerable to various types of attacks and can cause to host malware and/or illegal content, as a stepping stone to attack the Organization's internal network, if it is inadequately designed, operated, and managed. To uphold the security of the organization's website, they should take appropriate proactive security measures on each website development and management. The design, implementation, hosting, operation, and management of a website should be steered in a standardized and secured manner so that the desired objective can be achieved.

The purpose of this standard is to provide minimum security requirements and measures that should be taken by organizations to meet the intended desire of their websites as organized requirement gathering and analysis, design, implementation, hosting, operation, and management with defined security requirements that must be considered under each focus area.

Thus, all government and key private organizations must meet the minimum security requirements defined in this standard.

1.1. Purpose

The standard pursues to assist government and key private organizations in integrating security features into their website design, implementation, hosting, operation, and management based on the services they provide. This standard also provides applicable requirements that should be taken to prevent the most common security threats to websites.

1.2. Scope

This standard will be applicable on Ethiopian federal and regional government and key private organizations of the country.

1.3. Objectives

- ➢ The main objective of the standard is to enhance the security of the website to enable the organizations to provide their services with acceptable security risks.
- ➢ To make government and key private organizations website's secured and standardized.

1.4. Principles

II. **Mission-oriented:** websites should reflect organizations' business requirement and they should be developed and managed in a way that helps organizations achieve their mission.

III. **Simplicity:** websites should be simple for users and administrators/managers.

IV. **Accessibility:** websites should be accessible at any time and place using any device.

V. **Risk-based:** the security controls implemented on websites should be based on thorough risk assessment results.

VI. **Integrate security**: security features should be integrated at each component of the website while designing, implementing, hosting, operating, and managing it.

2. Focus Areas

There are five focus areas that the standard emphases on in order to secure the website. Each of these focus areas have their own considerable security requirements that the organizations should implement. The requirements defined in this standard will enhance the website's security to fight cybercrime through development and management.

Implementation of the requirement should be supported by secure software development and management and critical mass cyber security requirement standards.

2.1. Requirement Gathering and Analysis

The objective of the requirement gathering and analysis is to organize, analyze, and reflect the intents of the organization's website while developing and managing.

A. The business requirement gathering should comprise the most fundamental issues that address the organization's missions, business objectives, and acceptable risk criteria.

B. The gathered organizational business requirement should be relevant and provide reliable information in alignment with the requirement A.

C. The requirement should include security objectives and needs of all relevant stakeholders.

D. The requirements should provide details of how the website should behave securely and specify what is needed to be done during design, implementation, hosting, operation, and management.

E. The requirements gathering document should address post implementation security needs of stakeholders such as about hosting, operation, and management of the website.

F. The requirement analysis should be unambiguous, and recorded as organizational asset.

G. Contracts with developers must consider the protection of the intellectual property of source code to protect organizational interests.

H. Security requirements must be approved by top management of the organization or relevant business owner.

2.2. Design

The objective of this focus area is to define considerable security requirements in website design.

A. The Website should be designed based on secure software development and management standard V.1 requirements.

B. The Website design document should be reviewed and approved by the respective responsible body of the organizations.

2.3. Implementation

The objective of this focus area is to provide security requirements for coding and testing of the website.

A. The Website should be implemented based on secure software development and management standard V.1 requirements.

B. Website developers should sufficiently be aware of security requirements of the organization.

C. Organizations must ensure that their website is awarded accreditation before hosted based on Critical Mass Cyber Security Requirement Standard Version 1.0.

D. The website must be audited before hosted based on the auditing Process defined in the Critical Mass Cyber Security Requirement Standard.

E. All documentation must adequately be protected from unauthorized access.

2.4. Hosting

The Website hosting security requirement intends to proactively manage security issues related to the hosting services.

A. The organization should prepare a comprehensive hosting security requirement document that comprises technical and non-technical issues before hosting its website.

B. Website hosting security requirements document should examine the hosting service provider's security capability in terms of technical parameters including but not limited to:

   i. Staff capability of hosting service provider

   ii. Network infrastructure security

   iii. System infrastructure security including the server operating system, hosting platform,

   iv. Implemented Communication encryption tools

v. Business continuity plan

vi. Disaster recovery capability

vii. Physical security.

C. Website hosting security requirements document should examine hosting service provider’s security capability in terms of non- technical parameters including but not limited to:

i. The most recent third-party security audit reports on the hosting service provider.

ii. Business processes of the hosting service provider

D. Government websites should be hosted on organization premises or on hosting entity infrastructure deployed in Ethiopia.

E. Separate comprehensive security agreements should be signed between the organization and the hosting service provider which comprise the following provisions.

i. Roles, Responsibility, and accountability of the contracting parties

ii. Breach handling procedures and responsibilities

iii. Exceptional events

iv. Expected service levels

v. Communication methods

vi. Not complying with National Standards, Regulations, and other related legal mandates

vii. Service contacts

viii. Data limits

ix. Bandwidth limits

x. downtime limits

xi. Domain namespaces scalability and changes

xii. Ability to unlink for any violations of law or regulation, breach or violation of any contract provisions

2.5. Operation and Management

The Objective of this focus area is to set requirements on how to manage all security anomalies faced during operations.

A. Organizations should have clear policy statements, to manage their organizational websites. Organizational Website policies should address at least the following points.

   i. Administrative Responsibilities.

   ii. Emergency communications.

   iii. Contents management

B. Organizations Website management and operation activities should be conducted based on documented procedures.

C. Website access rights provisions should be granted and revoked formally via documented procedures.

D. Website access privileges should be categorized based on business requirements and the website policy of the organization.

E. Organizational Access credentials should be updated in a fixed time frame and whenever there is change in structure or strategic mission.

F. Organizations should conduct security vulnerability and risk assessments on their website quarterly.

G. Additional security testing should be undertaken as deemed necessary by risk assessment reports.

H. Periodic testing and auditing should be performed to ensure the on-going effectiveness of website security controls as new threats emerge.

I. Website changes, including updates and patches, must be reviewed and tested to ensure that there is no adverse impact on the operation. This includes:

   i. Formal change control procedures must be established and documented, and evidence retained that the procedure is implemented and complied with;

   ii. Changes must be approved by the cyber security department.

J. When significant changes or enhancements are made, in advance operational risk assessment must be performed to consider the security implications of such changes

K. Website monitoring tools should be implemented to detect breaches or misuse of web applications.

L. The organization should have proper patch and configuration management plans for its website.

M. The patch and configuration management process must be tested on separate environment before implemented on the functional site.

N. The organizations should continuously ensure communication encryption certificate updates of its website.

O. The organization should follow and monitor periodic security updates and changes of the hosting service provider.

3. Annexes

Annex A:

Common vulnerabilities and threats of the website that must be considered during design, implementation, hosting, operation and management:

No	Vulnerability	Possible threats
1	SQL Injection	➢ Bypass login authentication ➢ Disclosure of sensitive data stored in the database ➢ system shutdown
2	Unchecked Path Parameter / Directory Traversal	➢ Disclosure of sensitive information ➢ Falsification and deletion of configuration files, data files and source codes
3	Improper Session Management	➢ Unauthorized access to personal information ➢ Webmail
4	Cross-Site Scripting	➢ Confusion caused by false information ➢ Disclosure of sensitive information through phishing attacks ➢ If the session ID is stored in the stolen cookie, it could lead to spoofing. ➢ If personal information is stored in the stolen cookie, the sensitive data would be disclosed.
5	CSRF (Cross-Site Request Forgery)	➢ Access the services normally available only for the users who have properly logged in.

		➢ Add and modify information normally permitted only for the users who have properly logged in
6	HTTP Header Injection	➢ When an HTTP Set-Cookie header is inserted, an arbitrary cookie is created and stored in the user's browser.
7	Mail Header Injection	➢ Used as a launching pad for the spam distribution.
8	Lack of Authentication and Authorization	➢ Disclosure of sensitive information

Annex B:

Minimum security testing of the website

No	**Deployment**	Pass	Fail
	Information Disclosure		
1.	Test for extraneous files in the document root		
2.	Test for extraneous directory listings		
3.	Test for accessible debug functionality		
4.	Test for sensitive information in log and error messages		
5.	Test for sensitive information in robots.txt		
6.	Test for sensitive information in source code		
7.	Test for disclosure of internal addresses		
	Privacy and Confidentiality		
8.	Test for sensitive information stored in URLs		
9.	Test for unencrypted sensitive information stored at the client-side		

10.	Test for sensitive information stored in (externally) archived pages		
11.	Test for content included from untrusted sources		
12.	Test for caching of pages with sensitive information		
13.	Test for insecure transmission of sensitive information		
14.	Test for non-SSL/TLS pages on sites processing sensitive information		
15.	Test for SSL/TLS pages served with mixed content		
16.	Test for missing HSTS header on full SSL sites		
17.	Test for known vulnerabilities in SSL/TLS		
18.	Test for weak, untrusted or expired SSL certificates		
19.	Test for the usage of unproven cryptographic primitives		
20.	Test for the incorrect usage of cryptographic primitives		
	State Management		
21.	Test for client-side state management		
22.	Test for invalid state transitions		
	Authentication and Authorization Process		
23.	Test for missing authentication or authorization		
24.	Test for client-side authentication		
25.	Test for predictable and default credentials		

26.	Test for predictable authentication or authorization tokens		
27.	Test for authentication or authorization based on obscurity		
28.	Test for identifier-based authorization/ Privilege escalation citation		
29.	Test for acceptance of weak passwords		
30.	Test for account recovery process		
31.	Test any “remember me” function		
32.	Test for fail-open conditions		
33.	Test any impersonation function/ re CAPTCHA		
34.	Test for plaintext retrieval of passwords		
35.	Test for username enumeration/ Test username uniqueness		
36.	Check for unsafe distribution of credentials		
37.	Test for missing rate limiting on authentication functionality		
38.	Test for missing re-authentication when changing credentials		
39.	Test for missing logout functionality		
40.	Test any multi-stage mechanisms		
	User Input Management		
41.	Test for SQL injection		
42.	Test for path traversal and filename injection		
43.	Test for cross-site scripting (Stored, DOM and reflected)		
44.	Test for system command injection		

45.	Test for XML injection		
46.	Test for XPath injection		
47.	Test for XSL(T) injection		
48.	Test for SMTP injection		
49.	Test for SSI injection		
50.	Test for HTTP header injection		
51.	Test for HTTP parameter injection		
52.	Test for native software flaws (buffer overflow, integer bugs, format strings)		
53.	Test for LDAP injection		
54.	Test for dynamic scripting injection		
55.	Test for regular expression injection		
56.	Test for data property/field injection		
57.	Test for protocol-specific injection		
58.	Test for expression language injection		
59.	Fuzz all request parameters		
60.	Test for arbitrary redirection		
	Session Management		
61.	Test for cross-site request forgery (CSRF)		
62.	Test for predictable CSRF tokens		
63.	Test for missing session revocation on logout		

64.	Test for missing session regeneration on login		
65.	Test for missing session regeneration when changing credentials		
66.	Test for missing revocation of other sessions when changing credentials		
67.	Test for missing Secure flag on session cookies		
68.	Test for missing HttpOnly Flag on session cookies		
69.	Test for non-restrictive domain on session cookies		
70.	Test for non-restrictive or missing path on session cookies		
71.	Test for predictable session identifiers		
72.	Test for session identifier collisions		
73.	Test for session fixation		
74.	Test for insecure transmission of session identifiers		
75.	Test for external session hijacking		
76.	Test for missing periodic expiration of sessions		
77.	Check for disclosure of tokens in logs		
	File Upload		
78.	Test for storage of uploaded files in the document root		
79.	Test for execution or interpretation of uploaded files		
80.	Test for uploading outside of designated upload directory		
81.	Test for missing size restrictions on uploaded files		
82.	Test for missing type validation on uploaded files		

	Content		
83.	Test for missing or non-specific content type definitions		
84.	Test for missing character set definitions		
85.	Test for missing anti content sniffing measures		
	XML Processing		
86.	Test for XML external entity expansion		
87.	Test for external DTD parsing		
88.	Test for extraneous or dangerous XML extensions		
89.	Test for recursive entity expansion		
	Deployment		
90.	Test for missing security updates		
91.	Test for unsupported or end-of-life software versions		
92.	Test for HTTP TRACK and TRACE methods/ dangerous Methods		
93.	Test for extraneous functionality		
94.	Test for default credentials		
95.	Test for Bugs in web server software		
	Miscellaneous		
96.	Test for missing anti-clickjacking measures		
97.	Test for open redirection		
98.	Test for insecure cross-domain access policy		

99.	Test for missing rate limiting on e-mail functionality		
100.	Test for missing rate limiting on resource intensive functionality		
101.	Test for inappropriate rate limiting resulting in a denial of service		
102.	Test for application- or setup-specific problems		

4. Reference

1. National Institute standards and Technology (NIST), Special Publication 800-95 –Guide to Secure Web Services.
2. INSA, 2009 E.C, Critical Mass Cyber Security Requirement Standard.
3. Government of South Australia, web Application security Standard.

☎ +251-11-371-71-14
Fax: +251-11-3-20-40-37
✉ P.O.BOX: 124498
@ contact@insa.gov.et
www.facebook.com/INSA.ETHIOPIA
www.insa.gov.et
Addis Ababa
Ethiopia