Security Standard: Web

Introduction and Scope

This standard applies to all web servers, services and applications (RIT and 3rd party) using web-oriented protocols, such as APIs, on all platforms.

The standard excludes embedded web servers that are not within the scope of the server standard, e.g., printers and other hardware devices.

Student web sites, services, and applications are subject to this standard if they are on the RIT web environment and publicly accessible.

Requirements

The following security controls shall be implemented.

1. Compliance with Other Standards

1.1. All servers within the scope of this standard shall comply with the requirements of the Server Security Standard in addition to other relevant information security standards.

1.2. . This standard provides the security requirements component for the RIT Web Standard

2. Registration

2.1. The department, owner, developer, administrator, and host location of web servers and services shall be registered and updated as changes occur, and annually in the centralized registration system. The identified owner, developer, and administrator shall be an RIT employee.

3. Private Information Management

3.1. Private information shall not be stored on web servers unless there is a legitimate business purpose approved by the Divisional VP and a security review has been conducted.

4. Vulnerability Scanning & Penetration Testing

4.1. ITS will conduct vulnerability scans and penetration tests of the web environment and custom web applications on a regular recurring basis (in addition to the Server Standard requirements and includes applications). In environments where ITS cannot conduct a vulnerability scan and penetration test (e.g., google apps), a reputable third party vulnerability scan and penetration test is acceptable.

4.2. Critical and severe vulnerabilities (as defined in the Server Standard) shall be logged in a ticketing system or email and shall be remediated, have a false positive reported, or have an exception filed within 1 month. If a CVSS or vulnerability rating is not available (e.g., internally developed applications), the administrator shall consult with the Information security office to determine the impact to the university.

4.2.1 Any vulnerabilities found in web applications hosting private or confidential information shall be initially be treated as critical until a full assessment has been done.

4.3. Moderate vulnerabilities shall be logged in a ticketing system or email and shall be remediated, have a false positive reported, or have an exception filed within 1 month.

5. Threat Management

5.1. Web system administrators are responsible for determining whether to implement a web firewall and/or a web application firewall or IPS. Recommended rule sets are available from the Information Security Office wiki.

6. Essential Security Updates including Patching

6.1. Web servers, services, and applications shall be patched within 5 business days after critical security patches are made available. Other non-critical patches shall be evaluated and implemented based on the professional judgment of the server or application administrator.

6.2. Unpatched servers, services, and applications lacking critical security patches may be quarantined at the discretion of the CIO or Information Security Office.

6.3. Services and applications that no longer have vendor- or developer-provided security patches shall be remediated or removed.

7. Minimum Encryption Levels

7.1. Web services shall use, as a minimum, the ISO-approved encryption standards. Web services and applications shall follow encryption best practices listed on the Information Security web site.

8. Content Filtering

8.1. Web applications shall filter client input on the server following practices listed on the Information Security web site.

8.2. The use of world-writable files in web services and applications shall be minimized to follow the practice of least privilege.

8.3. Application owners are responsible for monitoring the content on their website.

8.4 Appropriate controls shall be implemented to prevent form abuse. Refer to the RIT Web Environment | Web Form Security Policy (reCAPTCHA/Honeypot)

9. Logging (not applicable to student websites)

9.1. Web application logging shall meet the requirements of the Servers, Server-based Applications and Databases Standard.

10. Access controls

10.1. Root, service account, administrator, and user accounts shall be different. The passwords for each account shall be unique. The accounts shall be used exclusively for the purpose for which they were created.

10.1.1. Web server-associated processes shall run only under their own unique account. These accounts shall not have root or administrator privileges.

10.1.2. All accounts shall be authorized to provide the minimal level of access required

10.2. Session Management

10.2.1. Upon authentication, a new session ID shall be generated by the web application

10.2.2 Session IDs shall not be transmitted in cleartext.

10.2.3 Password handling shall follow the requirements of the Account Management Standard (and A&A roadmap)

10.3. Configuration File Permissions and Access Control

10.3.1. Web Service/Application Administrators shall provide appropriate access controls for configuration files, following the principle of least privilege.

10.3.2. In order to prevent users from modifying the server configuration, Web Service/Application Administrators shall limit access to user-modifiable configuration files (e.g., .htaccess) according to a documented plan.

11. Development & Acquisition

11.1. Web server, service, and application development or acquisition shall meet the following requirements:

11.1.1 Follow documented development guidelines incorporating security or documented review process, including security best practices available on the Information Security website.

11.1.2 Follow a documented sustainable maintenance program including security.

11.1.3 Be executed by individuals with the training/education commensurate with their role.

11.1.4 Application development and acquisition must follow the requirements of the Solutions Life Cycle Management Standard.

12. Actions Taken in the Event of Risk of Harm

12.1. The CIO, ISO, or their designees have the authority to take any website (or portion thereof) offline that poses a risk of harm to the RIT web environment.

12.2. The Service Desk will manage the communication and implementation of de-provisioning and re-provisioning websites.

Resources/Related Information

- Standards Lexicon (definitions of terms used in standards)
- Roles and Responsibilities in relation to specific standards
- Exceptions/Non-Compliance—use of non-compliant portable media requires an exception request approved by the information trustee and the RIT Information Security Office.
- Related RIT Policies
  - Information Access and Protection Standard
  - Server Standard
  - Network Standard
  - Solutions Life Cycle Management Standard
  - Account Management Standard
  - RIT Web Environment | Web Form Security Policy (reCAPTCHA/Honeypot)

- ISO-approved encryption standards
- Client Input Filtering
- Firewall rule sets

Effective Date: June 30, 2018

Standard History:
May 15, 2008
September 15, 2011
November 11, 2013
October 19, 2015