Security Standard: Web
Effective September 1, 2008

1.0 Purpose
The intent of this standard is to ensure the security of RIT’s web infrastructure and web-based applications. The standard addresses significant and growing internal and external threats including, but not limited to:
  • Unauthorized use
  • Malicious code
  • Theft of confidential information

2.0 Scope
This standard applies to all web servers and services (RIT and 3rd party) using HTTP-based protocols that:
  • Use RIT authentication services, and/or
  • Disseminate or host Private, Confidential, or Operationally Critical Information.

NOTE: Web servers subject to this standard are also subject to the Server Security Standard.

3.0 Audience
The audience for this standard is administrators and information trustees of all RIT web servers/hosts and web-based applications.

4.0 Definitions
  Security Review
  A process by which an implementation is evaluated for secure use at RIT either by the Information Security Office or through a peer review system with prior notification to the ISO.

  Web Content
  Any file or stream consumed directly or indirectly via a web-oriented protocol

  Web Content Service
  Any software system running on a server with the purpose of delivering or facilitating web content, directly or mapped

  Private, Confidential or Operationally Critical Information
  Definitions for Private, Confidential, and RIT Operationally Critical Information are found in the Information Access and Protection Standard

  Web/Application Administrative Access
  Any access to the system for the purpose of system maintenance or modifying system configuration
RIT Authentication Services

RIT Authentication Services are the centralized services that verify the digital identity of a user by examining the user’s credentials. Common credentials include user name and password. User credentials permitting access to RIT networks should be treated as Confidential information.

5.0 Minimum Standard

The following security controls should be applied to, enabled, and running on all web servers/hosts and web-based applications no later than September 1, 2008, and all times thereafter.

5.1 General

5.1.1 All servers within the scope of this standard should comply with the requirements of the Server Security Standard.

5.1.2 On servers where Private or Confidential information resides alongside general access accounts, the web content services administrator should follow a documented plan for protecting Private and Confidential information.

5.1.3 No Private or Confidential information may be recorded or stored in cookies.

5.1.4 Vulnerability Scanning

5.1.4.1 A vulnerability scan should be performed on all applications and systems before they go into production and at appropriate intervals (no less than annually) thereafter.

5.1.4.1.1 Vulnerability scanning should follow a documented plan determined by the Web Content Services Administrator. This plan should be developed in coordination with the Server Administrator.

5.1.4.1.2 Information about applications for appropriate scanning can be found on the Information Security web site.

5.1.4.1.3 High risk issues should be reported to the Information Security Office and then remediated.

5.1.5 Patching

5.1.5.1 In order to maximize protection of web content services from the exploitation of vulnerabilities, patch application should be included in a documented overall web content services maintenance process.

5.1.6 Minimum Encryption Levels

5.1.6.1 Whenever Private or Confidential information is passed over the network, SSL version 3/TLS should be used. RIT authentication services, including passwords, are considered Confidential information.
5.1.6.2 All RIT-deployed web applications requiring encryption should follow best practices listed on the Information Security web site.

5.1.6.3 Serving Confidential Information at lower encryption levels for traveling faculty or the global community

5.1.6.3.1 SSL version 3 or higher, TLS is required except where subject to export control or other applicable local laws.

5.1.6.3.2 Users accessing web services via SSL version 2 should be presented with a statement of risk

5.1.7 Web Content Services Administrators and Web Content Developers are responsible for ensuring that server-side applications filter client input on the server following practices listed on the Information Security web site.

5.2 Logging

5.2.1 Web server access logs should retain at least 2 weeks of information for all web sites hosted.

5.2.1.1 Logs should include the source IP address, full URL and timestamp as a minimum.

5.2.1.2 Additional information logging may be performed at the discretion of the system administrator.

5.3 Access controls

5.3.1 Stateless User Authentication

5.3.1.1 Session IDs should be transmitted through SSL and employ appropriate security mechanisms.

5.3.2 Web Services Administrator Access Control

5.3.2.1 Configuration file write access should be limited to a web services administrative user group.

5.3.2.2 Accounts within the web services administrative group should be used solely for administering web services. They may not be used for general purposes or as root or other system administrator accounts.

5.3.3 Local Configuration File Use and Access Control

5.3.3.1 In order to prevent users from modifying the server configuration, Web Content Service Administrators should limit access to user-modifiable configuration commands (e.g., .htaccess) according to a documented plan.

5.3.3.2 Web Content Service Administrator should provide appropriate access controls for local configuration files.
5.4 Development & Acquisition
5.4.1 The development or selection of any information system should undergo a security review. This review shall conform to requirements in published RIT security standards.

5.5 Non availability of appropriate products
5.5.1 If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. When the term “appropriate” is used, web systems administrators are expected to use their professional judgment in managing risks to the information and systems they support.

6.0 New Security Software and Appliances Notification Requirements
In order to ensure security integrity and promote economies of scale, before evaluating new security software or appliances for use in RIT Web server environments and selecting vendors, a written description of the proposed function should be submitted to the Information Security Office at infosec@rit.edu

7.0 Roles and Responsibilities
This section identifies roles and responsibilities for implementation and compliance.

- **Information Security Officer**
  - The person responsible for issuing security standards based on legal context, threats and the needs of the Institute for protection. The ISO champions implementation efforts, facilitates recognition and communication of best practices, offers acceptable alternatives, and provides exceptions as appropriate. The staff of the Information Security Office provides communication and training materials as appropriate.

- **Information Trustee (VP or Provost)**
  - The person responsible for comprehending the risks associated with the security standard and providing direction to all students, faculty, and staff within his or her domain to ensure full compliance with the Standard and wherever possible the associated Best Practices.

- **Information Security Coordinator**
  - The person responsible for acting as an information security liaison to their colleges, divisions, or departments. Responsible for information security project management, communications, and training for their constituents.

- **Institute Audit, Compliance & Advisement (IACA)**
  - IACA reviews compliance with this Security Standard (and all Security Standards) as part of departmental audits.
- **Server, Systems, or Network Administrator**
  - The person responsible for ensuring the server providing web content services is compliant with the Server Standard

- **End Users**
  - End users who have administrator rights or the ability to share systems are defined as systems administrators.

- **Web Content Services Administrator**
  - The person responsible for the configuration and support of a web content service. This person may be partially responsible for the deployment of web content.
  - This person ensures that all *existing supported* web servers are configured to support the minimum standard (above) no later than the dates listed in Section 5.0, or an alternate plan for risk management is provided to their Information Trustee in accordance with the Exception Process by the compliance dates listed in Section 5.0.
  - This person ensures that all *newly-supported* web servers, web applications, and web tools are configured to support the minimum standard (above) starting no later than the dates listed in Section 5.0.
  - The web content services administrator is responsible for ensuring that third-party applications meet the standard

- **Web Content Developer**
  - A person responsible for the development and possibly the deployment of software that operates within the content of a web service for the purpose of facilitating or delivering web content
  - The web content developer is responsible for ensuring that any applications they create meet the Web Security Standard

### 8.0 Non-Compliance and Exceptions

For Systems or Network Administrators—If any of the *Minimum Standards* contained within this document cannot be met on systems you support, an Exception Process should be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management. For more, see: [https://www.rit.edu/security/content/exception-process](https://www.rit.edu/security/content/exception-process).

Anyone not complying with the standard is subject to sanctions including suspension of computer and network privileges and/or the full range of current Institute personnel and student disciplinary processes.
9.0 Related RIT Policies, Procedures, Best Practices and Applicable Laws (not all inclusive)

- RIT Information Security Policy (C8.1)
  https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C81.html

- RIT Code of Conduct for Computer and Network Use (C8.2)
  https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C82.html

- RIT Information Security Exception Process
  https://www.rit.edu/security/content/exception-process

- RIT Server Security Standard
  https://www.rit.edu/security/content/server-security-standard

- RIT Network Standard
  http://www.rit.edu/security/content/network-security-standard

- Information Access & Protection Standard
  https://www.rit.edu/security/content/information-access-protection-standard

Information Security Office

Date Issued: May 15, 2008