

Security Standard: Servers, Server-based Applications and Databases

Effective **August 1, 2009**

1.0 Purpose

The intent of this standard is to make servers and server-based applications on the RIT network more secure and to protect the data that they provide. This will aid business continuity and disaster recovery. The standard addresses significant and growing internal and external threats including, but not limited to:

- Criminals who are testing the vulnerability of RIT computers
- Network-based attacks
- Undetermined system anomalies that might hinder availability or access to critical information and/or applications
- Eavesdropping programs designed to relay sensitive information

2.0 Scope

This standard applies to all servers (including production, training, test, and development servers) and the operating system, applications, and databases (unless explicitly excluded) defined by this standard that provide services to the RIT community.

Although this standard does not apply to individually student-owned servers or faculty-assigned student server projects, administrators of these servers are encouraged to meet the server standard. Student-owned servers must meet the Desktop and Portable Computer Security Standard and Code of Conduct for Computer and Network Use (C8.2).

The standard does not apply to dedicated network equipment as defined in the network standard, or printers, remote desktop, and any other services defined as out of scope at <http://security.rit.edu/server.html>.

3.0 Audience

This standard applies to administrators and information trustees of all servers that are connected to the Institute network.

4.0 Definitions

Administrative access (server and services)

Administrative access is the use, interactive or automated, of an account that has the ability to read, write, or execute files or directories that can affect all other users.

Authoritative Source

The information source with the highest level of information verification or data integrity.

CVSS

Common Vulnerability Scoring System, or CVSS, is an industry standard for assessing the severity of computer system security vulnerabilities. It is structured on a 10 point scale, where 0-3.9 is a *low* score, 4-6.9 is a *medium* score, and 7-10 is a *high* score.

Grid Computing

A large system of networked computers whose collective processing power is used to solve difficult and time-consuming tasks.

Interactive Login

A login console which requires a user to interact locally with the system. An example of this is the Windows environment, the user is required to press Control+Alt+Delete simultaneously.

Patch Cluster

A group of patches and/or vulnerability fixes that change the version of the operating system/service, e.g., a service pack or minor version update.

Security Review

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

Server (logical servers, virtual servers)

A server is any physical or virtual network host that if you were to block all incoming network connections would affect more than one user or system and any related test, development or staging system.

Service

A service is any program that maintains a network socket for listening purposes.

Trust Relationship

A trust relationship is a relationship where two or more systems share the same key to authenticate.

5.0 Minimum Standard

The following security controls must be applied to, enabled, and running on all servers that connect to (or access) the Institute network no later than **August 1, 2009**, and all times thereafter. 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, systems administrators are expected to use their professional judgment in managing risks to the information and systems they support.

5.1 Secure Network and Physical Environment

- 5.1.1 Servers must be secured in locked racks or areas with restricted access.
- 5.1.2 All non-removable media must be configured with file systems with access control enabled.

5.1.3 Initial server setup

5.1.3.1 Servers must be set up in an environment with appropriately restricted network access.

5.1.4 Whenever possible, the server shall display a trespassing banner at login.

5.1.4.1 Sample banner language may be found at <http://security.rit.edu/server.html>

5.2 Patching/ Server Maintenance

5.2.1 A documented maintenance process must be established to keep applications and operating systems at the latest practical patch levels.

5.2.1.1 Vendor-supported patches must be available to RIT for operating systems and applications.

5.2.1.1.1 Use of operating systems or applications that are no longer supported by the vendor or an open source community requires filing an exception request with the ISO.

5.2.1.2 The maintenance process must include a reasonable timetable for routine application of patches and patch clusters (service packs and patch rollups).

5.2.1.3 In order to maximize protection of servers from the exploitation of vulnerabilities, for systems supported by vendor patches, patch application must be integrated into an overall server maintenance process.

5.2.1.4 In order to support effective incident response, there must be a means to inventory the current level of patches specific to the server.

5.2.1.5 In order to reduce the exposure of unpatched servers and to reduce the efforts required to manage servers in a dynamic update environment, there must be a process for monitoring patch installation failures.

5.3 Logging

5.3.1 In order to support the creation of an operational baseline for system, and service activities, and to detect and document access control violations, servers must be configured with appropriate real-time OS/application logging turned on.

5.3.2 There must be a documented process for routine log monitoring and analysis.

5.3.3 The systems administrator must review the logging process for effectiveness on a semi-annual basis or at a more frequent interval appropriate for the system.

- 5.3.4 A log monitoring process must be done on an appropriate schedule.
 - 5.3.4.1 Where capabilities exist, logging must include at least 2 weeks of relevant OS/application information. Typically, logging should include the following elements:
 - 5.3.4.1.1 All authentication
 - 5.3.4.1.2 Privilege escalation
 - 5.3.4.1.3 User additions and deletions
 - 5.3.4.1.4 Access control changes
 - 5.3.4.1.5 Job schedule start-up
 - 5.3.4.1.6 System integrity information
 - 5.3.4.1.7 Log entries must be time and date stamped
 - 5.3.5 Intentional logging of private information, such as passwords, etc., is prohibited.
 - 5.3.6 Logging must be mirrored in real time and stored on another secure server.

5.4 System Integrity Controls

- 5.4.1 To prevent and detect unauthorized programs from running, systems must be configured to restrict changes to start-up procedures.
- 5.4.2 There must be a documented change control process for systems configuration.
- 5.4.3 Risks must be mitigated by disabling all unused services.
- 5.4.4 Up-to-date anti-virus software and definitions must be used where available.
- 5.4.5 Servers must use a host firewall.
- 5.4.6 Where available, host-based intrusion prevention system software must be enabled.
 - 5.4.6.1 Host-based intrusion prevention (HIPS) software must be employed on authentication servers
 - 5.4.6.2 A list of recommended host-based intrusion prevention software may be found at <http://security.rit.edu/saresources.html>
- 5.4.7 Hardware-based system integrity control must be enabled where available

5.5 Vulnerability Assessment

- 5.5.1 A pre-production configuration or vulnerability assessment must be performed on all servers or services prior to moving them to production.

- 5.5.2 Servers must be scanned using an ISO-approved vulnerability scanner before being moved to production, after being moved to production, and ISO-specified periods thereafter.
 - 5.5.2.1 Acceptable vulnerability scanners are listed at <http://security.rit.edu/server.html>.
- 5.5.3 The ISO is authorized to perform vulnerability scanning on any server on the network
 - 5.5.3.1 Explicit blacklisting or permanent whitelisting of the ISO vulnerability scanner is prohibited.
- 5.5.4 A systems/server administrator is authorized to perform scans when approved by the system owner or the Information Security Office.
- 5.5.5 In order to facilitate effective investigations, a copy of the configuration and/or vulnerability assessment reports done at configuration time must be retained and provided to the Information Security Office on request.
- 5.5.6 Vulnerability criticality measurements will use CVSS scores as measures of the severity of the vulnerability.
 - 5.5.6.1 Announced vulnerabilities with a CVSS ≥ 7 must be evaluated for risk within one business day and patches or configuration changes applied appropriately after being announced and made available by the vendor.
 - 5.5.6.2 If the patch would disable a production application or environment, then other steps must be taken to manage the risk of an unpatched vulnerability. The Information Security Officer and the Information Security Coordinator must be made aware of the risk within **one** business day of identifying the patch conflict.
 - 5.5.6.3 If no CVSS applies to the vulnerability then the vulnerability must be evaluated for remote exploitation
- 5.5.7 Only ISO-approved security assessment tools shall be used for scanning.
 - 5.5.7.1 Acceptable security assessment tools are listed at <http://security.rit.edu/saresources.html>.

5.6 Authentication and Access Control

- 5.6.1 All trust relationships will be identified and reviewed at appropriate intervals.
- 5.6.2 All manufacturer and default passwords must be changed.
- 5.6.3 Strong authentication is required for all users with root/administrator or system privileges.
 - 5.6.3.1 Strong authentication practices are defined on the ISO web site.

- 5.6.4 Access Control must be configured to allow only authorized, authenticated access to the system, application and data.
 - 5.6.4.1 There must be a process for granting and removing authorized access.
 - 5.6.4.2 Generic or persistent guest accounts allowing users interactive logins must be disabled.
 - 5.6.4.3 Service accounts are excluded from this requirement.

5.7 Backup, Restore, and Business Continuity

- 5.7.1 Operationally Critical data must be backed up.
 - 5.7.1.1 All servers with Operationally Critical data must have documented back-up, system and application restoration (including configurations) and data restoration procedures to support business continuity and disaster recovery planning.
 - 5.7.1.2 Back-up procedures must be verified at least monthly, through automated verification, customer restores, or through trial restores.
 - 5.7.1.3 Backups shall not be stored solely in the same building where the Operationally Critical data is located.
 - 5.7.1.4 Backups should be readily accessible.
 - 5.7.1.5 Server backups shall be transmitted securely.
 - 5.7.1.5.1 Back-up media must be handled according to the Portable Media Security Standard.

5.8 Applications Administration

- 5.8.1 The applications/module administrator is responsible for ensuring the security of their applications/modules.
 - 5.8.1.1 For each application, the application owner must identify an application administrator and systems administrator. These administrators must be approved by their management.
- 5.8.2 The application administrator is responsible for application-specific aspects including ensuring the application is in compliance with the server standard where applicable.

5.9 Security Review and Risk Management

- 5.9.1 When major modifications are made to services or servers, e.g., new installations, major software upgrade, hardware replacement, server replacement/retirement, the systems administrators and applications administrators must complete a security review/risk assessment.
- 5.9.2 The security review shall typically include an architectural diagram, technical and process security controls, and a security checklist. Refer to the ISO website for current security review requirements.

- 5.9.3 The application owner is responsible for ensuring Information Security Office acceptance of the security review.
- 5.9.4 The Information Security Office may also conduct security reviews.
- 5.9.5 Vendor Services
 - 5.9.5.1 Any system or application administration contracts must be reviewed by purchasing for appropriate risk management clauses.

5.10 Server Registration

- 5.10.1 All servers with network access must be registered in an ISO-approved centralized registration system.

5.11 Server Hardware Replacement and Retirement

- 5.11.1 All server storage media and devices that contain RIT Confidential Information must be degaussed or the data otherwise rendered unrecoverable.

5.12 Server Administration

- 5.12.1 All computers used to administer servers must conform to all requirements for RIT-owned or leased computers as stated in the Desktop and Portable Computer Security Standard.
- 5.12.2 Protocols Related to Server Administration
 - 5.12.2.1 Only secure protocols may be used for administrative functions and/or the transmission of login credentials.
 - 5.12.2.1.1 A list of approved protocols may be found at <http://security.rit.edu/saresources.html>.
 - 5.12.2.2 NTP and DNS require authoritative sources

5.13 High Performance/Distributed Computing (WCG, CONDOR, PLANET LAB, or other grids)

- 5.13.1 Servers participating in High Performance/Distributed Computing/ grid computing must employ appropriate and documented safeguards to protect RIT Confidential information and access to RIT internal networks.

6.0 New Security Software and Appliances Notification Requirements

Anyone evaluating the implementation of new server security software or appliances must send a written description of the proposed implementation to the Information Security Office at infosec@rit.edu prior to selecting vendors.

7.0 Roles and Responsibilities

This section identifies roles and responsibilities for implementation and compliance.

- **Information Security Office**—issues security standards based on 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 (Divisional VP or Dean)**—comprehends the risks associated with the security standard and provides 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*.
- **Security Coordinator**—acts as an information security liaison to his or her colleges, divisions, or departments. Responsible for information security project management, communications, and training for their constituents.
- **Institute Audit, Compliance & Advisement (IACA)**—reviews compliance with this Security Standard (and all Security Standards) as part of departmental audits.
- **Systems or Network Administrator**—ensures that:
 - All existing supported servers are configured to support the minimum standard (above) no later than the compliance date of the standard or that an alternate plan for risk management is provided to their Information Trustee in accordance with the Exception Process.
 - All new supported servers are configured to support the minimum standard (above) starting no later than the dates listed in Section 4.0.

End users who have administrator rights or the ability to share systems are defined as systems administrators.
- **Applications/Module Administrator**—ensures that applications/modules are in compliance with RIT Information Security standards.
- **Application Owner**—ensures that the application is supported by an application administrator and a systems administrator.

8.0 Non-Compliance and Exceptions

For System or Network Administrators—If any of the *Minimum Standards* contained within this document can not be met on systems you support, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office a plan for risk assessment and management. For more, see: security.rit.edu/process/exceptions.pdf.

Anyone not complying with the standard is subject to sanctions including suspension of computer and network privileges and/or current Institute personnel and student disciplinary processes.

9.0 Related RIT Policies, Procedures, Best Practices and Applicable Laws (not all inclusive)

- RIT's Information Security Policy (C8.1)
<http://www.rit.edu/~620www/Manual/sectionC/C81.html>
- RIT's Code of Conduct for Computer and Network Use (C8.2)
<http://www.rit.edu/~620www/Manual/sectionC/C82.html>
- RIT's Information Security Exception Process
<http://security.rit.edu/process/exceptions.pdf>
- RIT's Desktop and Portable Computer Security Standard
<http://security.rit.edu/desktop.html>
- RIT Network Security Standard
<http://security.rit.edu/network.html>
- RIT Portable Media Security Standard
<http://security.rit.edu/portablemedia.html>

RIT Information Security Office

Date issued: August 16, 2005

Revised: May 15, 2009