

Security Standard: Servers

Effective November 15, 2005

1.0 Purpose

The intent of this standard is to make servers connecting to the RIT network more secure and to protect the data that they provide. 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 or confidential information

2.0 Scope

This standard applies to any Institute-owned or leased desktop, portable computers, or servers that provide the RIT community (five or more users) with access to vital academic or production data where confidentiality or reliability is a concern. The definition of “server” also extends to any computer in a test environment that is loaded with production data, including RIT Confidential information.

3.0 Audience

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

4.0 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 November 15, 2005, 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.

NOTE: Documentation requirements apply to servers configured on or after November 15, 2005.

4.1 Preventive Controls:

- 4.1.1 To prevent booting from CD or alternate media, resulting in the circumvention of access controls, servers must be physically secured in racks or areas with restricted access.
- 4.1.2 To support access control restrictions to operating system components and to non-public data, all non-removable or writeable media must be configured with file systems that support access control.

- 4.1.3 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 OS logging turned on. The rationale for the logging level must be documented.
- 4.1.4 In order to maintain system integrity and to provide a record of changes in the event that the system should need to be restored, there must be a documented change control process for systems configuration.
 - 4.1.4.1 If any technical controls to detect undocumented or unauthorized changes are used, they must be documented. This documentation may be part of a sitebook.
- 4.1.5 Servers must be set up in a protected network environment.
- 4.1.6 In order to properly identify and segregate public information, and provide appropriate access control to non-public information, access to non-public file system areas requires authentication (proof of identity).
- 4.1.7 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.
 - 4.1.7.1 A maintenance process must be established to keep systems at the latest practical patch levels. The maintenance process must be documented. The maintenance process must include a timetable for service packs and patch rollups. Security patches must be evaluated for risk within one business day and applied appropriately after being made available by the vendor if the patch prevents unauthorized privilege escalation or install of software, or addresses a vulnerability that could lead to the compromise of personal or Institute data.
 - 4.1.7.2 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.
 - 4.1.7.3 If the server is not connected to the network for significant periods, then the patches must be applied in a safe environment.
 - 4.1.7.4 Service packs and patch rollups should be applied as appropriate, in a timely manner.
- 4.1.8 In order to support effective incident response, there must be a means to inventory the current level of patches specific to the server.

- 4.1.9 In order to minimize server/service downtime, and to minimize the possibility of data corruption, server changes should be evaluated prior to affecting a production environment.
 - 4.1.9.1 If availability or data integrity requirements are high, then patches must be tested prior to installation in the production environment if a test environment is available.
 - 4.1.9.2 If a test environment is not available, the lack of a test environment must be communicated to the customer, along with possible changes in the environment due to the patch.
- 4.1.10 In order to reduce exposures from unneeded software subsystems, and to focus efforts on baselines and monitoring of essential services, all unused services must be disabled.
- 4.1.11 In order to reduce the risks of privilege escalation, and the unintentional exposure of one guest user's information to another, generic or persistent guest accounts allowing users interactive login must be disabled, unless a risk assessment and management plan is communicated to the ISO.
- 4.1.12 In order to minimize risks of unintentional access, modification, or deletion of data, directories where full access privileges are extended to everyone, must be planned, controlled, and communicated. Systems administrators must document the risk management process for all directories that they create where there is world read and write access.

4.2 **Preventive and Detective Controls:**

- 4.2.1 In order to support access control, the systems administrator must ensure that there is a documented process for routine OS log monitoring and analysis.
 - 4.2.1.1 A log monitoring process must be done on an appropriate schedule.
- 4.2.2 In order to protect sensitive data when in the portable form of backups, backups of RIT Confidential data must be secured from unauthorized physical access. If backups are stored off-site, then they must be encrypted (as defined by the ISO website) or have a documented process to prevent unauthorized access.
- 4.2.3 In order to support the availability of information in the event of unauthorized or accidental deletion or modification, and to support the continuity of individual and university operational objectives, backups must be verified at least monthly, either through an automated verification, customer restores, or through trial restores.
- 4.2.4 In order to support the incident handling process for recent incidents, the systems administrator must follow a documented backup strategy for OS security logs (e.g.; account management, access control, data integrity, etc.).

4.2.4.1 The security log must retain at least 2 weeks of relevant OS log information.

4.2.5 In order to provide reasonable safeguards against viruses, up-to-date anti-virus software must be used on all Windows or Macintosh servers where non-systems users can create, attach, or upload files. Systems administrators must make available a description of the standard configuration including reports of any exceptions to the Information Security Office.

4.2.5.1 All Windows or Macintosh servers directly attaching to Storage Area Networks (SAN), and Network Attached Storage (NAS), must run up-to-date anti-virus software.

4.2.6 In order to identify unauthorized privileged access, all server administrator or root access must be logged.

4.3 **Preventive/Corrective Controls:**

In order to reasonably safeguard the availability of information, systems administrators must:

4.3.1 Maintain a documented data restoration procedure.

4.3.2 Maintain a documented system restoration procedure.

5.0 **New Security Software and Appliances Notification Requirements**

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

6.0 **Roles and Responsibilities**

This section identifies roles and responsibilities for implementation and compliance.

- **Information Security Officer**—issues 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)**—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*.
- **Information Security Coordinator**—acts as an information security liaison to their colleges, divisions, or departments. Responsible for information

security project management, communications, and training for their constituents.

- **Systems or Network Administrator**—ensures that:
 - All existing supported servers are configured to support the minimum standard (above) no later than the dates listed in Section 4.0, 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 4.0.
 - All newly 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.

7.0 Non-Compliance and Exceptions

For Systems 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, along with a plan for risk assessment and management. For more, see: <http://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 the full range of current Institute personnel and student disciplinary processes.

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

- RIT's Information Security Policy
<http://www.rit.edu/InformationSecurity<placeholder>>
- RIT's Code of Conduct for Computer and Network Use (C10.0)
<http://www.rit.edu/computerconduct>
- 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/articles/desktopstandard.pdf>

Jim Moore, Information Security Officer, CISSP, IAM

Date Issued: August 16, 2005

Next Scheduled Review Date: July 1, 2006