



Plain English Guide to the Server Security Standard

RIT has issued new requirements for servers in order to safeguard RIT information. These requirements were developed and reviewed by a team representing the RIT community. This Plain English Guide provides explanation and illustration of the standard and is provided as an aid to help you understand and implement the requirements of the standard. The standard itself is authoritative. The standard is effective on **August 1, 2009**.

Why we issued this standard

Appropriate protection for servers is essential because servers contain the largest concentrations of RIT Confidential and Operationally Critical information and are a prime target for attackers. Server compromises may result in a number of undesirable outcomes, including embarrassment or liability to RIT, productivity loss, student or personnel identity theft and potential regulatory sanctions. The server standard provides measures to prevent, detect, and correct server compromises based on both new practices and best practices currently in use at RIT.

Who do the requirements apply to?

The requirements apply to **administrators** of all **servers, including production, training, test, and development** servers, as well as the **administrators** of all **operating systems, applications, and databases** residing on RIT servers (unless explicitly excluded) that provide services to the RIT community. The audience for this standard also includes **server owners** and **information trustees** of all servers connecting to the Institute network.

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

What will I have to do?

Server owners and systems administrators will need to adopt controls in several different areas in order to ensure the security of servers and the data residing on them. Systems and applications administrators will need to meet technical requirements on the servers, follow specific processes, and provide adequate documentation.

If you are a server owner whose server is supported by an RIT systems administrator (ITS, FAST, COB, etc.), you should contact your systems administrators to see if they are assuming some or all of the responsibility for providing appropriate protection as outlined below.

Secure Network and Physical Environment

Servers must be secured in locked racks or in areas with restricted access.

System Integrity and Authentication and Access Controls

Servers must have system integrity controls in place, including appropriate software and hardware-based integrity controls. In order to mitigate risk, all unused services and generic or persistent guest accounts should be disabled, and all default passwords should be changed or disabled. There must also be a documented change control process for systems configuration.

File systems residing on servers should have appropriate access control protection to ensure only authorized users are able to access sensitive data. Users with root or administrative level privileges should use strong authentication as defined on the Information Security website (<http://security.rit.edu>). There should be a documented process for granting and removing authorized access.

Vulnerability Assessment & Patching/Server Maintenance

The Information Security Office (ISO) will conduct periodic vulnerability assessments of systems in order to identify potential high-risk vulnerabilities. These scans must be performed before and after moving a server into production, and a copy of the report must be retained and provided to the ISO upon request. A systems/server administrator may perform scans if approved by the systems owner or ISO. Vulnerability criticality measurements will use an industry standard known as CVSS scores. More information on the RIT Vulnerability Management program can be found at <http://security.rit.edu/scanning.html>.

Routine (non-critical) patching and maintenance should be regularly scheduled in order to keep applications and operating systems at the latest practical patch levels. Patch application should be integrated into an overall server maintenance process, which should include a means for monitoring patch installation failures. The process and schedule for server maintenance should be documented.

Logging

Servers must be configured with real-time operating system and application logging enabled. There must be a documented process and schedule for routine log monitoring and review. Where possible, logging should include at least 2 weeks of relevant information, including all authentication, access control changes, user additions/deletions, and system integrity information. There should be *no* intentional logging of private information, such as passwords. Logging must be mirrored in real time and stored on a separate secure server.

Backup, Restore, and Business Continuity

All servers with Operationally Critical data must have documented back-up, system and application restoration, and data restoration procedures to support business continuity and disaster recovery planning. Back-ups should be verified at least monthly and be readily accessible. Back-ups must not be stored solely in the same building where the Operationally Critical data is located, and they must be transmitted securely. Back-up media *must* meet the requirements of the [Portable Media Security Standard](#).

Server and Applications Administration

All computers used to administer servers must meet the requirements the [Desktop and Portable Security Standard](#). Only secure protocols may be used for administrative functions (a list of approved protocols is available at <http://security.rit.edu/saresources.html>).

Application/module owners must designate an application administrator and a systems administrator for each application. These administrators must be approved by their management and are responsible for ensuring the security of their applications/modules.

Server Registration and Hardware Replacement

All servers with network access must be registered in an ISO-approved centralized registration system. Any servers, server storage media, or other devices that contain RIT Confidential information must be degaussed or the data otherwise rendered unrecoverable. See <http://security.rit.edu/dsd/iap/disposal.html> for more information on safe disposal.

Security Review and Risk Management

Upon any major changes to services or servers (including but not limited to new installations, software upgrades, and hardware replacement), the systems and applications administrators must complete a security review/risk assessment. Specific requirements for security reviews can be found on the ISO website. The application **owner** is responsible for ensuring ISO acceptance of the security review.

Any system or application administration contracts must be reviewed by Purchasing for appropriate risk management clauses.

Grid/High Performance/Distributed Computing

Any servers participating in grid/high performance/distributed computing must employ appropriate and documented safeguards to protect RIT Confidential information and access to RIT internal networks.

Where do I go for more information?

Detailed requirements can be found in the standard. We have also created a Server Security Checklist to aid systems administrators in complying with this standard.

Visit the Server Security Standard webpage at <http://security.rit.edu/server.html> to read the standard, download the checklist, or find out more ways to protect your servers. For more information, contact RIT Information Security at infosec@rit.edu.