Server Security Checklist (2009 Standard)

Server identification and location: _____

Completed by (please print): _____ Date: _____

Signature: _____ Next scheduled review date: _____

Manager's signature: _____ Date: _____

Secure Network and Physical Environment		Initials
1. Server is secured in locked rack or in an area with restricted access.	*(5.1.1)*	
2. All non-removable media is configured with file systems with access controls enabled.	*(5.1.2)*	
3. Server is set up in an environment with appropriately restricted network access.	*(5.1.3.1)*	
4. The server displays a trespassing banner at login. If unable to display banner, check box ☐	*(5.1.4)*	

Patching/ Server Maintenance		Initials
5. There is a documented maintenance process to keep applications and operating systems at the latest practical patch levels. Where is it documented? _____	*(5.2.1)*	
6. Vendor-supported operating systems and application patches are readily available to RIT.	*(5.2.1.1)*	
7. Operating systems or applications that are no longer supported by the vendor or an open source community have an exception request pending or granted by the ISO.	*(5.2.1.1.1)*	
8. There is a documented maintenance process which includes a reasonable timetable for routine application of patches and patch clusters (service packs and patch rollups). Where is this documented? _____	*(5.2.1.2)*	
9. Systems supported by vendor patches have the patch application integrated into a documented server maintenance process. Where is this documented?_____ _____	*(5.2.1.3)*	
10. There is a process to inventory the current level of patches specific to this server	*(5.2.1.4)*	
11. There is a process for monitoring patch installation failures	*(5.2.1.5)*	

Logging		Initials
12. Server is configured with appropriate real-time OS/application logging turned on.	*(5.3.1)*	
13. There is a documented process for routine log monitoring and analysis. Where is it documented? _____	*(5.3.2)*	

14. Reviews are conducted periodically to ensure the effectiveness of the server logging process. *(5.3.3)* How often? (At least monthly): _____	
15. There is a schedule for log monitoring of the server. Where is it documented? _____ *(5.3.4)*	
16. Logging has been configured to include at least 2 weeks of relevant OS/application information. The logging elements include: *(5.3.4.1)* ☐ All authentication ☐ Privilege escalation ☐ User additions and deletions ☐ Access control changes ☐ Job schedule start-up ☐ System integrity information ☐ Log entries must be time and date stamped	
17. Intentional logging of private information, such as passwords, has been disabled. *(5.3.5)*	
18. Logging is mirrored in real time and stored on another secure server. *(5.3.6)*	

System Integrity Controls	**Initials**
19. System is configured to restrict changes to start-up procedures. *(5.4.1)*	
20. There is a documented change control process for system configurations. *(5.4.2)* Where is it documented? _____	
21. All unused services are disabled. *(5.4.3)*	
22. If available, anti-virus software and definitions are current and up-to-date. *(5.4.4)*	
23. Server has a host firewall installed and enabled. *(5.4.5)*	
24. Is host-based intrusion prevention software (HIPS) enabled? (**Y**/**N**)_____ *(5.4.6)*	
25. Is this an authentication server?(**Y**/**N**)_____ (Host-based intrusion prevention software is required for authentication servers) *(5.4.6.1)*	
26. If available, hardware-based system integrity control is enabled. *(5.4.7)*	

Vulnerability Assessment	**Initials**
27. A pre-production configuration or vulnerability assessment has been performed on the server and its services prior to moving to production. *(5.5.1)*	
28. Server has been 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)* How often is the server being scanned? _____	
29. A copy of the configuration and/or vulnerability assessment reports done at initial server configuration has been retained for possible future use by the ISO. *(5.5.5)*	
30. After vulnerabilities with the CVSS score of 7 or greater are announced the corresponding patches and/or configurations are updated within one business day. *(5.5.6.1)*	

31. If no CVSS applies to a vulnerability then the vulnerability must be evaluated for remote exploitation. *(5.5.6.3)*	
32. The ISO is authorized to perform vulnerability scanning for this server. *(5.5.3)*	
33. The ISO vulnerability scanner is not blocked specifically or permanently whitelisted. *(5.5.3.1)*	
34. A systems/server administrator is authorized to perform scans when approved by the system owner or the ISO. Is there anyone else authorized to perform scanning?(**Y/N)**_____ If **yes**, who? _____ *(5.5.4)*	

Authentication and Access Control	**Initials**
35. All trust relationships have been identified and reviewed. *(5.6.1)*	
36. All manufacturer and default passwords have been changed. *(5.6.2)*	
37. Strong authentication has been configured for all users with root or administrator system privileges. Refer to the ISO website for a list of strong authentication practices. *(5.6.3)*	
38. Access Control has been configured to allow only authorized, authenticated access to the system and its applications and data. *(5.6.4)*	
39. There is a documented process for granting and removing authorized access Where is it documented? _____ *(5.6.4.1)*	
40. Generic or persistent guest accounts allowing user interactive logins have been disabled. (Service accounts are excluded from this requirement.) *(5.6.4.2 and 5.6.4.3)*	

Backup, Restore, and Business Continuity	**Initials**
41. Operationally Critical data has been backed up. *(5.7.1)*	
42. All servers with Operationally Critical data have documented back-up, system and application restoration (including configurations) and data restoration procedures to support business continuity and disaster recovery planning. Where is this documented? _____ *(5.7.1.1)*	
43. Back-up procedures are verified at least monthly through automated verification, customer restores, or through trial restores. How often are they verified? _____ *(5.7.1.2)*	
44. Backups are not being stored solely in the same building where the Operationally Critical data is located. *(5.7.1.3)*	
45. Backups have been made readily accessible. *(5.7.1.4)*	
46. Measures to transmit server back-ups securely have been put in to place. *(5.7.1.5)*	
47. Back-up media is compliant with the Portable Media Security Standard. *(5.7.1.6)*	

Applications Administration	**Initials**
48. The application administrator is responsible for application-specific aspects including ensuring the application is in compliance with the server standard where applicable. *(5.8.2)*	
49. The applications/module administrator is responsible for ensuring the security of their applications/modules. *(5.8.1)*	
50. For each application, the application owner must identify an application administrator and systems administrator. These administrators must be approved by their management. Use the form on the last page to list all applications and their application and systems administrators. *(5.8.1.1)*	

Security Review and Risk Management	Initials
51. Is this a new server installation? (**Y**/**N**) _____ *(5.9.1)* (See ISO Server Security Standard Section 5.9.2 for specific criteria.) Answer question 52 only if answer to 51 is **YES.**	
52. A security review/risk assessment has been completed *(5.9.1)* When? _____ By who? _____ Are they ISO approved? _____	

Server Registration	Initials
53. The server has network access and has been registered in an ISO-approved centralized registration system. *(5.10.1)*	

Server Hardware Replacement and Retirement	Initials
54. Have there been any server storage media and/or devices containing RIT Confidential Information been removed or replaced? (**Y**/**N**)_____ *(5.11.1)* If **yes**, the media or device must be degaussed or the data otherwise rendered unrecoverable.	

Server Administration	Initials
55. All computers used to administer servers conform to the requirements for RIT-owned or leased computers as stated in the Desktop and Portable Computer Security Standard. *(5.12.1)*	
56. Secure protocols are being used for administrative functions and transmission of login credentials. *(5.12.2.1)*	
57. NTP and DNS have authoritative sources. *(5.12.2.2.1)*	

High Performance and Distributed Computing	Initials
58. Does this server participate in High Performance/Distributed Computing/grid computing? *(5.13.1)* (**Y**/**N**) _____ If **yes**, list which one: _____ Servers that do participate in this type of computing must employ appropriate and documented safeguards to protect RIT Confidential Information and access to RIT internal networks.	

Application	Application Administrator	Systems Administrator

For more information:
RIT Information Security
585-475-4122
infosec@rit.edu
https://www.rit.edu/security