



Server Security Set-up Checklist

Server identification and location: _____

Completed by (please print): _____ Date: _____

Signature: _____ Next scheduled review date: _____

Manager's signature: _____ Date: _____

| Type of Control | Initials |
|--|----------|
| Preventive Controls | |
| 1. Server is physically secured. (4.1.1) | |
| 2. All hard drives and logical volumes are configured with file systems that support access control. (4.1.2) | |
| 3. Appropriate OS accounting/logging is turned on. (4.1.3) Where is the rationale for the logging level documented? _____ | |
| 4. Authentication (proof of identity) is required for all services that are capable of checking identity. (4.1.6) | |
| 5. A maintenance process has been established to keep systems at the latest practical patch levels. (4.1.7) Where is this maintenance process documented? _____ | |
| 6. There is a method available to inventory the current level of patches on the server. (4.1.8) | |
| 7. All unnecessary services are disabled. (4.1.10) | |
| 8. Persistent guest accounts are disabled. (4.1.11) | |

| | |
|--|--|
| Preventive/Detective Controls | |
| 9. Security logs retain at least 2 weeks of relevant log information. (4.2.3.1) | |
| 10. All server administrator or root access is logged. (4.2.6) | |
| 11. Up-to-date anti-virus software is used on all Windows and Macintosh servers where non systems users can create, attach, or upload files. (4.2.4) | |

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



Server Security Documentation Checklist

Server identification and location: _____

Completed by (please print): _____ Date: _____

Signature: _____ Next scheduled review date: _____

Manager's signature: _____ Date: _____

| Type of Control | Initials |
|--|----------|
| Preventive Controls | |
| 1. Are availability or data integrity requirements high for this server? YES NO (4.1.9) If YES, continue to part A. If NO, go to item 2. A. Are patches tested in a test environment prior to installation in the production environment? YES NO If YES, go to item 2, if NO go to part B B. Has the lack of a test environment been communicated to the customer? YES NO Continue to item 2 | |
| 2. A change control process for systems configuration exists. (4.1.4) Where is this control process documented? _____ | |
| 3. If controls are in place to detect undocumented or unauthorized changes, these controls are documented. (Controls may include monitoring, restricting, and reporting attempted changes to start procedures.) (4.1.4.1) | |
| 4. A maintenance process has been established to keep systems at the latest practical patch levels. (4.1.7) Where is this maintenance process documented? _____ | |
| 5. Risks have been documented for all directories created by the system administrator with unrestricted read-write access. (4.1.12) Where is this assessment documented? _____ | |
| Preventive/Detective Controls | |
| 6. There is a documented process for routine log monitoring and analysis. (4.2.1) Where is this process documented? _____ | |
| 7. The log monitoring process is done on an appropriate schedule. (4.2.1.1) | |
| 8. Backups of sensitive data are secured from physical access. (If backups are stored off-site, then they must be encrypted or the security of the site evaluated and documented.) (4.2.2) | |
| 9. Backups are verified at least monthly, either through an automated verification, customer restores or through manual tests. (4.2.3) | |

| | |
|---|--|
| 10. A backup strategy for OS security logs (e.g.; account management, access control, data integrity, etc.) is documented and followed. Where is this process documented? _____ (4.2.4) | |
| 11. A description of the standard anti-virus configuration including reports of any exceptions has been sent to the Information Security Office. (4.2.5) | |
| Preventive/Corrective Controls | |
| 12. A plan for system remediation in the event of a preventive or detective control failure has been created. Where is this plan documented? _____ (4.3.2) | |
| 13. A documented procedure for data restoration exists and is maintained. Where is this procedure documented? _____ (4.3.1) | |

Security Software and Appliances Evaluation

| | |
|---|--|
| 14. When new security software or appliances are being evaluated for production, a written description will be sent to the Information Security Office. (5.0) | |
|---|--|

For more information:
RIT Information Security
585-475-4122
infosec@rit.edu
<http://security.rit.edu>