# RIT | Information Security

# Network Security Documentation Checklist (2009)

---

**Network Device identification and location:** _____

Completed by (please print): _____ Date: _____

Signature: _____ Next scheduled review date: _____

Manager's signature: _____ Date: _____

| Type of Control | | Initials |
|---|---|---|
| **Physical Security** | | |
| 1. The network device is secured in an area with physical access control. | *(5.3.1)* | |
| 2. Is the network device considered a Core network device as defined by the standard?  (**Y/N**) _____  If **No**, skip to item **5**. | *(4.0)* | |
| 3. The core network device is located in an alarmed area. | *(5.3.2)* | |
| 4. The core network device is attached to an appropriately designed UPS and generator system. | *(5.3.3)* | |
| **Authentication & Access Lists** | | |
| 5. Access lists are configured to limit the number of locations the device may be accessed from. | *(5.4.1)* | |
| 6. Access to configuration backups is restricted to authorized personnel. | *(5.4.1.1)* | |
| 7. The device is protected from Layer-3 IP address spoofing. | *(5.4.2)* | |
| 8. All external connections to RIT are protected in accordance with the ITS-maintained access list. | *(5.4.3)* | |
| 9. Centralized user-level authentication is used to authenticate all interactive users making changes to the network device. | *(5.4.4)* | |
| 10. If possible, the network device displays a trespassing banner at login that does not reveal underlying characteristics of the network. | *(5.4.5)* | |
| **Network Management** | | |
| 11. If the network device utilizes a 802.1q trunk, the native VLAN is not VLAN 1. | *(5.5.1)* | |
| 12. Plain-text protocols are not utilized for management of the device. | *(5.5.2)* | |
| 13. Management traffic is separated from user traffic. | *(5.5.3)* | |
| 14. Management interfaces for the device are located on a management network. | *(5.5.4)* | |
| 15. Any console ports used for device management are secured by a username/password or other ISO approved method. | *(5.5.5)* | |
| 16. The network device has transitioned to SNMPv3 or another option that does not use plaintext community strings for network management services. | *(5.5.6)* | |
| 17. Default SNMP community strings have been changed. | *(5.5.7)* | |
| 18. The device does not use LDAP without ~~SSLv3 or~~ TLS, FTP, telnet, remote host protocols, SSHv1, SSLv1, SSLv2, and SSLv3. A list of prohibited protocols can be found at http://www.rit.edu/security/content/network-security-standard . *(5.5.8)* | | |

---

Network Checklist final b.doc

revised 5/18/09

| | |
|---|---|
| **Intrusion Detection System** | |
| 19. An IDS service is deployed on the links to/from the Institute network and the public Internet/Internet2. *(5.6.1)* | |
| 20. Hosts that are detected via the rule set are automatically blocked from further network access until the cause of the detection is understood and remediated. *(5.6.1)* | |
| **Anti ARP-spoofing** | |
| 21. Is the network device a user-edge network device? *(5.7)*<br><br>(**Y/N**) _____ If **No**, skip to item **23**. | |
| 22. DHCP/ARP Snooping support is enabled on the device. *(5.7.1.1)* | |
| **Change Control** | |
| 23. Will the addition of, or changes to this device involve significant risk to the Institute Network? *(5.8)*<br><br>(**Y/N**) _____ If **No**, skip to item **25**. | |
| 24. A change control process for the device exists, including a problem statement, supporting data, potential solutions, potential impact/risks, and management approval. *(5.8.1)*<br><br>Who has approved this process? _____ | |
| **Logging and Monitoring** | |
| 25. The network device logs to a logging/management system. *(5.9.1)*<br><br>Where is the logging process documented? _____ | |
| 26. The network device is regularly monitored for its ability to be reached by the central network management system. *(5.9.2)* | |
| **Passwords** | |
| 27. The process to change the password on the device is in accordance with the password standard. *(5.10.1)* | |
| 28. All manufacturers' default passwords have been disabled or changed. *(5.10.2)* | |
| **Configuration Backups** | |
| 29. The configuration of the device is backed up regularly. *(5.11.1)* | |
| 30. The device configuration is subject to managed revision control, and changes in configuration result in the automatic notification of the network administrator. *(5.11.2)* | |
| **VPN** | |
| 31. Does this network device provide or assist with providing VPN service for use at RIT? *(5.12)*<br><br>(**Y/N**) _____ If **No**, skip to item **34**. | |
| 32. The VPN service only allows connection to the Internet through RIT. *(5.12.1)* | |
| 33. The VPN service has undergone a security review. *(5.12.2)*<br><br>Where are the results of the security review documented? _____ | |
| **Vulnerability Scanning & Quarantine** | |
| 34. The network device is regularly scanned for hosts that are vulnerable to remote exploits. *(5.13.1)* | |
| 35. Vulnerable hosts are moved to a quarantine network where they have the capability to access services necessary to patch and remediate infections. *(5.13.3)* | |
| 36. The network device is not configured to explicitly blacklist or permanently whitelist the ISO vulnerability scanner. *(5.13.5)* | |

| | | |
|---|---:|---|
| **Wireless Security** | | |
| 37. Is this network device a wireless network device?<br><br>   (**Y/N**) _____     If **No**, skip to item **40**. | *(5.14)* | |
| 38. The wireless device supports ISO-approved encryption methods. | *(5.14.1)* | |
| 39. The wireless device adheres to minimum levels of security developed by the ISO. | *(5.14.2)* | |
| **Device Registration** | | |
| 40. Does the network device have an IP address?<br>   (**Y/N**) _____     If **No**, you mean skip the remaining items. | *(5.15.1)* | |
| 41. The IP and all MAC addresses are registered in an ISO-approved registration system.<br>   Where is the device registered? _____ | *(5.15.1.1)* | |
| 42. Any guest access on the device is registered with appropriate contact information. | *(5.15.1.2)* | |

RIT Information Security
infosec@rit.edu
https://www.rit.edu/security/