Minimum Security Standard: Servers [1]

Standard	What to do	RISK/DATA
Patching	Patch systems within two weeks of a security update addressing a Critical or High vulnerability [2] becoming available. Users need to document alternative mitigation methods if they are unable to patch.	
Vulnerability Management	ITSO conducts monthly scans, which may uncover vulnerabilities on hosts or applications. Machines which handle sensitive data are scanned every 2 weeks. Do not explicitly block our vulnerability scanning.	
Firewall	Enable host-based firewall in default deny mode and permit the minimum necessary services.	
Credentials and Access Control	Review existing accounts and privileges annually. Enforce password complexity. Use of Kerberos and Duke NetIDs for accounts and authentication is recommended.	
Two-Step Authentication	Require multi-factor authentication [3] for all administrator logins (Public/Restricted/Sensitive) and interactive users of (Restricted/Sensitive) systems.	

Centralized Logging	Forward logs to a remote log server. University IT Splunk service recommended.	
Monitor for Security Updates	Join and monitor security and IT group lists to receive notification of updates.	
Malware Protection	Deploy Crowdstrike on servers and configure it to report device status updates to a management console. Review alerts as they are received.	
Physical Protection	Place system hardware in a data center or secure area behind a locked door/card access/etc. Log physical access for machines handling sensitive data.	
Security, Privacy, and Legal Review	Request a Data Risk Review by ITSO prior to deployment of a system storing or accessing sensitive data.	
Regulated Data Security Controls	Implement PCI DSS [4], HIPAA [5], or export controls as applicable.	
Equipment Disposal	All Duke-owned machines must go through Duke Surplus before disposal.	
Credentials and Access Control	Configure servers to prohibit anonymous access. Set an account lockout policy (recommended: after five unsuccessful attempts followed by a five-minute lockout). Require password-protected screen savers, with a recommended 15-minute timer for inactivity.	

Last Reviewed: 08/17

Document Type:
Standard

Applicable To:
Duke University

Source URL: https://security.duke.edu/policies/minimum-security-standards-servers

Links
[1] https://security.duke.edu/policies/minimum-security-standards-servers
[2] https://security.duke.edu/secure/policies/vulnerability-management-procedure
[3] https://security.duke.edu/multi-factor-authentication
[4] https://finance.duke.edu/banking/ecommerce/reginfo.php
[5] https://www.dukehealth.org/patients-and-visitors/patient-bill-of-rights