Published on *IT Security Office* (https://security.duke.edu)

Duke University Standard: Server Security [1]

Version 4.1

Author

Office of Information Technology (OIT)

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Definitions

Term	Definition
Application	Any software that runs on a computer or other networked device and is used by end users or other applications or devices, including but not limited to databases, web applications, client/server applications.
Departmental Staff	Duke University staff who work for a specific department and who are involved in installation or support of departmental servers. For the purpose of this document, all contract and temporary employees are included.
Encryption Options	For the purposes of this standard, the minimal key strength must be 128-bit for symmetrical, and 1024-bit for public key encryption. Organizations that are involved with HIPAA/HITECH data in any way should consider using a FIPS 140-2 validated encryption method (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm [2]), and if not deployed, document the reasons for not deploying encryption.
End-User Account	Accounts used by the non-administrator community to access services offered by the server. Note that this refers to an account on the server and does not necessarily refer to institutional accounts such as the Duke NetID.
Individual Administrator Account	Accounts that are system-level accounts and are not predefined by the vendor: individualized accounts with full privileges on the system.
Operating System	A program that manages a networked device's hardware resources.
Privileged Access	Access to system-level accounts.
Protected Data	Any information classified as either Sensitive ot Restricted by the Duke standard.
Sensitive and Restricted Data	As defined in the Duke University Classification Standard.
Server	A server is any device with an active network connection that provides services or resources to users and/or to other systems. Touchscreen panels that control other devices, video and audio storage devices, and desktop or lab machines which act as servers should follow this standard. Desktop systems that only provide services intended for one primary user or thw administrators of the computer are not included in this standard.

Service or System-Level Account	Accounts that have full system privileges and are an integral part of the operating system, database, or application into which they are bundled. These accounts often cannot be renamed because the named accounts are needed to perform certain functions (e.g., root, Oracle).
Web application or web-based application	An application that is accessed via a web browser over a network, or is dependent on a browser to execute code.

Purpose

The purpose of this standard is to assist Duke system administrators in establishing strict rules for the base configuration and management of servers owned and/or operated by Duke University. **Compliance with this standard does not exempt a server from meeting University, federal, or state laws or other required standards.** (For example, if a server is collecting or storing credit card data, then the application and server must comply with all PCI-DSS policies implemented by Duke's Treasury and Cash Management Office.)

As there are a wide variety of operating systems, software and system configurations used across campus, this document is NOT intended to be a "How-To" on system security. Instead, this standard is intended to identify areas for systems administrators where there are issues to be addressed and documented in a manner that is appropriate to the server and the services it provides. It is expected that all servers will comply with the requirements of this standard before being put into production. All recommended practices listed should be implemented unless they significantly disrupt business operations. If the standard is customized for a unique business operation (or a unique organization, such as research or cluster computing), the systems administrators should document all customizations. Campus organizational units (departments, schools, institutes, and others) bear the responsibility for detailing their adherence to and departure from this standard.

Effective implementation of this standard should minimize the likelihood of unauthorized access to campus computing resources and protected data. However, all security events should be reported to security@duke.edu [3] as soon as they are discovered, in order to ensure compliance with legal obligations.

Scope

This standard applies to all server equipment (as defined above) administered or serviced by university staff or by third parties via contractual agreements with university departments or other organization groups.

Server/Service Standard

Overview

When it comes to security, a layered approach, also known as "defense in depth" helps mitigate risks to critical systems. With a layered approach, even if an intruder is able to bypass one security control, overlapping layers of security make it more likely that the break-in will be contained by another mechanism. Similarly, overlapping security controls can prevent accidental or intentional harm to information resources by employees or third parties. To emphasize this principle, this document is organized in the following conceptual layers:

4.2 Physical
4.3 Network
4.4 Operating System
4.5 Data
4.6 Application
4.7 User
4.8 Administrative

The method for addressing each of the above security layers should be documented by each department and kept up-to-date to reflect changes in system administration practices.

The standards that follow are meant to provide a baseline for security of servers on the Duke network. As such, the ITSO strongly recommends that a qualified IT professional or competent individual with equivalent expertise manage the servers. Servers should be managed by such qualified individuals because of the potential exposure they create to the campus network. Unmanaged servers can cause unneeded risks through missing patches, unneeded services, or misconfiguration. It should also be understood that if a server adversely impacts the network, then the server manager could be held accountable for the state of the server.

4.2 Physical

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.2.1	Physically locate servers in an access-controlled environment.	✓	✓	✓

4.2.2	Only grant physical access to servers to authorized individuals and accompanied service personnel.	✓	✓	✓
4.2.3	Log all physical access to servers to the access-controlled environment.			✓

4.3 Network

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.3.1	All server operating systems must run appropriate host-based access controls (e.g. firewall, port controls, access lists). Rule sets must allow access to only those ports that are necessary to provide service and to maintain the servers. **All rule sets must be in 'default deny' configuration if Sensitive or Restricted data is stored or processed by the server.**	✓	✓	✓
4.3.2	Implement a network firewall - see the OIT Firewall service for recommended base configuration settings.		✓	✓
4.3.3	Perform all privileged access over secure channels, (e.g., encrypted network connections using Secure Shell (SSH) or Virtual Private Network (VPN)). Access via the Internet must always be performed using an encrypted mechanism. If a challenge response system is used for authentication, it must take place over an encrypted channel. Private networks (networks using non-routed IP addresses and which are physically isolated) may be a reasonable substitute for encryption, but encryption is strongly recommended and departmental management must explicitly approve any instances of unencrypted privileged access.	✓	✓	✓
4.3.4	Encrypt all authentication traffic. Alternatives may be implemented based on the type of access needed (examples include sFTP, SCP, SSH, and SSL encapsulated protocols).	✓	✓	✓
4.3.5	Log all network based access to the server			✓
4.3.6	Implement the following safeguards to provide vendor access to servers (whether via modem, Internet or other means): • fully document the contractual understanding of the responsibilities of the vendor • vendor access is disabled except when required for a specific business need • access to the server requires individualized authentication (NetID authentication is preferred) • logging must be turned on and logs reviewed on a regular basis • password/authentication controls associated with the login software must be implemented • remote logging of the system must be implemented • where possible, vendor access should be limited to test and development servers			✓
4.3.7	Trust relationships (for authentication purposes) between systems that are based on DNS response or IP information are a security risk, and their use should be avoided. Cryptographically secure mechanisms should be used instead. If trust relationships are necessary, they must be documented.			✓

4.4 Operating System

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.4.1	Include a visible statement on all screens where login prompts are presented to potential users containing words to the effect of "Unauthorized access or use of this system is prohibited."	✓	✓	

4.4.2	Include a visible statement on all screens where login prompts are presented to potential users containing words to the effect of "You are about to access a Duke University computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution."			✓
4.4.3	Login scripts should indicate the last login date and time as verification to the user that no unauthorized access has been attempted using that ID.		✓	✓
4.4.4	Implement facilities to disconnect inactive logins, and document the timeout period.	✓	✓	✓
4.4.5	Strip all banner and error messages that are produced by remote services and are visible to users of administrative information about the system (such as operating system, version numbers, installed applications, and patch levels) whenever possible.			✓
4.4.6	Remove or disable all services and applications that will not be used. Document any exceptions.	✓	✓	✓
4.4.7	Mitigate all relevant vendor announced vulnerabilities within 2 weeks on systems with Sensitive data, and within 4 weeks on systems with Restricted or Public data. Mitigation make take many forms including establishing that the vulnerability does not impact the service, applying patches, adding new port blocks or firewall rules, or implementing other compensating controls. Document exceptions.	✓	✓	✓
4.4.8	Install anti-virus software and configure it to automatically check for updated virus signature and component files. Configure anti-virus software to perform a full scan of the system on a regular basis as well as to scan incoming and outgoing files for viruses. Any systems for which there is not AV available may be documented as exceptions.	✓	✓	✓
4.4.9	Servers must only use operating systems currently supported by the vendor (i.e. operating systems where security updates and patches are still available). Exceptions can be made for legacy systems that will be retired within the next six (6) months, if there is a plan in place to mitigate risks caused by running an unpatched system.	✓	✓	✓
4.4.10	Disable or block web browsers at a host firewall level for systems that do not receive OS updates using a browser.	✓	✓	✓
4.4.11	Routine down times to support vulnerability mitigation should be scheduled as appropriate.	✓	✓	✓
4.4.12	Device status updates related to antivirus, patch levels, hard drive encryption, and other controls must be reported to a management console and reviewed regularly (managed and reviewed by OIT or by the department).		✓	✓

4.5 Data

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.5.1	Overwrite all data from all hard drives before the disposal of old equipment. All campus machines with hard drives are also required to go through Duke Surplus whose policy is to clean or destroy hard drives. More information regarding disk wiping can be found at here [4].	✓	✓	✓
4.5.2	Server documentation must include information identifying the protected data stored in or processed by that system.			✓

4.5.3	Only encrypted channels may be usd to access protected data. If that is not possible, steps must be taken (and documented) to prevent user ID, authentication information, and data disclosure.		✓	✓
4.5.4	Limit access to protected data to those whose access has been approved by the data owner.		✓	✓
4.5.5	Run a data integrity checker on servers to assist with the verification of system security and data integrity. Review the integrity checker reports daily for any inconsistencies.			✓
4.5.6	Remove all production data from test or development systems.		✓	✓
4.5.7	Do not store SSNs without the explicit approval of the CIO.			✓
4.5.8	If the system stores or processes ePHI as defined by HIPAA, you must implement a mechanism to encrypt and decrypt ePHI.			✓

4.6 Applications

All items in this section apply to any applications as defined above - including but not limited to databases, web applications, client/server applications.

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.6.1	Apply application security patches within 2 weeks of release on systems with Sensitive data, within 4 weeks on systems with Restricted or Public data. If this is not practical due to business needs, a plan for mitigating the security risk must be documented.	✓	✓	✓
4.6.2	When deploying production servers, uninstall or disable all development tools, examples, code samples, and any other applications that aid in development, but are not necessary in a production environment.	✓	✓	✓
4.6.3	For applications and web applications developed by or for Duke, include security in the initial design phase of the software development cycle (SDLC).		✓	✓
4.6.4	Use a sandboxed or managed code environment for development.		✓	✓
4.6.5	Use de-identified data for development and testing.			✓
4.6.6	Follow the principle of least privilege, meaning that applications have access to do only what they need to do. For example, restrict or remove administrative access to production applications when possible. If administrator's access is built-in consider stricter controls for such access.	✓	✓	✓
4.6.7	If the application needs a username and/or password to log into some other service as part of its function, those credentials should not be stored in the same file as the program source code.	✓	✓	✓
4.6.8	If the application stores user password information, it must do so as a salted, cryptographically secure hash (3DES minimum).	✓	✓	✓
4.6.9	Publicly available applications must not execute OS shell commands, and must not pass non-administrative user input to the shell.	✓	✓	✓
4.6.10	A code review by someone other than the developer(s) should be performed before and application is moved into production.			✓

4.6.11	Remove comments and commented code from all production applications.	✓	✓	✓
4.6.12	Remove same scripts from all production applications.	✓	✓	✓
4.6.13	Remove development tools from all production applications.	✓	✓	✓
4.6.14	Do not use shared user accounts (such as DukeUser1) in production applications.	✓	✓	✓
4.6.15	Do not post production code that might provide configuration information to public mailing lists.	✓	✓	✓
4.6.16	For web applications, disable path traversal and directory browsing; place index files in each of the web directories. You can also look closer at your specific server settings such as setting permissions in an .htaccess file.	✓	✓	✓
4.6.17	Encrypt any web application data passed to a client, e.g. use SSL. (Data passed to a client, such as cookies, session IDs, or hidden fields are modifiable by the client.)		✓	✓
4.6.18	Use a standard input validation mechanism in web applications to validate all input data for length, type, syntax, and business rules before accepting the data to be displayed or stored. Use an "accept known good" validation strategy. Reject invalid input rather than attempting to sanitize potentially hostile data. Do not forget that error messages might also include invalid data.	✓	✓	✓
4.6.19	If a web application is using Duke credentials, verify that all exchanges of usernames/passwords are encrypted from the web server to other Duke servers. Audit web directories for unused files and remove them	✓	✓	✓
4.6.20	Do not rely on robots.txt files for security - it is a map to interesting pages for some users.		✓	✓
4.6.21	Protect against all the top vulnerabilities on the current OWASP list.	✓	✓	✓
4.6.22	Programmers/developers must keep up-to-date with emerging security threats that affect applications and web applications, and should complete annual security awareness training on secure development. It is recommended that developers achieve (and keep current) certification for secure programming or web application security through SANS or other professional organizations.			✓
4.6.23	Implement a web application firewall.			✓

4.7 User

Password Management
When a password policy cannot be enforced automatically (for example, if NetID is used for authentication), it is the user's responsibility to follow departmental password management guidelines or policies, i.e. change passwords on regular basis, use password complexity, etc.

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.7.1	Encrypt (or hash with salt) any passwords stored on a campus server (3DES minimum).	✓	✓	✓
4.7.2	In addition to specific password complexity requirements, password age and password reset policies should be implemented and documented for departmental servers (see recommended Password Management definitions).		✓	✓

4.7.3	Two-factor authentication and digital certificate-based authentication are recommended where practical.			✓
4.7.4	Use campus Identity Management services for authentication and document exceptions.			✓

Account Management
User Accounts

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.7.5	Only the person to whom it is assigned must use a user account. The password and other credentials associated with a user account must not be shared with anyone. Each user account holder (including requestors of accounts for vendor access) is responsible for all actions accomplished with his/her account and password, including unauthorized access that results from negligence in maintaining password secrecy.		✓	✓
4.7.6	Individually authenticate all access to systems containing protected data.		✓	✓
4.7.7	Review all user accounts and group memberships on servers at least monthly and disable or delete them when no longer required on systems with Sensitive or Restricted data. Review all user accounts every 6 months on systems with Public data. Document the account list used and how it is obtained.	✓	✓	✓
4.7.8	Supervisors of account holders are responsible for notifying systems administrators of the need to delete accounts.	✓	✓	✓
4.7.9	System administrators must delete or lock such accounts within one business day of the request.		✓	✓
4.7.10	Abandoned (unused) accounts must not be left active for more than 3 months.		✓	✓
4.7.11	Strong authentication is required on user accounts. OIT's password requirements for NetIDs are a good minimum standard: https://oit.duke.edu/help/articles/netid-password-sync-faq [5]	✓	✓	✓
4.7.12	Log changes to user accounts (e.g. group memberships, individual account permissions).		✓	✓

Administrator Accounts
An administrator account is a user account with administrative privileges.

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.7.13	Implement complex passwords or passphrases on all shared administrator accounts and log commands and events so that they are identifiable to a specific user.	✓	✓	✓
4.7.14	Change passwords regularly; recommended requirement is at least every 180 days.		✓	✓
4.7.15	Use of system accounts should follow the principle of least-privilege. For example, do not give administrative privileges when backup operator access is all that is needed.	✓	✓	✓
4.7.16	Do not use a Superuser account ('root', 'Administrator', etc.) as the use of	✓	✓	✓

	this account is difficult to individualize. Alternatives such as 'sudo' or 'Run As' allow for temporary privileged access and should be used wherever possible.			
4.7.17	Two-factor authentication and digital certificate-based authentication are recommended wherever practical.			✓

Service Accounts
Service accounts can be automatically created by applications or manually created run specific daemons or services. A service account (sometimes called a system level account) must be used only by the application for which it is originally authorized.

The shared secret and other credentials associated with a service account must not be shared with anyone or any other systems (aside from any documented exceptions). For manually created service accounts, service account sponsors are responsible for all actions accomplished with the service account and its credentials, including unauthorized access that results from negligence in maintaining credential secrecy.

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.7.18	Document all service accounts, including the reason for the account and who has access to it.	✓	✓	✓
4.7.19	Reassign any service accounts managed by a departing staff member and the change the passwords of the service accounts. If the staff member is terminated, revoke all account access within 48 hours or another (documented) time frame.	✓	✓	✓
4.7.20	Service account sponsors must review service accounts at least annually to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. This review must be documented.		✓	✓
4.7.21	Configure service accounts to be non-interactive when possible.	✓	✓	✓
4.7.22	Remove or disable all default service accounts that do not run a service or an application.	✓	✓	✓

4.8 Administrative

Req	Description	RISK/DATA		
		Public	Restricted	Sensitive
4.8.1	Authentication and authorization: Grant access to non-public IT resources by unique user credentials and require authentication. University-provided credentials (e.g. NetID and password, Windows ID and password, or other accounts) may not be shared between users. All University IT resources must use only encrypted authentication and authorization mechanisms	✓	✓	✓
4.8.2	All Duke-owned workstations and laptops must have a Duke system administrator.	✓	✓	✓
4.8.3	An operational group that is responsible for the administration of servers must register each server in the institutional DNS tables unless they maintain their own authoritative DNS services.	✓	✓	✓
4.8.4	Each server registration record in the authoritative network management database (currently, https://dukereg.duke.edu [6]) must be created and maintained by a responsible person. As an alternative, DNS RP (responsible person) record can be created.	✓	✓	✓
4.8.5	Administrators for the service must keep informed of security updates for the application(s) by either subscribing to an available mailing list or by regularly checking the vendor's website.	✓	✓	✓

4.8.6	Document configuration changes for production servers and follow appropriate change management procedures.	✓	✓	✓
4.8.7	The University IT Security Office runs scheduled vulnerability scans. As these scans are intended to assist administrators in understanding potential problems, they must not be explicitly blocked. For servers storing or processing Sensitive data, scans will be run every 2 weeks. For servers with Restricted or Public data, scans will be run every 4 weeks.	✓	✓	✓
4.8.8	When building a new system, all security patches must be installed on new systems before they are deployed on a public network.	✓	✓	✓
4.8.9	Review all vendor default settings and change default passwords before placing a system into production.	✓	✓	✓
4.8.10	Configure and document system security parameters (e.g. Windows GPO seetings).	✓	✓	✓
4.8.11	Recommended documentation for all department-managed servers includes: • Hardware information • Software installed • OS levels • Network connections • Security protections	✓	✓	✓
4.8.12	At least one administrator for the server must, at a minimum, receive CERT updates and preferably the applicable security updates for the operating system of the server.	✓	✓	✓
4.8.13	System administrators must regularly undergo security training. The University IT Security Office will assist departments when ever possible and will participate and sponsor training events when possible.	✓	✓	✓
4.8.14	Enable backups. OIT has a back up service: https://oit.duke.edu/what-we-do/applications/enterprise-tsm-backup [7]			✓
4.8.15	Document the backup process and restoration process (or lack of such processes for systems with Public data).	✓	✓	✓
4.8.16	Report all security-related events to security@duke.edu [3] within one (1) day of discovery.	✓	✓	
4.8.17	Report all security-related events to security@duke.edu [3] within three (3) hours of discovery and prior to any action taken (including a graceful shutdown of the system).			✓
4.8.18	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems.			✓
4.8.19	Establish (and implement as needed) procedures to restore any loss of data.			✓
4.8.20	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of Sensitve data while operating in emergency mode.			✓

Enforcement

It is the responsibility of server owners to ensure that the controls described in this document are implemented. IT administrators understand that the secure implementation of servers is a critical part of Duke's overall information security strategy.

Campus departments undergo periodic internal and external audits. These audits typically include an analysis of the processes and controls used by departments to secure and manage servers. The Office of Internal Audits carries out internal audits. The initiation of an internal audit is based on a risk analysis, also performed by the Office of Internal Audits. A requirement for an external audit may be recommended as a result of the internal audit, or be requested independently by a department's management. The department is responsible for remediation of any findings of non-compliance with this standard within the time frame agreed to with the auditors.

Recommended Departmental/Organizational Policies

In addition to documenting the configuration of a mobile device, the services it provides, and any customizations to the ITSO Mobile Device Security standard for business operations, departmental IT staff should also work with their management to create the following departmental policies:

1. Account, Access, and Data Management policy (ITSO template)
2. Asset Management policy (ITSO template)
3. Back Up, Disaster Recovery, and Emergency Access policy (ITSO template)
4. Service Acceptable Use policy for any services the department provides (ITSO template)
5. Logging policy (Duke Log Standard [8])

Review Frequency: Annually
Updated: 06/13

In Compliance with:
Duke University Data Classification Standard [9]
Duke University Acceptable Use Policy [10]
Duke University Log Standard [8]

References:
University IT Security Office website: http://www/security.duke.edu [11]
Center for Internet Security: http://cisecurity.org [12]
National Institute for Standards and Technology: http://www.nist.gov [13]
SANS Institute: http://www.sans.org [14]

Document Type: Standard**Applicable To:** Duke University

Source URL: https://security.duke.edu/secure/policies/server-security-standard

Links
[1] https://security.duke.edu/secure/policies/server-security-standard
[2] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
[3] mailto:security@duke.edu
[4] https://security.duke.edu/policies/media-control-and-disposal
[5] https://oit.duke.edu/help/articles/netid-password-sync-faq
[6] https://dukereg.duke.edu
[7] https://oit.duke.edu/what-we-do/applications/enterprise-tsm-backup
[8] https://security.duke.edu/secure/policies/log-standard
[9] https://security.duke.edu/policies/data-classification-standard
[10] https://security.duke.edu/policies/acceptable-use
[11] http://www/security.duke.edu
[12] http://cisecurity.org
[13] http://www.nist.gov
[14] http://www.sans.org