

University IT Security Office Standard: Server Security

Version 3.0

September 1, 2009

1. Definitions

Application: Any software that runs on a computer or other networked device and is used by end users or other applications or devices.

Departmental staff or University 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.

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 or Restricted by the Duke framework.

Sensitive and Restricted Data: as defined in the Duke University Information Classification Framework.

Server: A server is any device with an active network connection which provides services or resources to users and/or to other systems. Touchscreen panels which control other devices, video and audio storage devices, and desktop or lab machines which act as servers should follow this standard. Desktop systems which only provide services intended for one primary user or the administrators of the computer are not included in this standard.

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).

2. 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 regulations 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 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 which 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, all customizations should be documented by the systems administrators.

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

3. 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 organizational groups.

4. Server/Service Standard

4.1 Overview

When it comes to security, a layered approach, also known as "defense in depth" works best. With a layered approach, even if an intruder is able to bypass one security control, overlapping layers of security ensure 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. To emphasize this principle, this document is organized in the following conceptual layers:

- Physical
- Network
- Operating System
- Data
- Application
- User
- Administrative

The method for addressing each of the above security layers must be documented and kept up-to-date to reflect changing conditions.

4.2 Physical Required

- Servers must be physically located in an access-controlled environment.
- Physical access must only be granted to authorized individuals and accompanied service personnel.

Recommended

- Physical access to the access-controlled environment should be logged.

4.3 Network Required

- All server operating systems for which there are commercial or publicly available hostbased firewalls (e.g. ipfilters, iptables, Windows IPsec, etc.) must run these firewalls or appropriate TCP wrappers.
- Firewall/TCP Wrapper rule sets must allow access to only those ports which are necessary to provide service and to maintain the servers. All rule sets must be in 'default deny' configuration.
- Network based access to the server must be logged where feasible.
- Privileged access must be performed 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 any instances of unencrypted privileged access must be explicitly approved by departmental management.
- For vendor access to servers (whether via modem, Internet or other means), the following safeguards must be implemented:
 - contractual understanding of the responsibilities of the vendor is fully documented
 - access for the vendor is enabled when needed and disabled when the vendor's work is completed
 - 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
- Departmental servers must prohibit the unencrypted transport of authentication information and other protected data across the Duke network or the Internet. Alternatives can be implemented based on the type of access needed (examples include sFTP, SCP, SSH and SSL encapsulated protocols).

Recommended

- Trust relationships between systems which 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.
- For vendor access to servers (whether via modem, Internet or other means), the following safe guards must be addressed:
 - where possible, vendor access should be limited to test and development servers
- Screens where login prompts are presented to potential users should include a visible statement containing words to the effect of "Unauthorized access or use of this system is prohibited."
- Banners and error messages that are produced by remote services and are visible to users should be stripped of information about the system (such as operating system, version numbers, installed applications, and patch levels) whenever possible.

4.4 Operating System

Required

- All security-related events must be logged. Decisions regarding events that are not to be logged MUST be documented.
- Remote logging must be enabled.
- Log retention periods (based on log sensitivity and size) for each server/service must be documented.
- Logs must be reviewed on a regular basis, although some log types (e.g. mail) may only require review in the event of an anomaly.
- Security-related events on systems containing Sensitive or Restricted data must be reported to security@duke.edu within three (3) hours of discovery and prior to any overwriting of evidence. Other security related events must be reported to security@duke.edu within one day.
- Services and applications that will not be used must be disabled.
- Relevant vendor announced vulnerabilities must be examined and mitigated within 2 weeks. Mitigation may 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.
- Anti-virus software must be installed on servers running a Windows operating system, and configured 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.
- Servers on the campus networks must 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 are expected to be retired within the next six (6) months, if there is a plan in place to mitigate the risk caused by running an unpatched system.

Recommended

- Events related to the operating system should be logged.
- Web browsers should be either disabled or blocked at a host firewall level for systems that do not receive OS updates using a browser.
- Routine down times to support vulnerability mitigation should be scheduled as appropriate.
- Server or network login scripts should be used to indicate the last login date and time as verification to the user that no unauthorized access has been attempted using that ID.

- Facilities to disconnect inactive logins should be implemented, and the timeout period documented.

4.5 Data

Required

- All data must be removed from hard drives before disposal of old equipment. All campus servers are required to go through Duke Surplus whose policy is to clean or destroy hard drives. Note that a simple delete or even reformat is not enough to destroy data, an overwrite of the data is required. More information regarding disk wiping can be found at: <http://www.security.duke.edu/mediaguidelines.html>.
- Any access to protected information must be over encrypted channels where possible. If not possible, steps must be taken (and documented) to prevent user id, authentication information, and data disclosure.
- Server documentation must include information identifying the protected information stored in that system.

Recommended

- Servers should run a data integrity checker to assist with the verification of system security and data integrity. The integrity checker should be run nightly and the reports reviewed daily for any inconsistencies.

4.6 Application

Required

- Application logging, including access logs on servers which store protected information, must be enabled where available.
- Application security patches must be applied within 30 days of release. If this is not practical due to business needs, a plan for mitigating the security risk must be documented.

Recommended

- When deploying production servers, all development tools, examples, code samples, and any other applications that aid in development, but not necessary in production environment, should be either uninstalled or disabled.

4.7 User

User Password Management

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). Two-factor authentication and digital certificate-based authentication are recommended where ever practical. 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. Encrypt (or hash with salt) any passwords stored on a campus server.

User Accounts

Required

- All access to systems containing protected information must be individually authenticated.
- All local end-user accounts on the server must be reviewed at least monthly and disabled or deleted when no longer required.
- Supervisors of account holders are responsible for notifying systems administrators of the need to delete accounts.
- System administrators must delete or lock such accounts within one business day of the request.

Recommended

- Abandoned (unused) accounts should not be left active for more than 3 months.
- User accounts should require strong authentication such as a complex password (information regarding what makes for a strong password can be found at <http://www.security.duke.edu/password.html>).

Administrator Accounts

Required

- Shared administrator accounts must utilize complex passwords or passphrases (see <http://www.security.duke.edu/password.html>).
- Passwords must change regularly, such as within every 30 days.
- Passwords must be changed immediately when an administrator with access to the shared account leaves their administrative role.

Recommended

- Two-factor authentication is strongly recommended.
- 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.
- Use of a Superuser account ('root', 'Administrator', etc.) should be minimized 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.

4.8 Administrative

Required

- All servers deployed by departmental IT staff must be maintained by operational groups that are responsible for system administration.
- 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.
- Each server registration record in the NetReg database (<https://netreg.duke.edu>) must be created and maintained by a responsible person. As an alternative, DNS RP (responsible person) record can be created.
- 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.
- Configuration changes for production servers must be documented and follow appropriate change management procedures.
- 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.
- Documentation for all information system hardware and software installations, connections to the network (including wireless), maintenance, and security testing must be maintained.
- Security incidents must be reported to the University IT Security Office. If the incident occurs on a system with protected information, the reporting must occur within three hours and before any effort is made to restore the server or reinstall the operating system.

Recommended

- At least one administrator for the server should, at a minimum, receive CERT updates and preferably the applicable security updates for the operating system of the server.
- The department should provide security training for system administrators and end users regularly. The University IT Security Office will assist departments when ever possible and will participate and sponsor training events when possible.

5. Enforcement

It is the responsibility of server owners to ensure that the controls described in this document are implemented. It is expected that the secure implementation of servers is a part of everyone's job within the department.

Campus servers will undergo periodic internal and external audits. Internal audits are carried out by the Office of Internal Audits. The initiation of an internal audit should be 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 indicated by the auditors.

Based on industry standards and practices:

SANS Software Security Institute
Center for Internet Security benchmarks (cisecurity.org)
National Institute of Standards Technology (NIST)

Review Frequency: Annually

Updated: 8/09

Authority:

Duke University Chief Information Officer
Duke University Chief Information Security Officer

In Compliance with:

Duke University Information Classification Framework

Other resources:

University IT Security Office website: <http://www.security.duke.edu>
Center for Internet Security: <http://cisecurity.org>
National Institute for Standards and Technology: <http://www.nist.gov>
SANS Institute: <http://www.sans.org>