

OIT Information Security Standard: Server Security

Version 2.0

September 8, 2006

1 Definitions

- **Server** - For purposes of this standard, a server is defined as a system that provides services or resources to user communities or other systems. Desktop systems or lab machines that act as servers will follow the server standards. Desktop systems which only provide services intended for the 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).
- **Individual Administrator Account** - Accounts that are system-level accounts and are not predefined by the vendor. Although it has full privileges it is individualized.
- **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 service and does not necessarily refer to broader authentication schemes such as the Duke NetID.
- **Sensitive Data** - There are a number of regulations defining sensitive data, however, for purposes of this document, sensitive data is defined as a person's name and any of the following:
 1. Information that could be used to impersonate a person or allow unauthorized access to their personal information (such as Social Security number, taxpayer ID number, driver's license number, state id card number, passport number, passwords, finger prints and other biometrics, mother's maiden name, PIN, digital signature, etc.);
 2. Information in a student education record (such as family members' name(s), family address, personal identifiers such as SSN or student number, courses, grades, etc.);
 3. Protected health information (information that relates to either the physical or mental health of an individual, or the provision of health care to an individual, or an individual's payment for health care); or
 4. Financial information (e.g. credit or debit card numbers, checking or savings account information, salary, etc.)
- **SHOULD** - Used to indicate items which are highly recommended, but not mandatory. Departments or work groups will want to determine where the items are applicable and feasible to their service.
- **MUST** - Used to indicate items which are required under the OIT Server Security Standard. If a department or work group believes that these items are not feasible for their service, then the issues need to be documented and discussed with the IT Security Office.

2 Purpose

The purpose of this policy is to establish standards for the base configuration and management of servers owned and/or operated by the Office of Information Technology at Duke University (OIT). Effective implementation of this standard should minimize the likelihood of unauthorized access to OIT computing resources and confidential information. However, all such security events must be reported to security@duke.edu in order to ensure compliance with legal obligations

As there are a wide variety of operating systems, software and system configurations used within OIT, this document is NOT intended as a “How-To” on system security. Instead, this standard is intended to note areas 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 this standard before being put into production.

3 Scope

This standard applies to all server equipment (as defined above) administered by OIT staff or attached to subnets where OIT maintains servers housing sensitive data.

4 Enforcement

It is the responsibility of the departments operating the service to ensure that the controls described in this document are implemented. It is expected that the secure operation of services is a part of everyone’s job within OIT. Adherence to the standard should be considered a part of each employee’s job performance and should be evaluated as such for the purposes of performance reviews.

5 Exceptions

All OIT servers covered in the scope of this document are expected to adhere to this standard. Any request for an exemption from the standard MUST be based upon business need and MUST be submitted to the University IT Security Office. Approval for such exemptions will be determined by the IT Security Office and the OIT Management Team.

6 Server/Service Standard

6.1 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 and Database
- Application
- User
- Departmental

The department's method for addressing each of the above security layers **MUST** be documented and kept up-to-date to reflect changing conditions.

6.2 Physical

- Servers **MUST** be physically located in an access-controlled environment
- Physical access **MUST** only be granted to authorized individuals and accompanied service personnel
- Physical access to the access-controlled environment **MUST** be logged

6.3 Network

- All server operating systems for which there are commercial or publicly available host-based 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 the service and to maintain the servers.
- Network based access to the server **MUST** be logged where feasible.
- Trust relationships between systems which is based on DNS response or IP information are a security risk, and their use **SHOULD** be avoided. Cryptographically secure mechanisms **SHOULD** be used instead.
- 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. Private networks (networks using non-routed IP addresses and which are physically isolated) may be a reasonable substitute for encryption.
- 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
 - contractual understanding of the responsibilities of the vendor
 - access for the vendor is enabled when needed and disabled when the vendor's work is completed
 - access to the server **MUST** require 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 available
 - deviation from the above **MUST** be discussed with and agreed to by the IT Security Office.
- Screens where login prompts are presented to potential users **SHOULD** include a visible statement containing words to the effect of "Unauthorized use of this system is prohibited."
- OIT servers **MUST** prohibit the unencrypted transport of authentication information and other sensitive data across the Duke network. Alternatives **SHOULD** be made available based on the needed access to the server, examples include sFTP, SCP, SSH and SSL encapsulated protocols.

6.4 Operating System

6.4.1 Logging

- All security-related events **MUST** be logged. Other events related to the operating system **SHOULD** also be logged. Decisions regarding events that are not to be logged **MUST** be documented.
- Remote logging **MUST** be enabled. Remote logging software exists for all known operating systems currently used at Duke. There is no longer a technical reason not to log remotely.

- 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. Several programs exist which allow for a consolidated view of log information (e.g. swatch and epylog).
- Security-related events on systems containing confidential or sensitive information 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.

6.4.2 Additional

- 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 or adding new port blocks or firewall rules. Routine downtimes to support such mitigation SHOULD be scheduled as appropriate.
- If the facilities are available, 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 where these systems make sense.
- Anti-virus software MUST be installed on servers running the Windows operating system, and SHOULD be configured to automatically check for updated virus signature and component files. Anti-virus software SHOULD be configured 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 OIT network 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.

6.5 Data and Database

- 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.
- All sensitive data, such as social security numbers and financial data, MUST be removed from hard drives before disposal of old equipment. If any equipment is being sold off or donated to another individual/department, it needs 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/media-guidelines.html>
- Database access to sensitive or confidential information MUST be over encrypted channels where possible. If not possible, steps MUST be taken to prevent userid, authentication information and confidential data disclosure.
- Server documentation MUST include information identifying the sensitive or confidential information stored in that system.

6.6 Application

- Application logging, including access logs on servers which host sensitive or confidential 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 requirements, a plan for mitigating the security risk MUST be discussed with the IT Security Office.

6.7 User

- End User Accounts
 - All authenticated server access to systems containing sensitive or confidential information **MUST** be **individually** authenticated.
 - All 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.
 - Abandoned (unused) accounts **SHOULD** not be left active for more than 3 months.
 - User accounts **SHOULD** require strong authentication such as a strong password (information regarding what makes for a strong password can be found at www.security.duke.edu/password.html).
- Administrator Accounts
 - Shared administrator accounts **MUST** require strong authentication. Additionally, these accounts are subject to the following requirements:
 - * Authentication tokens (e.g., passwords) **MUST** change regularly
 - * Authentication tokens **MUST** be changed immediately after employee turnover
 - 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 Unix's root and Windows' administrator accounts **SHOULD** be minimized as the use of these accounts is difficult to individualize. Alternatives such as 'sudo' or 'Run As' allow for temporary privileged access and **SHOULD** be used wherever possible.

6.8 Departmental

- All internal servers deployed by OIT **MUST** be maintained by operational groups that are responsible for system administration.
- An operational group that is responsible for the administration of the system **MUST** register each server in the DNS tables.
- DNS entries **MUST** contain a valid rp (responsible person) entry and an email account (preferably a group account) for contact with system administrators.
- At least one administrator for the server **SHOULD**, at a minimum, subscribe to the CERT mailing list and preferably the applicable security mailing list for the operating system of the server.
- 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 security testing. As these scans are intended to assist administrators in understanding potential problems, they **MUST** not be *explicitly* blocked. Furthermore, departments **SHOULD** periodically run (or work with the IT Security Office to run) more comprehensive scans.
- 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 IT Security Office. If the incident occurs on a system with sensitive or confidential information, the reporting **MUST** occur within three hours and before any effort is made at restoring the service or reinstalling the operating system.

7 Reference

Any questions on this standard should be referred to security@duke.edu.

Standard does NOT apply to the following OIT departments or workgroups:

Developed by: IT Security Office

Scheduled Review Date: March 15, 2007