Policy Title: Server Security Policy	**Policy Number:**
Date Issued: February 25, 2005	**Responsible Executive: Vice President of Information Technology**
Date Last Revised: April 2, 2020	**Responsible Office: Information Technology Services**

Server Security Policy

Policy Statement

This policy is for all computer system administrators managing a computer server connected to the Baylor University ("Baylor" or the "University") network. This policy defines common sense security practices expected of all computer server administrators.

Reason for the Policy

Every server administrator at Baylor must take reasonable security measures to secure their hosts as outlined in this policy. Computer security is not something that is done once a year, once a month, or even once a day. It is the frame of mind that there are real threats and that part of the job includes keeping users, data, and transactions safe from these threats.

Individuals/Entities Affected by this Policy

This policy addresses any server connected to the Baylor University network providing any type of service to other users.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

Password Policies
Incident Response Policy

Forms and Tools

Forms and tools are available at www.baylor.edu/its/.

1. Server Security Policy

Contacts

Subject	Contact	Telephone	Office email/web site
Support	ITS Help Desk	254-710-4357	https://www.baylor.edu/its/index.php?id=44608

Responsibilities

Server Administrators	A server administrator, upon connecting their server to Baylor's network, is responsible for the security of that device in accordance with ITS guidelines. An administrator is held accountable when a compromise occurs. It is also expected that the administrator will demonstrate reasonable precautions to ensure the security of their hosts.

Principles

Server Location

Servers should be placed in physically secured areas accessible only to authorized personnel. There is no substitute for physical security.

Services Supported

Administrators should run only services on a server that are needed for it to complete its designated task. Every service running should be regarded as a mode of entry. The number of entry points should be limited to only those needed.

Note: The chance that a computer will be compromised is increased with the number of services being run. Therefore, it is expected that every administrator knows exactly what and why services are running.

Security Updates

The latest system patches should be applied regularly.

Note: Security related patches for systems often mean that there has been a successful exploit of a particular vulnerability. The vulnerability of a system is directly proportional to the age of the patches. The longer one waits before applying a patch, the more likely it is that it will be successfully exploited. It is not uncommon to have a three-month-old vulnerability incorporated into an automated tool that thousands of hackers use. Patching a system is something that should be done on a regular schedule and immediately if a threat has been reported. At some point, if patches are not applied in a timely manner, the server could be disconnected from the network until vulnerabilities have been addressed.

Virus Protection

It is expected that administrators regularly scan all servers with updated virus detection software.

Log-on Limits

Administrators should limit log-on retries.

Note: Password guessing applications have a greater probability of cracking a password if given ample opportunity. For most situations, Information Technology Services recommends account lockout after three failed log-on attempts.

Account Reviews

Accounts must be regularly reviewed for inactivity, and any dormant accounts disabled.

Note: Old accounts should be terminated regularly. When people leave the University, administrators should have a clear deadline for account termination. Dormant (unused for more than 60 days) accounts make attractive targets to intruders, since no one will likely notice the activity.

Local Accounts

Whenever possible, accounts should be located on and authenticated against a Kerberos, NTLM, LDAP or Active Directory based infrastructure. Administrators should only use local accounts when absolutely necessary.

Note: In most cases, local accounts are not scrutinized as closely as directory based accounts and thus more susceptible to attack by automated tools.

Privileged Accounts

Special care should be taken with privileged accounts (including but not limited to “root” for UNIX and “administrator” for NT), commensurate with the privileges afforded the account. Passwords for privileged accounts should be given only to people with a need for privileged access. For NT servers, the “administrator” account should be renamed.

Note: Failing to change the name of the account gives would-be intruders half the equation to compromising the server. All privileged server accounts should be password protected.

Password Protection

All accounts must conform to the Baylor University Password Policies.

Service Banners

Wherever feasible, a log-on banner, stating that the system is for authorized use only, should be displayed for anyone attempting to connect to the system.

Note: If possible, log-on restrictions (by time of day, by system address, etc.) should be implemented. All operating system, version/release numbers, and vendor information provided in log-on/sign-on banners should be limited or disabled. Providing this information makes attacks easier by allowing intruders to pinpoint hosts with known security vulnerabilities.

Backups

Information Technology Services encourages server administrators to maintain backups on all servers for 30 days.

Note: In the event of a security breach, backups are important to track down when changes occurred and which files were modified. Backups are also important to restore a server to its configuration before the intrusion occurred (i.e. no code is present which was inserted during the intrusion).

Server Logs

Logs of user activity must be retained for a period of time.

Note: ITS recommends that these logs be kept for at least six months. Logs should include (where feasible) the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.). Logs should be checked for signs of malicious activity on a regular daily or weekly basis. Knowledge that logs are kept acts as a deterrent to abuse. Logs are also essential in investigating incidents after the fact. Many attempted break-ins can be detected early, and sometimes prevented, by early detection of unusual activity.

Sensitive Information

Baylor University Information Technology Services must be made aware of any server that contains sensitive data. This includes, but is not limited to, social security number, credit card numbers, grades, and other personal data.

Note: Extra precaution must be taken with systems containing sensitive data. As a result, proof of compelling reasons that a system needs to contain private information may be requested by the Office of General Counsel.

Remote Administration

In order for a vendor or consultant to gain access to a server from off campus, they must be assigned a VPN account. The system administrator is responsible for registering the vendor or consultant before the VPN can be assigned. In addition, the vendor or consultant may be required to sign a non-disclosure agreement before gaining access to a server.

Note: Many servers require administration by outside vendors or consultants. In these cases, it is preferred that this outside access be obtained by using a VPN account. The account allows for secure remote access to the server. In the case of Windows servers, Terminal services should be used through the VPN connection to administer the server. Unix, Linux, or Mac servers should use SSH.

Incident Response

A server administrator must read and understand the Baylor University Incident Response Policy.

1) The server will be analyzed by Information Technology Services and the server administrator to attempt to determine the method by which the server was compromised.
2) If it has been determined that the server was compromised, then the server's system volume will be reformatted. The operating system will be reinstated with the latest security patches.
3) The server must pass a security scan before being reconnected to the Baylor network.

Incident Confidentiality

Information regarding security incidents will be kept confidential by all parties involved. Only authorized personnel may disclose such information.

Compliance

Information Technology Services reserves the right to scan systems for known vulnerabilities. When vulnerabilities are discovered, it is expected that administrators will immediately act to close all known security vulnerabilities for which there are reasonable methods to close such vulnerabilities. If the administrator is unable to do this in a timely

fashion, it is expected that they will remove the server from the network to protect other systems.

Enforcement

All servers should be registered with Baylor Information Technology Services. For registration information, click ITS Forms Library.

Note: All server administrators must notify Information Technology Services of servers running in their department. This registration will require names and phone numbers of people to call in emergency situations including contact information during semester breaks. When security related issues arise and this information is not available, there may be no choice other than to disconnect a server without notice. Information Technology Services must be notified upon discovery of any system breach or suspected system breach. Information Technology Services reserves the right to disconnect any server which poses a threat to the campus network. Any server not following the above procedures will be considered unsafe, and as such, poses a threat to the campus network and other systems.