

Server Hardening Policy Statement

Servers are depended upon to deliver data in a secure, reliable fashion. Data integrity, confidentiality and availability must be maintained. Servers must be installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Purpose

The purpose of this policy is to describe the requirements for installation and operation of a server in a secure fashion, maintaining the security integrity of the server and application software.

Responsibilities

The policy applies to all individuals that are responsible for the installation of new Information Resources (IR) for academic, administrative, research or business outreach purposes, the operations of existing Information Resources, including but not limited to Custodians of IR, and individuals charged with IR Security.

Policy for Server Hardening

A server must be accepted by Information Services (IS) and registered in Active Directory before it is connected to and operational on the Bryant network. At the time of registration an individual and/or department will be identified and assigned by IS as owner and custodian.

- At the time of registration, and at periodic intervals thereafter, all servers will be classified by the owner or the custodian on behalf of the owner, as Mission Critical (MC) or Non-Mission Critical (NMC). If ANY information stored or processed by the server can be classified as MC, then the Server is MC.
- All servers, as Information Resources whether MC or NMC, are subject to the University's Acceptable Use and Network Access Policies.
- All servers, whether MC or NMC, are subject to the following rules:
 - Only authorized and approved software may be installed.
 - Servers must be part of the campus Active Directory Domain.
 - Custodian(s) will install and maintain current Anti-Virus software according to policy.
 - All systems shall display a logon banner with warning statements that include the following:
 - Unauthorized use is prohibited;
 - Usage may be subject to security monitoring and testing;
 - Misuse is subject to criminal prosecution;
 - No expectation of privacy except as otherwise provided by applicable privacy laws

- Custodian(s) will take necessary steps to ensure that the Operating System (OS) is kept secure according to the current Standards for OS Platform Hardening maintained by Bryant University IS Division, including, but not limited to:
 - Resetting of default passwords.
 - Installation of security patches in a timely manner, or as required in an emergency situation.
 - Deactivation and/or de-installation of unnecessary software or services.
 - Activation of OS and application software security controls which establish protection of the server and data.
 - Anti-virus protection installed (Windows OS).
- Owners and/or Custodians must maintain an Incident Response, Disaster Recovery and Business Continuity Plan commensurate with the impact of a failure or loss of the server, in accordance with the University's Backup, Disaster Recovery and Business Continuity policies.
- Servers classified as Mission Critical (MC) are subject to the following additional rules:
 - Reside in the data center (a physically secure environment).
 - Custodian(s) must implement appropriate access controls and the corresponding documented approval procedures which assure the protection of data against unauthorized access.
 - Custodian(s) must maintain auditing and security logs which record and archive security events necessary to fulfill the requirements of the Incident Response Policies.
 - Custodian(s) will implement Change Control procedures which assure the integrity of data and applications, in accordance with the IT Change Control Policies.
 - Custodian(s) will maintain any additional security controls such as host based Intrusion Detection software, security key management, etc.
- Custodian(s) of Mission Critical servers must have appropriate training and/or certification as specified by Bryant IT for the hardware and software.

All servers are required to pass a vulnerability assessment performed by the Computer Operations group prior to use. Administrators are required to correct all network/operating system vulnerabilities identified as high or medium risk during the vulnerability assessment. Examples of medium or high risk issues would include:

- Accounts with blank or weak passwords
- Outdated version or patch levels of server software and services.

The Computer Operations group will monitor the release of security patches and routinely monitor to ensure systems are in compliance. Failure to comply with patch guidelines can result in server(s) being removed from the network.

Computer Operations will perform due diligence in testing security patches before release when practical.