BOISE STATE UNIVERSITY

University Policy 8020

Enterprise Servers and Storage

Effective Date

November 1997

Last Revision Date

January 11, 2023

Responsible Party

Office of Information Technology, (208) 426-4357
Executive Director of Cloud Service and Infrastructure, (208) 426-5655
Chief Information Security Officer, (208) 426-4127

Scope and Audience

This policy applies to all colleges, departments, and units, including all computing devices located at or controlled by Boise State University.

1. Policy Purpose

To protect University data, provide a reliable network, and reduce the risk of data loss or loss of service due to absence or loss of personnel, disasters, or other incidents.

2. Policy Statement

Boise State University is committed to maintaining effective, efficient, reliable, and secure management of its Servers consistent with the mission and goals of the university. To support a reliable network, all users of the university's Information Technology (IT) resources are expected to follow the guidelines in this policy.

3. Definitions

3.1 Best Practices

Data management and network procedures generally recognized by the industry for ensuring secure, reliable, scalable, and efficient data repositories and networks.

3.2 Servers

Computers explicitly purchased to provide services to other computers on the network. These services include, but are not limited to file sharing, printing, database access, e-mail, web services, authentication, and any other applications that are accessible via the network. These Servers can be either physical, standalone devices, or housed in virtual environments with hypervisor software and includes all operating systems and manufacturers.

3.3 Network Attached Storage and Derivatives

Network-attached storage (NAS) is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity. Users on a local area network (LAN) access the shared storage via a standard Ethernet connection.

4. Minimum Security Standards for Systems

a. All Servers must adhere to the Boise State University Minimum Security Standards for Systems. This standard defines the criteria needed for all Servers and additional criteria for systems that contain Level 1 Data. At minimum, all systems need to be documented, protected, backed-up, and refreshed on a regular basis. Any incident involving a server is subject to the Incident Handling and Reporting response.

b. Acquisition of Servers and Network Attached Storage and Derivatives is only done by the Office of Information Technology (OIT). OIT is responsible for installing, configuring, managing, and administering all on-premise and cloud Servers and storage installed in the network. On-premise and Cloud Servers, as well as Network Attached Storage and Derivatives acquired without an exception to policy will be denied access to the Network. Exceptions must be approved prior to purchase (see Section 8).

5. Minimum Security Standards for Server Rooms

All Servers must exist in a commissioned server room. All server rooms must adhere to the Boise State University Minimum Security Standards for Server Rooms. This standard defines the criteria needed for all Servers and additional criteria for systems that contain Level 1 Data.

6. Best Practices

The University Technology Advisory Group will review and adopt appropriate standards and procedures that represent Best Practices with regard to the acquisition, implementation, management, and replacement of IT resources.

7. Responsibilities

a. The OIT Executive Director of Cloud Service and Infrastructure is responsible for administering this policy, including its maintenance and compliance.

b. A subcommittee consisting of the OIT Systems Engineering Group will review this policy and the minimum standards periodically and make recommendations regarding additions, deletions, and/or modifications to the OIT Executive Director of Cloud Service and Infrastructure.

c. Others wishing to make recommendations may make them directly to the OIT Executive Director of Cloud Service and Infrastructure.

8. Exceptions to Policy

A request for exception, along with a plan for risk assessment and management, can be submitted for review by the OIT Executive Director of Cloud Service and Infrastructure by completing a self-service support request. Non-compliance with these standards may result in revocation of access, notification to the supervisor, and reporting to Internal Audit and Advisory Services and Institutional Compliance and Ethics.

9. Enforcement

a. Failure to comply with this policy may result in the suspension of access to network resources until policy standards have been met.

b. Should the university incur monetary fines or other incidental expenses from security breaches, the University may recoup these costs, as reasonable and appropriate, from the non-compliant department, school, or auxiliary organization.

10. Related Information

Data Classification Standards
https://www.boisestate.edu/oit/itgrc/it-standards/data-classification-standards/

Self-Service Support for Requesting an Exception
https://boisestateproduction.service-now.com/bsu_sp

Incident Handling and Reporting
https://www.boisestate.edu/oit/itgrc/it-plans-procedures/it-incident-response-procedure/

Minimum Security Standards for Systems
https://www.boisestate.edu/oit/itgrc/it-standards/minimum-security-standards-for-systems/

Minimum Security Standards for Server Rooms
https://www.boisestate.edu/oit/itgrc/it-standards/minimum-security-standards-for-server-rooms/

Revision History

June 2004; January 11, 2023