BOISE STATE UNIVERSITY

University Policy 8020

Server Administration

Effective Date

November 1997

Last Revision Date

June 2004

Responsible Party

Vice President and Chief Financial Officer, (208) 426-1200
Chief Information Officer, (208) 426-5775

Scope and Audience

This policy applies to all colleges, departments, and offices of Boise State University, including all computing devices located at Boise State University that offer services to other computing devices as defined by Section III. Examples of these devices include, but are not limited to, Novell servers, Microsoft servers, Macintosh servers, and Unix servers.

1. Policy Purpose

The purpose of this policy is to protect the data of Boise State University, provide a reliable network, and reduce the risk of data loss or loss of service due to absence or loss of personnel, disasters, etc.

2. Policy Statement

To support a reliable network, all users of Boise State University's Information Technology (IT) resources shall conform to the guidelines detailed in this policy.

3. Definitions

3.1 Servers

Servers are 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.

3.2 Best Practices

Best practices are those data management and network procedures generally recognized by the industry for assuring secure, reliable, scaleable and efficient data repositories and networks.

4. Responsibilities and Procedures

4.1 Servers

When a server is needed to provide services or hold data, then it is important enough to devote the resources to ensure the server will be available and reliable. This should be done through the use of redundant equipment, a consistent backup scheme, and a detailed plan for a timely recovery of the services provided to University users.

4.1.1 Requirements

4.1.1A Virus Protection

Server antivirus software is required for all servers connected to the University's backbone. It must be installed and running, and its virus definitions kept up-to-date.

4.1.1B Documentation

Server IP address(es), licenses, services provided, and contact information (primary and alternate) must be documented and readily available.

4.1.1C Secure System Configuration

Servers must be secured to the greatest extent possible, including the disabling of all unnecessary services, configuration of file sharing services to provide reasonable and appropriate security, and changing of all default passwords.

4.1.1D Patches

Security and operating system (OS) patches or hot fixes must be applied in a timely fashion that is appropriately balanced between the type of OS installed and severity of risk to the Boise State University Network.

4.1.1E Backups

Appropriate backups of the server's OS, applications, data, and configuration documentation must be maintained, with type and frequency of the backups dependent upon the criticality of service(s) hosted.

4.2 Best Practices

a. Managers of Boise State University IT resources shall seek and adopt whenever possible best practices with regards to the acquisition, implementation, management and replacement of IT resources.

b. The Network Administrators Group shall review and adopt appropriate standards and procedures that represent best practices.

4.3 Responsibility

4.3.1 Modification of Policy

a. The Executive Director of Information Technology is responsible for administering this policy including its maintenance and compliance.

b. A subcommittee of the Network Administrators Group (the Server Administration Policy Subcommittee) will review this policy periodically and make recommendations regarding additions, deletions, and/or modifications to the Executive Director of IT. Others wishing to make recommendations may make them directly to the Executive Director of IT.

4.3.2 Exceptions to Policy

a. Any college, department, or office that wishes an exception to this policy must present its written request to the Server Administration Policy Subcommittee.

b. The Server Administration Policy Subcommittee will review and forward requests for exception with the Subcommittee's recommendation to the Executive Director of IT. The Executive Director of IT will then either approve or deny the exception. The

Subcommittees' recommendation and the decision from the Executive Director of IT will be forwarded to the requesting party within thirty days.

c. Only the Executive Director of OIT may authorize an exception to this policy.

4.4 Procedures

Non-Compliance with this Policy

4.4.1 First Offense

Non-compliance with this policy will result in a warning notice being sent from the Server Administration Policy Subcommittee to the responsible System Administrator. The warning notice shall include a description of the violation referencing specific policy and recommending the necessary corrective action and acceptable time frame for such action. A copy of this notice will be maintained by the Subcommittee in the event another incident occurs.

4.4.2 Second Offense

A second offence of non-compliance with this policy will result in a warning notice of non-compliance from the Server Administration Policy Subcommittee to the responsible System Administrator with copies to the appropriate Dean or Director and the Executive Director of IT. The warning notice shall include a description of the violation referencing specific policy and recommending the necessary corrective action and acceptable time frame for such action.

4.4.3 Continued Offenses

A third violation of this policy will result in the termination of network services to the offending department or college. The Executive Director of IT will direct that services be terminated with notice to the appropriate Dean or Director with a copy to the IT Governance Council. Such services will not be reestablished until the Server Administration Policy Subcommittee notifies the Executive Director of IT that the violation has been resolved in accordance with established policy.

Revision History

June 2004