University Policy #8130

Remote Access

Effective Date

December 2013

Responsible Party

Information Security Services, (208) 426-5501

Scope and Audience

This policy applies to all Boise State employees, students, and third parties.

Additional Authority

University Policy 8000 (Information Resource Use)
University Policy 8060 (Information Privacy and Security)
Minimum Security Standards for Systems

1. Policy Purpose

To state the requirements for remote access to computing resources hosted at Boise State University using remote access technologies.

2. Policy Statement

Approved Boise State employees, students, and authorized third parties (entities) may use the benefits of the Boise State provided VPN technology. The VPN connection is made via a User Managed Service with appropriate university Log-In Credentials. This policy aims to minimize the potential exposure to Boise State from damages which may result from unauthorized use of Boise State resources. Damages include the loss of protected data, intellectual property, damage to public image, damage to critical Boise State internal systems.
3. Definitions

3.1 Authorized Third Party

Any individual, entity, or vendor providing services to the University that is not employed by the University.

3.2 Information Security Officer (ISO)

The individual responsible for protecting confidential information in the custody of the university; the security of the equipment and/or repository where this information is processed and/or maintained and the related privacy rights of university students, faculty and staff concerning this information.

3.3 Internet Service Provider (ISP)

A business or organization that offers user(s) access to the Internet and related services.

3.4 Log-in Credentials

University assigned username and private personal password.

3.5 Private Network Resource

A resource or service provided to on-campus clients but is not available to individuals accessing Boise State’s network from the Internet.

3.6 Remote Access

The ability to log-in to a network from a distant location.

3.7 Remote Access Connection

A secured private network connection built on top of a public network, such as the Internet.

3.8 User Managed Service

A service where the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

3.9 Virtual Private Network (VPN)

A secure connection to a private network through a public network.
4. Responsibilities and Procedures

4.1 Requirements

a. Authorized Boise State employees, students, and entities must use the Boise State provided VPN technology as outlined in the [VPN Standards](https://www.boisestate.edu/oit-itgrc/it-standards-category/boise-state-virtual-private-network-standard/).

b. Secure Remote Access must be strictly controlled. Control is enforced via Boise State’s VPN gateway.

c. No one should provide their Log-in Credentials to another person.

d. People and entities with Remote Access privileges must ensure their Boise State-owned/personal computer or device is not connected to another network while it is connected to the Boise State private network.

e. All systems connected to Boise State’s non-public networks via Remote Access must meet the requirements defined in the [Minimum Security Standards for Systems](https://www.boisestate.edu/oit-itgrc/it-standards-category/boise-state-university-minimum-security-standards-for-systems/).

f. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Boise State production network must obtain prior approval from the Information.

5. Related Information

VPN Standards

Minimum Security Standards for Systems