University Policy 8030

Desktop, Laptop, and Tablet PC Computing Standards

Effective Date

November 1997

Last Revision Date

January 2020

Responsible Party

Office of Information Technology, (208) 426-4357

Scope and Audience

This policy applies to all University colleges, departments, divisions, and units.

1. Policy Purpose

To provide reliable desktop, laptop, and tablet PC platforms to enhance the workflow, security, and productivity of the University community. These standards are set forth to provide consistency, support, access to, and the secure use of University systems.

2. Policy Statement

Desktop, laptop, and tablet PC computing standards apply to all colleges, departments, divisions, and units of Boise State University to promote the secure sharing of information throughout the institution. Standards promote device and data security and compatibility for thorough, consistent support from the Office of Information Technology and vendors.
3. Modification of Standards

3.1. Responsibility for Standards

Responsibility for these standards belongs to the Associate Vice President and Chief Information Officer. Standards will be periodically evaluated and reviewed. Hardware and software standards are updated regularly.

3.2 Updates of Supported Products

A list of supported products will be updated regularly and be made available to the University community at: https://www.boisestate.edu/oit/request-for-it-security-policy-standards-exception.

a. It is the responsibility of individual departments and users to stay current on products supported and recommended.

b. These standards apply to all acquisitions independent of acquisition method or funding source, e.g., grants, donations, rental or leases, etc.

3.3 Exception to Standards

a. Any college, department, division, or unit that wishes an exception to these standards must submit the exception request at: https://www.boisestate.edu/oit/request-for-it-security-policy-standards-exception. The exception request will, at a minimum, state the following:

- The requested exception
- Justification
- A signed statement of support from the appropriate dean or director.

b. The user must commit funding and other appropriate resources to providing hardware and software support for the exception. Only the Chief Information Security Officer can authorize an exception to these standards.
4. Standards

4.1 Full Support

Support from the product vendor including security and technology updates are still available, the product is fully compatible with campus administrative systems, OIT staff members are fully product knowledgeable, and documentation is available. For fully supported products users may expect problem resolution, user seminars may be offered, and product consultation may be arranged.

4.2 Partial Support

The product may or may not be supported by the vendor, the product may not be fully compatible with campus administrative systems or specific known compatibility issues exist, and product documentation and user training is not available. Under these circumstances, OIT staff will provide limited product support with no claims as to customer satisfaction.

4.3 Mail and Calendaring

Google G Suite for Education is the primary tool for campus email, calendaring, and collaboration for the campus community. It is fully supported by the Office of Information Technology.

4.4 Web Browsers

The current versions of the three most commonly used browsers throughout the browser life cycle. The campus administrative systems can dictate which browsers are covered by full support. Information about Browser versions can be found at: https://www.boisestate.edu/oit-hardware/computers/standards.

4.5 Desktop Computers Standards

The Operating System installed on the computer will be fully supported within the manufacturer’s support product life cycle or end of life statements. Anti-virus software is required for all desktop devices. Security vulnerabilities and campus administrative systems can dictate the rate at which new Operating System versions are introduced to campus. Desktop Configuration Management software is required an all University-owned desktop computers to facilitate University device inventory and patching requirements. All University-owned desktop computers must be joined to the Boise State network domain for security and compliance requirements. Reference support questions at: https://www.boisestate.edu/oit-hardware/computers/standards.
4.6 Laptops and Tablet PCs

Extra security precautions including data encryption is required on laptops and/or tablet PCs in case the device is lost or stolen. Anti-virus software is required for all laptop and tablet PC devices. Desktop Configuration Management software is required on all University-owned laptops and tablet PCs to facilitate University device inventory and patching requirements. All University-owned laptop and tablet PC computers must be joined to the Boise State network domain for security and compliance requirements. User may reference the laptop and tablet PC encryption security guidelines at: https://www.boisestate.edu/oit-itgrc/it-guideline-category/system-security-encryption-guideline.

4.7 Support

The Office of Information Technology will only support and patch current licensed and supported versions of software and operating systems. Software or operating systems no longer supported by the vendor must be upgraded to the most current supported version.

4.8 Device Disposal

Upon completion of a device's useful lifespan, all hard drives and electronic storage devices will be erased using either DOD (Department of Defense) zero fill standards, magnetron, or device destruction. Hardware will be disposed of in accordance with Boise State and State of Idaho policy and procedures.

4.9 Backups

a. Backups are an important part of computing and the following information is to remind users of that as they acquire new computing resources. Lost or corrupted data means the re-entering of data and/or the possibility of data that can never be recovered.

b. Responsibility for all data stored on local drives belongs to the assigned user of the computer. All files created or revised each day should be backed up if those files are stored on a local drive. Users should also ensure weekly backups of all files.

c. Mission-critical data must be stored on University network file servers or approved cloud storage vendors where backups are performed automatically.
5. Related Information

Desktop and Software Standards
https://www.boisestate.edu/oit-hardware/computers/standards

Request for IT Security Policy/Standards Exception
https://www.boisestate.edu/oit/request-for-it-security-policy-standards-exception

System Security Encryption Guideline
https://www.boisestate.edu/oit-itgrc/it-guideline-category/system-security-encryption-guideline

Revision History

April 1998; March 2000; July 2001; December 2005; October 2006; January 2020