PRP 2510

Information Security Policy

> Recommended by the General Administrative Committee: February 23, 2016
> Endorsed by University Forum: April 20, 2016

1. Rationale for Policy

The Information Security Policy acknowledges the need to protect the confidentiality, integrity and availability of Bloomsburg University data and the systems that store, process or transmit it. This policy applies to all faculty, staff, vendors and other university affiliates who are authorized to access university data.

2. Keywords

information security, security, security policy, institutional data.

3. Background Information

All Bloomsburg University data, and the systems that store and transmit the data, must be protected from unauthorized access and use. All Bloomsburg University personnel and others who have authorization to access university data must be aware of their obligation to protect university data. This is particularly relevant since cloud storage services allow university personnel to place university data on non-university systems. Therefore, it is necessary to have in place appropriate local policies and procedures, as well as formal contracts with cloud storage vendors, which ensure the protection of all university data. Only cloud storage vendors who have current contracts with Bloomsburg University can be utilized to store university data. The University's Office of Technology maintains a list of vendors with whom the university has formal cloud storage contracts.

4. Policy

Throughout its lifecycle, all university data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology and maintained by the information security officer, given the level of sensitivity, value and criticality that the university data has to the University. The documentation can be found in the Information Security Guidelines in Support of Information Security Policy.

Any university information system that stores, processes or transmits university data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology and maintained by the information security officer, given the level of sensitivity, value and criticality that the university data has to the University. The documentation can be found in the Information Security Guidelines in Support of Information Security Policy.

Individuals who are authorized to access university data shall adhere to the appropriate roles and responsibilities, as defined in documentation approved by the University's Office of Technology and maintained by the Information security officer. The documentation can be found in the Information Security Guidelines in Support of Information Security Policy.

Maintenance
This Policy will be reviewed by the University's Office of Technology as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement
Violations of this policy may result in suspension or loss of the violator's use privileges, with respect to university data and university owned information systems. Additional administrative sanctions may apply up to and including termination of employment (for personnel) or cancellation of contracted services (for vendors). Criminal or civil prosecution under local, state or federal laws may also apply.

Exceptions
Exceptions to this Policy must be approved by the Office of Technology, in consultation with the Executive Staff, and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Definitions
University data is defined as any data that is owned or licensed by the university.

Vendor is defined as any third party that has been contracted by the university to provide a set of services and who stores, processes or transmits university data as part of those services.

Revision #5
Created 2 November 2023 13:20:44 by Douglas Hoffman
Updated 2 November 2023 13:49:31 by Douglas Hoffman