Policies

University policies related to technology.

- PRP 2510
- PRP 2550
- PRP 3408
- PRP 3410
- PRP 5365
- PRP 5366

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.

PRP 2550

Acceptable Use of Technology Policy

> Issued by: Dr. Richard H. Rugen, Vice President for Administration and Finance
> Effective date: April 21, 2010

Purpose

This policy addresses the use of university issued/owned information technology resources.

Bloomsburg University provides numerous information technology resources for use by the university's students, faculty and staff. The term Information technology resources includes, but is not limited to, all university computing equipment, personal data assistants, cellular phones, storage devices and any electronic device issued by the university and intended for business purposes, as well as software, systems and networks. These resources are provided to support the university's mission and institutional goals. The use of these systems is a privilege and all users are expected to act responsibly and to follow the university's policies and any applicable local, state and federal laws (e.g. copyright, criminal use of communication device, harassment, etc.) related to the use of these resources.

Scope

This policy applies to all users including faculty, staff, students, contractors and guest users of the Bloomsburg University computer network resources, equipment, or connecting resources. Use of the university's information technology resources signifies agreement to comply with this policy.

While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology, except as required by state or federal law. For example, the university may be required to provide information stored in its information technology resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the University may also be viewed by technical staff working to resolve technical issues.

This policy is subject to the terms and conditions of the various collective bargaining agreements that apply to faculty and staff.

Policy

A. Acceptable Use of Information Technology Resources

Responsibilities of User of University Information Technology Resources:

1. Respect the intellectual property rights of authors, contributors and publishers in all media;
2. Protect user identification, password, information and system from unauthorized use;
3. Report lost or stolen devices, including devices that contain private or university information to IT within 24 hours of discovery of the loss;
4. Adhere to the terms of software licenses and other contracts. Persons loading software on any University computer must adhere to all licensing requirements for the software. Except where allowed by the university site licenses, copying software licensed for university use for personal use is a violation of this policy;
5. Adherence to all other applicable university policies and/or terms of any collective bargaining agreement;
6. To use the university information technology resources in a manner that complies with State and Federal law.

B. Prohibited Uses of University Information Technology Resources

1. Providing false or misleading information to obtain a university computing account, or hiding or disguising one's identity to avoid responsibility for behavior in the use of information technologies;
2. Unauthorized use of another user's account;
3. Attempting to gain or gaining unauthorized access to university information technology resources, or to the files of another;
4. Performing any act(s) that impede the normal operation of or interfere with the proper functioning of university information technology resources;
5. Interfering with the security mechanisms or integrity of the university's information technology resources;
6. Use of the university information technology resources to transmit abusive, threatening, or harassing material, chain letters, spam, or other communications prohibited by state or federal law;
7. Copyright infringement, including illegal file sharing of video, audio, software of data;
8. Excessive use that overburdens the information technology resources to the exclusion of other users;
9. Excessive or prohibited personal use by employees;
10. Use of the university information technology resources for personal profit, commercial reasons, non-university fundraising, political campaigns or any illegal purpose;
11. The prohibition against using university information technology resources for personal profit does not apply to:
    1. Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members; or
    2. Other activities that relate to the faculty member's professional development.
    3. Other activities as approved by the University President

12. Non-authorized solicitations on behalf of individuals, groups, or organizations are prohibited;
13. Intentionally or knowingly installing, executing, providing to another, a program or file, on any of the university's information technology resources that could result in the damage to any file, system, or network. This includes, but is not limited to computer viruses, Trojan horses, worms, spyware or other malicious program(s) or file(s).

Enforcement

A university employee or student who violates this policy risks a range of sanctions imposed by relevant university disciplinary processes, ranging from denial of access to any or all information technology resources up to and including termination (for an employee) or dismissal (for a student). He or she also risks referral for prosecution under applicable local, state or federal laws.

PRP 3408

Student Use of University Assigned Email Accounts

> Issued by: James Mackin, Ph.D., Provost and vice President for Academic Affairs
> Effective date: Fall 2006
> Notes: Approved by BUCC 02/22/06. Reported to the University Forum 03/01/06.

The University assigned student email account shall be the primary means of official communication with all students at Bloomsburg University. Students are responsible for all messages and attachments sent to them via their university assigned email account or posted to course websites and/or course management systems such as Blackboard. Students will not be able to forward their university assigned account to an alternate email account. This policy does not preclude departments or offices from using traditional, non-electronic modes of communication at their discretion.

PRP 3410

Student and Pennsylvania Resident Printer Paper Use Policy

> Issued by: Dr. James E. Mackin, Provost and Vice President for Academic Affairs
> Effective date: Fall 2006
> Notes: Amended and approved by the Council of Trustees, February 1, 2006.

Each student at Bloomsburg University is given an allocation of 500 pages of printer paper each semester. A student can print as many pages as needed up to that limit at no charge, using any of the designated printers on campus. Any student who prints more than 500 pages of paper in a semester is billed at a rate of $.04 per page printed above the 500 page limit. This policy also applies to any Pennsylvania resident who uses the computers and printers on the Bloomsburg University campus.

PRP 5365

Cellular Phone Service and Other Wireless Communications Devices Stipend

> Issued by: Dr. Richard H. Rugen, Vice President for Administration and Finance
> Effective date: May 1, 2009
> Notes: Reviewed by FORUM March 25, 2009 and April 22, 2009.
> Approved by FORUM April 22, 2009

Preamble

The University seeks to achieve maximum productivity and cost-effectiveness when employing cell phone service and other wireless communications device technology as a business solution; to comply with IRS rules and regulations governing the taxability of these devices, and to effectively manage the reimbursement of costs associated with business use related to personally owned wireless devices and plans.

The Policy

This policy institutes a wireless communications stipend to cover presumed business use of personal cell phones for faculty, staff, and administrators who, as a part of the official University employment, have constant and recurring need for using a wireless communications device. The institutional stipend is intended to reimburse the employee for the business use of the device. The stipend is not intended to fund the cost of the device nor pay for the entire monthly bill. The assumption is that most employees also use their wireless communications devices for personal calls.

Employee Responsibilities

The employee will purchase cellular phone service and equipment and assume responsibility for vendor terms and conditions. The employee is responsible for plan choices, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. The employee is also responsible for the purchase, loss, damage, insurance, and/or replacement of phone equipment.

Definitions

Wireless Communication Device

A device that transmits and receives voice, data, and/or text without being physically connected to University network. This definition includes but is not limited to such devices as cellular telephones, pagers, wireless internet services, wireless data devices and cellular telephone/two-way devices. This policy does not include radio devices that interface with a defined non-public radio frequency such as the 800 MHz Statewide Radio System.

Wireless Communications Stipend

The wireless communications stipend does not constitute an increase in base pay, nor will it be included in the calculation of percentage increases to base pay. The stipend will be itemized and reported on employee pay statements and W-2s and subject to withholding taxes.

Policy will be implemented based upon most current wireless communications and other wireless communications devices stipend procedures.

PRP 5366

University Provided Cellular Phone Equipment/Service and Other Wireless Communications Devices Usage

> Issued by: Dr. Richard H. Rugen, Vice President for Administration and Finance
> Effective Date: May 1, 2009
> Notes: Reviewed by FORUM March 25, 2009 and April 22, 2009.
> Approved by FORUM April 22, 2009

Preamble

The University seeks to achieve maximum productivity and cost-effectiveness when employing cell phone service and other wireless communications device technology as a business solution; to comply with IRS rules and regulations governing the taxability of these devices, and to effectively manage the business use of such devices.

The Policy

There are some circumstances where a “departmentally assigned cellular phone or other wireless communications device” is deemed appropriate. In these instances, the University will provide the wireless communication device equipment and service. Personal use of such equipment and service is prohibited. This policy applies to all faculty, staff, and administrators who, as part of their official University employment, are assigned a university owned wireless communication device for use during their assigned work schedule only.

Responsibilities

Employee

The employee must maintain a record of the business purpose of each business related call/activity, specifically the amount of the expense, date and time of each call/activity, and business purpose.

Supervisor

The supervisor, as part of their review process, shall randomly audit the employee’s call logs to confirm that personal calls/activities were not made.

Definitions

Wireless Communication Device

A device that transmits and receives voice, data, and/or text without being physically connected to University network. This definition includes but is not limited to such devices as cellular telephones, pagers, wireless internet services, wireless data devices and cellular telephone/two-way devices. This policy does not include radio devices that interface with a defined non-public radio frequency such as the 800 MHz Statewide Radio System.

Policy will be implemented based upon most current wireless communications and other wireless communications devices stipend procedures.