

# Bloomsburg University

## Information Security Policy

Author: \_\_\_\_\_

Department: \_\_\_\_\_

### Amendment/Edit History

Author	Date	Amendment / Edits


## Contents

Objective: .....	3
Scope of Policy: .....	3
Risks Addressed: .....	3
Policy Statement: .....	3
Security Policies and Procedures: .....	4
Establishing, Updating and Terminating User Access: .....	4
System and Application Access: .....	5
Physical Access: .....	5
Access Audits: .....	5
Authenticating a User: .....	6
Access Methods: .....	7
Storage of Data: .....	8
Handling and Distribution of Data: .....	8
Protection of Data: .....	11
Disposal of Data: .....	11
Standards - Secure Media Disposal .....	11
System / Application Logging Requirements: .....	12
Security Fault Log .....	12
Operating Standards: .....	13

## Objective:

**Bloomsburg University** information is extremely valuable and must be treated as an asset that must be protected from prohibited disclosure, revision, use, or destruction. Prudent and practical steps must be taken to ensure that data integrity, confidentiality of information, and application/data availability are not compromised. Security tools and processes must be implemented and configured to enable adequate and proper restriction of access to programs, data, and other information resources. Physical access measures must also be incorporated are implemented to ensure that only authorized individuals have the ability to access or use information resources. Access, both physical and logical, should and will be audited quarterly by qualified personnel.

## Scope of Policy:

Information Security may apply to any activity that involves the access to, use , or modification of **Bloomsburg University** information and/or resources. Information Security affects and encompasses **Bloomsburg University** total information and physical environments. The scope or impact is any access, logical or physical, that has the potential to affect **Bloomsburg University** in a negative way. Areas that must be managed include, but are not limited to:

Physical security	Logical security
Network security and monitoring	Application security (including application purchase, implementation and development)
Segregation of duties	Establishing, editing, and terminating user access
Backup and recovery	Business continuity
Incident Response	Third party security
Security education and awareness	Data storage
Handling and distribution of data	Confidential information
Password policies	Security monitoring
Access to student and cardholder data	Threat reporting and response
<b>More +</b>	

## Risks Addressed:

The prohibited or unauthorized use, modification, and/or destruction of **Bloomsburg University's** information and/or resources.

## Policy Statement:

Rights to use to **Bloomsburg University's** information systems and computing resources will be based on each user's access privileges. Access privileges will be granted on the basis of specific business need (i.e. a "need to know" basis). Access controls must ensure that even legitimate users cannot access

information unless they are authorized to do so. All **Bloomsburg University** resources, systems and applications will have access controls unless specifically designated as a public access resource.

**Bloomsburg University's** employees, temps, contractors, consultants, and other workers including all personnel affiliated with third parties, are responsible for participating in maintaining secure access to **Bloomsburg University** information systems and computing resources. **Bloomsburg University's** management must provide guidance in creating this secure access environment by establishing access management policies, approving roles and responsibilities, and providing consistent coordination of security efforts across **Bloomsburg University**. The Security Policies and Procedures listed below are approved by management and act to govern the information environment at **Bloomsburg University**.

### Policy Update and Notification

**Bloomsburg University** reserves the right to revise the conditions of this policy at any time. Adequate notification of updates will be provided to all employees. Employees are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this policy.

## Security Policies and Procedures:

### Establishing, Updating and Terminating User Access:

#### Establishing Access

Newly hired **Bloomsburg University** employees must have a notification issued by **Bloomsburg University**. The notification of a newly hired employee, temp, contractor or other will go to the individuals or departments responsible for establishing the application and systems access required for the new employee to perform his or her job requirements. The notification will only be issued by appropriate personnel. **Bloomsburg University** Helpdesk Support, Applications, Network Services and Human Resources will all receive the notification. Notifications will be retained for a minimum of 24 months for audit and tracking purposes and should be available upon request.

#### Employee Position Change

A form issuance or electronic notification is required when an employee changes positions within the organization at **Bloomsburg University**. All employee position change notifications should include the following to allow application and systems owners to updated logical and physical access accordingly.

- Title change
- Department Transfer
- Physical Location Change
- Access Establishment Requirements
- Access Termination Requirements

Employee change notifications will only be initiated by the department's management or Human Resources personnel. Access should be updated accordingly and notification issuance retained permanently.

## Terminating Access

When an employee is terminated voluntarily or involuntarily and exits **Bloomsburg University** a notification will be sent to all applicable parties. The termination notification is issued immediately upon termination (when the employee no longer requires logical or physical resources). The notification will only be issued by appropriate personnel. **Bloomsburg University** Helpdesk Support, Applications, Network Services and Human Resources will all receive the notification. Upon receipt of a termination notification, all domain and application/systems access is immediately disabled. All logical accounts on the corporate domain and billing/accounting/finance applications and systems are audited quarterly. Disabled accounts greater than 30 days old are permanently deleted.

## **System and Application Access:**

### Network Server Access

Access to the system servers can only occur after the senior management approves access rights and a username and password to the appropriate employee. All access to corporate servers determined to be “in-scope” for audit and/or compliance requirements will be audited semiannually for accuracy and validity.

### Enterprise Business Applications Access

Access to enterprise business applications (ERP and/or CRM) is controlled for the production environment at **Bloomsburg University**. All requests for access require a written or electronic form with appropriate management approval. Access requires a profile including a valid username and password. Group permissions are reflective of job requirements and are audited semiannually for accuracy and validity.

*Important: Access is restricted to the production environment. Promotion of code from the test to production environment is performed utilizing proper separation of duties (SoD).*

## **Physical Access:**

### Employee Access

Physical access will only be granted to areas required for an employee to perform their job as per or management’s specifications. Physical access will be granted via the issuance of an employee badge that must be worn and visible at all times. The badge must be returned upon termination of employment.

### Ad Hoc Access (Contract and Temporary Labor)

Contract and temporary labor will only gain physical access as required by their job responsibilities by the issuance of a contract employee badge that must be worn and visible at all times. The badge must be returned upon completion of contract or temporary employment period.

### Visitor Access

All visitors to secured areas are required to sign in and be greeted by or escorted to their party.

## **Access Audits:**

Employee access to **Bloomsburg University** systems is audited on a semiannual basis. **Bloomsburg University** audits employee access levels to all corporate systems. Semiannual audit results are

submitted for review to the manager/system owner for each in-scope system and application. Semiannual audit results are to be stored for a minimum of 18 months.

Physical access rights are reviewed semi-annually by the Manager of ID Card Services.

*Note: "In-Scope" systems and application are those determined to be vital to business operations and usually encompass billing, accounting, finance, production etc.*

## **Enforcement**

Users are responsible for all personal account usernames, passwords, tokens, and related personal identification numbers (PIN). **Bloomsburg University** users are not to share personal account information with any other individual for any reason. Sharing of account usernames, passwords, tokens, and/or PIN pertaining to any **Bloomsburg University** systems or applications is strictly forbidden and punishable by disciplinary action.

## **Authenticating a User:**

### **Unique Application and Systems Users**

All unique usernames assigned to users in order to access **Bloomsburg University's** information systems and/or computer resources will be unique to that information system or computer resource and unique to each user.

### **Restricted Access Devices**

All **Bloomsburg University** information system and/or computer resource usernames will have an associated password or a stronger mechanism (such as a token or password generator) to ensure that only the authorized user is able to access and utilize applications and/or systems.

Generic passwords or PINs will never be used at **Bloomsburg University**. After a user's initial login, the user is required to change the password or PIN linked to the user's account for that information system or computer resource.

### **Password Policy Settings**

All **Bloomsburg University** users must change their application and/or systems passwords according to the following criteria:

- Password change every 90 days
- At least 8 characters long
- Cannot be one of the last three previous passwords
- Cannot contain the users account ID or full name
- Must be comprised of at least three of the following four character groups:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Numerals (0 through 9)
  - Non-alphabetic characters (such as: !, \$, #, %)

Users should immediately change their password if they suspect that it has been discovered or used by another. Further, users must notify the appropriate security administrator if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

#### Invalid Login

In order control user logons and maintain the effectiveness of access and authentication, user policies for all users on the **Bloomsburg University** domain are set to lockout the user after exceeding invalid attempts. If a user attempts to logon to a **Bloomsburg University** domain incorrectly more than 5 times, the account will lock for no less than 10 minutes. All lockout counters reset after no less than 5 minutes once a successfully login is achieved within no more than five attempts.

#### Inactive Workstations

Inactive workstations are automatically locked after 20 minutes. Users are required to verify their identity as the last user of that workstation in order to unlock an inactive workstation.

### **Access Methods:**

#### LAN (Local Area Network)

Users accessing the **Bloomsburg University** LAN must have a unique and valid username and password. The username and password combination must adhere to the username and password policy settings noted above.

#### Remote Access

Remote access to **Bloomsburg University** resources must be approved by management prior to establishing remote accounts. Remote access must incorporate advanced technologies to leverage adequate security standards, such as; VPN tunnel, logmein.com, gotomypc.com etc.

#### Mobile Computing

Only **Bloomsburg University** approved portable computing devices may be used to access **Bloomsburg University** information resources. To access the Internet, the mobile device must be compliant with the IEEE 802.11b or IEEE 802.11g protocol. Mobile computing devices at **Bloomsburg University** must adhere to the following:

- Portable computing devices must be password protected in accordance with the **Bloomsburg University** Password Policy.
- Confidential data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all confidential **Bloomsburg University** data must be encrypted using approved encryption techniques wherever possible.
- Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized as detailed above
- All remote access connections made to the **Bloomsburg University** environment must be made through the approved remote access tools provided by and **Bloomsburg University**

- Non **Bloomsburg University** computer systems that require network connectivity must conform to **Bloomsburg University** IT standards and must be approved in writing by **Bloomsburg University** IT management

### Storage of Data:

Business Units will establish procedures for the secure storage of all electronically stored **Bloomsburg University** information that is owned or controlled by such Business Unit.

**Bloomsburg University** users are strictly prohibited from downloading any **Bloomsburg University** data or **Bloomsburg University** student information onto laptops, disk, flashdrives, or other removable media.

*Note: Organizations responsible for PCI DSS 1.2, PCI PED and or PCI PABP compliance should ensure the following regarding retention of customer payment information:*

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

*\* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.*

*\*\* Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

These security requirements apply to all "system components." System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

### Handling and Distribution of Data:

Individual departments and management must establish procedures for the handling all data and information stored **Bloomsburg University**.

All **Bloomsburg University** data and information must be categorized into two main classifications:

- **Bloomsburg University** Public
- **Bloomsburg University** Confidential

**Bloomsburg University** “Public” information is information that has been declared public knowledge by management and can freely be given to anyone without any possible consequential damage to **Bloomsburg University**.

**Bloomsburg University** “Confidential” information contains all other data and information that is not “Public”. Much of **Bloomsburg University’s** information must be protected very closely, such as customer payment data, trade secrets and any other proprietary information vital to the success of **Bloomsburg University**. Sharing of “confidential” data or information with a third party should be under a fully executed non-disclosure agreement and/or other contracts requirements.

*Note: **Bloomsburg University** customer data relating to customer payment information will not be shared with third parties that are not currently PCI compliant and can attest and prove their current compliance status.*

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels.

**Minimal Sensitivity:** General corporate information; some personnel and technical information

<b>Access</b>	<b>Bloomsburg University</b> employees, contractors, people with a business need to know.
<b>Distribution within Bloomsburg University</b>	Standard interoffice mail, approved electronic mail and electronic file transmission methods.
<b>Distribution outside of Bloomsburg University internal mail</b>	U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
<b>Electronic distribution</b>	No restrictions except that it is sent to only approved recipients.
<b>Storage</b>	Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
<b>Disposal/Destruction</b>	Deposit outdated paper information in specially marked disposal bins on <b>Bloomsburg University</b> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
<b>Penalty for deliberate or inadvertent disclosure</b>	Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

**More Sensitive:** Business, financial, technical, and most personnel information

<b>Access</b>	<b>Bloomsburg University</b> employees and non-employees with signed non-disclosure agreements who have a business need to know.
<b>Distribution within Bloomsburg University</b>	Standard interoffice mail, approved electronic mail and electronic file transmission methods.
<b>Distribution outside of Bloomsburg University internal mail</b>	Sent via U.S. mail or approved private carriers.
<b>Electronic distribution</b>	No restrictions to approved recipients within <b>Bloomsburg University</b> , but should be encrypted or sent via a private link to approved recipients outside of <b>Bloomsburg University</b> premises.
<b>Storage</b>	Individual access controls are highly recommended for electronic information.
<b>Disposal/Destruction</b>	In specially marked disposal bins on <b>Bloomsburg University</b> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
<b>Penalty for deliberate or inadvertent disclosure</b>	Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

**Most Sensitive:** Trade secrets & marketing, operational, personnel, customer payment information, financial, source code, & technical information integral to the success of our company

<b>Access</b>	Only those individuals ( <b>Bloomsburg University</b> employees and non-employees) designated with approved access and signed non-disclosure agreements.
<b>Distribution within Bloomsburg University</b>	Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
<b>Distribution outside of Bloomsburg University internal mail</b>	Delivered direct; signature required; approved private carriers.
<b>Electronic distribution</b>	No restrictions to approved recipients within <b>Bloomsburg University</b> , but it is highly recommended that all information be strongly encrypted.
<b>Storage</b>	Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
<b>Disposal/Destruction</b>	Strongly Encouraged: In specially marked disposal bins on <b>Bloomsburg University</b> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
<b>Penalty for deliberate or</b>	Up to and including termination, possible civil and/or

inadvertent disclosure

criminal prosecution to the full extent of the law.

## Protection of Data:

### Backups

Backups of all essential **Bloomsburg University** electronically stored business data will be routinely created and properly stored to ensure prompt restoration.

### Environmental

Adequate environmental controls will be in place and monitored to prevent data loss due to preventable and/or treatable environmental threats.

## Disposal of Data:

### Removable Media

When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable State, Federal, or Business Unit requirements.

### Storage Devices

Prior to disposal or re-use, equipment containing storage media should be cleansed to prevent unauthorized exposure of data. Cleansing procedures should be used that will render all information unrecoverable. An “erase” feature (i.e. putting a document in the desktop recycle bin) is not sufficient.

### Printed Material

When no longer required, all sensitive printed material shall be disposed of by a internal machine or third party service that will cross-shred and dispose of all material in the bins on-site at an agreed upon frequency.

### Destruction of Media

Prior to disposal, destroy defective or damaged media (floppy disks, CDs, tapes) containing sensitive information to render the information unrecoverable. Shred all hardcopy materials that contain sensitive information.

## Standards - Secure Media Disposal

Dispose of worn, damaged, or otherwise no longer required media in a secure manner. To prevent the compromise of sensitive information through careless or inadequate disposal of computer media, consider the following controls:

- Media that may require secure disposal include: paper documents, recordings, output reports, magnetic tapes, removable disks or cassettes, optical storage media, program listings, test data, and system documentation.
- Dispose of media containing sensitive information by secure incineration or shredding.
- If planning to reuse magnetic or optical media, completely empty it of data through use of special software designed to securely erase and/or reformat the media. If software is unavailable, reformatting the media a minimum of three times is required.
- Maintain a log of the disposal of all sensitive items so as to provide an audit trail.

- Consider the extra risks associated with accumulating a large volume of media prior to disposal. In large quantities, it may be more difficult to detect missing items.
- Use access restrictions to identify unauthorized personnel.
- Maintain formal records of the recipients of data.
- Store media in accordance with manufacturer's specifications.
- Restrict distribution of information
- Indicate the authorized recipient of all copies of data.
- Review distribution lists and verify authorized recipients at regular intervals.

### **System / Application Logging Requirements:**

Maintain and appropriately store operator logs. These logs are subject to regular, independent reviews and should include:

- System Logs
- Security Logs
- Security Alerts (from security appliances)
- Application Logs
- Network equipment Logs (including firewalls and wireless equipment)
- System errors and corrective actions taken (especially automated error recovery)
- Communication session statistics
- Successful and unsuccessful logins

### **Security Fault Log**

A log of all security faults involving **Bloomsburg University** information systems and services is maintained.

### **Standards - Logon Monitoring**

A user event logging system will contain at a minimum the following information:

- User ID
- Dates and times of logon and logoff.
- Logon method, location, terminal identity (if possible), Network address
- Records of successful and unsuccessful system access attempts
- Records of successful and rejected data access and other resource access attempts.

### **Log Archiving**

The length of retention should reflect the availability of resources and the need to track historical information. The retention of logs should also reflect the possibility of providing evidence in future investigations. The storage and access to the logs should be sufficient to meet the requirements of evidence collection.

---

## Operating Standards:

1. An annual risk assessment must be performed by qualified personnel to properly identify security risks, threats and vulnerabilities.
2. This Information Security Policy must be reviewed at least annually and updated as needed to reflect changes in the operating environment at **Bloomsburg University**.
3. **Bloomsburg University** should create a tracking list of all devices, systems and applications used in processing, transmitting and /or storing sensitive **Bloomsburg University** data including customer payment information
4. All systems and applications at **Bloomsburg University** should disconnect or deactivate after a period of inactivity.
5. All **Bloomsburg University** resources are for employees and approved third parties only. There must be a legitimate business case for using and accessing **Bloomsburg University** resources.
6. **Bloomsburg University** employees will *never* copy company confidential information and data to any storage media device.
7. A formal security awareness plan should be documented, available and disseminated to employees annually and upon new hire.
8. A qualified incident response team should be formally assigned and responsible for crisis management including reporting theft and/or data breaches to the proper authorities and third parties.
9. A formal incident response plan should be documented and executable in the event of a crisis.
10. Background checks will be performed prior to hire for all newly hired / potential candidates.
11. Business units should maintain a listing of third parties, including service providers.
12. Management and/or system owners must approve all newly created accounts within the systems and/or applications they own.
13. All newly hired employees should review and sign the [Security Awareness Training presentation](#). The signed [Security Awareness Training documentation](#) should be placed in the employee's personnel file.
14. Terminated employee's user accounts to all applications, systems, resources and physical access should be revoked, disabled and terminated immediately following exit.
15. **Bloomsburg University** information must be protected from unauthorized disclosure, modification, or destruction. Prudent information about security standards and practices must

be implemented to ensure that the integrity, confidentiality, and availability of **Bloomsburg University** information are not compromised.

16. All hardware and software operated by business units of **Bloomsburg University** should be documented in compliance with all applicable Corporate or Business Unit asset management standards.
17. All sensitive documents must be assigned a classification in order to determine the level of sensitivity in which they must be handled.
18. All data that has a classification assigned by the owner must be handled according to the level of sensitivity.
19. Business Units must conduct personnel screenings of prospective employees and contractors who will be granted access to **Bloomsburg University** information systems.
20. Each business unit shall ensure delivery of a security awareness program to its employees, and the completion of such training shall be documented.
21. Each business unit shall implement a security incident reporting process and train its employees on how to use the process.
22. Each business unit shall develop a procedure for users to report weaknesses and threats related to the security of information systems.
23. Business units shall adopt procedures and facility-hardening measures to prevent and detect unauthorized access or damage to facilities that contain information systems.
24. Restricted areas within facilities that house sensitive or critical information systems will at a minimum utilize physical access controls designed to permit access by authorized users only.
25. To maintain the availability, integrity and confidentiality of information, computer and communications equipment should be secured from physical and environmental threats.
26. Prior to re-use, equipment containing storage media should be cleansed to prevent unauthorized exposure of data.
27. Changes to all information processing facilities, systems, software, or procedures will be strictly controlled according to formal change management procedures.
28. Security incident management procedures should be established within each business unit to ensure quick, orderly, and effective responses to security incidents.

29. System capacity requirements should be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
30. System acceptance criteria for all new information systems and system upgrades must be defined, documented, and utilized to minimize risk of system failure, in addition, a clear back out method must be documented and available.
31. Security awareness, prevention, and detection controls should be utilized to protect information systems and services against malicious code.
32. Back-ups of all essential **Bloomsburg University** electronically stored business data will be routinely created and properly stored to ensure prompt restoration.
33. Systems will maintain appropriate log(s) of activities involving **Bloomsburg University** information systems and services.
34. A log of all security faults involving **Bloomsburg University** information systems and services should be maintained.
35. Business Units will establish controls to ensure the security of the information system networks that they operate.
36. When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable State, Federal or Business Unit record retention requirements.
37. Business Units will establish internal procedures for the secure handling and storage of all electronically stored **Bloomsburg University** information that is owned or controlled by such Business Unit.
38. Corporate system documentation for **Bloomsburg University** information systems will be protected from unauthorized access.
39. Electronic mail will be governed for acceptable use, and shall be open to inspection or review by management to comply with State and Federal regulations as well as any applicable business unit standards.
40. Access to **Bloomsburg University** information systems and computing resources will be based on each user's access privileges. Access privileges will be granted on the basis of specific business need (i.e. a "need to know" basis). Access Controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so.

41. The owner of the system environment or their designee will authorize user access to all systems.
42. Business Units will establish procedures to modify the functionality, connectivity, and services supported by information systems that restrict users' privileges based on requirements of their job function.
43. System utilities will be available to only those users who have a business case for accessing the specific utility.
44. All applications will have access controls unless specifically designated as a public access resource.
45. **Bloomsburg University** computing resources will be sufficiently monitored by appropriate business unit personnel to detect deviations from authorized use.
46. Where appropriate and necessary, procedures will be established to monitor the events and activities of each user accessing resources.
47. Adequate environmental controls will be in place and monitored to prevent data loss due to preventable and/or treatable environmental threats.
48. Formal meeting minutes will be documented and stored permanently for all team and department weekly, monthly, quarterly, and annual meetings.
49. Users are responsible for all personal account usernames, passwords, tokens, and related personal identification numbers (PIN). **Bloomsburg University** employees are not to share personal account information with any other individual for any reason. Sharing of account usernames, passwords, tokens, and / or PIN pertaining to any **Bloomsburg University** systems or applications is strictly forbidden and punishable by disciplinary action.
50. Procedures and policies exist at **Bloomsburg University** to control user logons and maintain the effectiveness of access and authentication. Proper personnel should set user policies for all users on a **Bloomsburg University** domain. If a user attempts to logon to a **Bloomsburg University** domain incorrectly more than 5 times, the account will lock for 10 minutes. All **Bloomsburg University** users must change their passwords every 90 days and the system remembers the last three passwords used. The new user password cannot be the same as any of the last three passwords. All **Bloomsburg University** user passwords must be:
  - The password must be at least 8 characters long
  - The password cannot be one of the last five previous passwords
  - The password cannot contain your account or full name
  - The password must be comprised of at least three of the following four character groups:
  - English uppercase characters (A through Z)

- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphabetic characters (such as: ! \$, #, %)

All lockout counters reset after a minimum of 5 minutes once a successful logon is achieved within five attempts. Inactive workstations are automatically locked after 20 minutes. A user cannot gain access to any **Bloomsburg University** domain unless they follow the New Hire, contract or management/system owner approval processes. Users are responsible for all personal account usernames, passwords, tokens, and related personal identification numbers (PIN). **Bloomsburg University** employees are not to share personal account information with any other individual for any reason. Sharing of account usernames, passwords, tokens, and / or PIN pertaining to any **Bloomsburg University** systems or applications is strictly forbidden and punishable by immediate termination.

---

I have read and been understand the content, requirements and expectations of the **Bloomsburg University's** Information Security Policy. I have received a copy of the policy and agree to operate within the policy guidelines during and as a condition of my employment at **Bloomsburg University**.

I understand that if I have questions regarding the **Bloomsburg University** Information Security Policy, It is my responsibility to consult with my immediate supervisor, Human Resources or management.

Your signature indicated that you have read and understand the **Bloomsburg University** Information Security Policy.

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Employee Printed Name: \_\_\_\_\_ Date: \_\_\_\_\_