



West Liberty University Data Security Plan

1. Objectives and Scope

- **Objective:** To safeguard sensitive students, staff, and institutional data and financial information, ensuring compliance with GLBA and NIST standards.
 - **Scope:** Covers all departments, information systems, data storage methods, and communication networks across the university.
-

2. Governance and Oversight

The West Liberty University President will annually appoint a **Privacy Officer** responsible for overseeing and implementing the information security program. The Privacy Officer is responsible for the development, implementation, and oversight of WLU's compliance with the policies and procedures required by the Gramm Leach Bliley Act (GLBA) Safeguards Rule. The Privacy Officer shall be granted the authority and resources necessary to enforce the program effectively.

3. Risk Assessment

In accordance with **16 CFR 314.4(b) of the GLBA Safeguards Rule and NIST SP 800-30**, West Liberty University conducts risk assessments to identify reasonably foreseeable internal and external threats to the security, confidentiality, and integrity of sensitive customer information. These assessments are designed to evaluate the adequacy of existing safeguards and inform appropriate updates or corrective actions. All risk assessments are formally documented in writing, retained for audit purposes, reviewed during annual assessments, and include:

- Identified risks, evaluation criteria, mitigation strategies, and acceptable decisions.
- Identify and classify sensitive data (e.g., financial, personal, academic).
- Evaluate internal and external threats to data confidentiality, integrity, and availability.
- Assess the effectiveness of current administrative, technical, and physical safeguards.
- Categorize risks using a defined risk matrix based on impact and likelihood.
- Recommend mitigation strategies or document risk acceptance decisions.
- Assign responsible parties and timelines for remediation.
- Be reviewed by the Privacy Officer and reported to executive leadership.

4. Security Policies and Standards

- **Data Access Control:** Access to secure and sensitive data through university information systems is limited to employees with a legitimate business need to access such data. Access to these systems is restricted through access controls such as role-based accounts, group policy, and network segmentation. Access to sensitive data is based on the principle of least privilege.
 - Access control is granted and removed based on the hire / termination date of employees. There will be no exceptions.
 - Authorized Vendors and Volunteers may be granted access based on university needs. All non-employee access requests must be made, in writing, and will be adjudicated by the IT Department.
 - Access will be reviewed and documented, at least annually, by the IT Department following the WLU Data Access Audit Procedure Guidelines.
- **Data Classification and Handling:** See University Policy #82, “Information Privacy”.
 - Classify data.
 - Define handling protocols for each classification.
- **Data Retention and Disposal:** See University Policy #90, “Record Retention Policy”
 - Implement secure data retention policies.
 - Paper records that are no longer required will be shredded. Shredded materials will be removed by a vendor with an AAA certification from the National Association for Information Destruction.
 - Computer equipment that is being retired will be returned to the IT Department for recycling and data destruction utilizing HIPAA and DoD compliant methods.
 - All disposal practices are conducted in accordance with applicable federal and state data retention laws and university policy to prevent unauthorized access to customer information.
- **Change Management:**
 - West Liberty University has established change management procedures to ensure that all modifications to information systems are appropriately documented.

5. Technical Safeguards

- West Liberty University will implement controls based on **NIST Cybersecurity Framework (CSF):**
 - The IT Department will maintain an inventory of hardware, software, and data assets to be reviewed and documented annually.
 - The IT Department will protect University assets utilizing:
 - Firewalls, intrusion detection/prevention systems.
 - Regularly updating and patching systems
 - Deploying endpoint protection and monitoring tools.

- The IT Department will monitor threat detection resources utilizing firewall and a Security Information and Event Management tool for real-time threat detection.
 - The IT Department will conduct, at least annually, backup testing.
 - The IT Department will conduct periodic vulnerability assessments and penetration testing.
 - **Identification:** Risk assessments are conducted across all relevant operational areas of the university.
 - **Encryption Standards:**
 - Encrypt sensitive data in transit and at rest using NIST-approved algorithms
 - Encrypt all university data storage devices (hard drives, flash drives, etc.)
 - **Multi-Factor Authentication (MFA):**
 - In accordance with **GLBA Safeguards Rule 16 CFR 314.4(c)(5)**, West Liberty University requires multi-factor authentication (MFA) for all systems and users accessing university information systems that support MFA and contain sensitive or customer information. MFA is mandatory for all systems and applications that store, transmit, or process such data.
 - Exceptions to MFA are permitted only when technically infeasible and must be documented and approved in writing by the University's Privacy Officer.
 - **Software Development:** Secure development practices are in place for in-house developed applications used to transmit, access, or store customer information.
-

6. Physical Security

- Physical Access to servers, network hardware, and sensitive documents will be restricted to authorized personnel. Data Center and data closets will be physically locked, and access controlled by locks and badge access where possible.
 - Surveillance equipment will be deployed where possible.
-

7. Safeguard Testing, Monitoring, and Auditing

West Liberty University implements information safeguards based on risks identified through its annual risk assessments. To ensure these safeguards remain effective, the university conducts regular testing and monitoring of key controls, systems, and procedures. Logs are reviewed regularly to detect unauthorized access, misuse, or tampering. Alerts from the SIEM system are triaged by IT personnel, and incidents are escalated according to the University Policy #81, "Data Breach Response". The IT Department will:

- Continuously monitor system activity for anomalies.
 - Perform annual compliance audits against GLBA and NIST standards.
 - Document audit findings and remediation efforts.
-

8. Employee Management, Training, and Awareness

- Background checks are performed on all employees before hire.
 - Cybersecurity training is provided upon hire.
 - Annually GLBA and cybersecurity training is required for all staff and employees.
-

9. Vendor Management

- West Liberty University performs due diligence when selecting third-party service providers that access or process customer information, ensuring they can maintain appropriate safeguards.
 - Third party vendors will have their information security safeguards reviewed prior to engaging their services.
 - Third party vendor contracts and performance are reviewed annually.
-

10. Evaluation and Improvement

- Conduct annual reviews of the data security plan.
 - Update the plan in response to regulatory changes, new threats, or university needs.
-

11. Incident Response

See University Policy #81, “Data Breach Response”

- Review University Policy #81, “Data Breach Response”, annually to ensure that it remains relevant.
 - Review for organizational changes
 - Revisions in law
 - Revisions in best practice.
 - Conduct, annually, tabletop training via the Privacy Officer and the IT Department to ensure readiness for a breach incident.
-

12. Breach Notification

In accordance with 16 CFR 314.4(j) of the GLBA Safeguards Rule, West Liberty University will notify the Federal Trade Commission (FTC) no later than 30 days after discovery of any unauthorized acquisition of unencrypted customer information involving 500 or more

individuals.

The notification will include:

- Name and contact information of the institution
- Description of the types of information involved
- Date or estimated date of the breach
- Number of consumers affected or potentially affected
- Summary of the breach and any remedial actions taken

The report will be submitted via the FTC's breach notification portal at <https://www.ftc.gov>.
