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

- Establish a **Data Security Governance Committee** and Data Stewards responsible for oversight, including representatives from IT, legal, and academics, and Presidents Cabinet per University Policy #82, "Information Privacy".
  - The Data Governance Committee shall meet at least annually to review the classification of confidential information and to ensure that the policy and data classifications remain relevant.
  - Classifications will be reviewed by the University General Counsel to ensure that committee recommendations abide by all relevant law.
- Appoint a **Privacy Officer or Chief Information Privacy Officer** (CISO) to oversee the security program.
  - The Privacy Officer serves to manage the policies and procedures of WLU to protect Personally Identifiable Information (PII) and other sensitive information.
    - The Privacy Officer or CISO shall:
      - Be appointed by the University President annually via a documented notice.
      - Be a member of the Data Governance Committee.
      - Be alerted at any time an information privacy matter, or a potential information privacy matter, occurs.
      - Comply with all HEPC and West Virginia reporting requirements for a privacy breech event, dictated by those bodies.

---

3. Risk Assessment

- Conduct an annual risk assessment in accordance with the **GLBA Safeguards Rule** and **NIST SP 800-30**.
    - Identify sensitive data (e.g., financial, personal, academic).
    - Assess threats and vulnerabilities to data confidentiality, integrity, and availability.
    - Prioritize risks based on impact and likelihood.
    - Remediate risks

---

4. Security Policies and Standards

Develop and maintain policies in the following areas:

- **Data Access Control**: Limit access to sensitive data 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 Chief Information Officer.
    - Access will be reviewed and documented, at least annually, by the IT Department following the WLU Data Access Audit Procedure.
- **Data Classification and Handling –** See University Policy #82, "Information Privacy".
    - Classify data.
    - Define handling protocols for each classification.
- **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.)
- **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 Critical Incident Response Team (CIRT) to ensure readiness for a breach incident.
- **Data Retention and Disposal**:
    - 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.

5. Technical Safeguards

- 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 update and patch systems.
        - Deploy endpoint protection and monitoring tools.
    - The IT Department will monitor threat detection resources utilizing firewall and a Managed Detection and Response (MDR) application.
    - The IT Department will implement a Security Information and Event Management tool for real-time threat detection.
    - The IT Department will train staff to follow the Data Breach Response Policy (University Policy # 81) during incidents.
    - The IT Department will conduct, at least annually, backup testing to ensure robust data backups including full server and system state recovery.
- Conduct periodic vulnerability assessments and penetration testing.

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.
- Surveillance equipment will be deployed where possible.

7. Training and Awareness

- Provide annual GLBA and cybersecurity training for all staff and faculty.
- Include role-specific training for IT and administrative staff.

8. Monitoring and Auditing

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

9. Vendor Management

- Vet third-party vendors for security practices.
  - Acquire cloud vendors SOC reports
  - Interview vendors annually to ensure compliance with NIST standards.
- Require vendors to sign agreements ensuring compliance with and NIST and GLBA where applicable.
- Annually review vendor contracts and performance.

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.