## Policy 418: Gramm-Leach-Bliley Act (GLBA) Compliance Policy

Category: Information Technology, Cyber Security, and Data Management

Covered Individuals: All CEI Employees and Students

Approved: 6/24/2025

Formerly Approved: 10/3/2024 (Provisional Approval by PAC)

### **418.1 Policy**

The College of Eastern Idaho (CEI) is committed to safeguarding the privacy and security of personal financial information as required by the Gramm-Leach-Bliley Act (GLBA). This policy outlines the steps CEI will take to comply with the GLBA's Safeguards Rule and Privacy Rule, ensuring that all nonpublic personal information (NPI) is protected from unauthorized access, theft, or misuse.

**418.2 Procedures**

**Compliance Overview**

CEI’s GLBA compliance policy follows the three primary components required under the Safeguards Rule:

1. **Risk Assessment**
2. **Information Security Plan**
3. **Third-Party Oversight**

**1. Risk Assessment**

CEI will regularly assess the risks to the security, confidentiality, and integrity of NPI, especially in regard to systems that store and transmit this information. This assessment will:

* Identify potential threats (e.g., cyber-attacks, data breaches, physical theft, etc.).
* Evaluate existing security controls.
* Determine vulnerabilities and the likelihood of compromise.

**Key Actions:**

* Annual review of systems and protocols.
* Periodic internal audits of data security practices.
* Implement corrective actions based on risk findings.

**2. Information Security Plan**

CEI will establish and maintain a comprehensive written information security plan **[see Appendix A]** that includes:

* **Administrative Safeguards:** Designating key personnel responsible for overseeing information security, including a dedicated Information Security Officer (ISO) and a GLBA compliance coordinator.
* **Physical Safeguards:** Securing physical access to sensitive records through locked cabinets, access control systems, and restricted access policies.
* **Technical Safeguards:** Using encryption, firewalls, intrusion detection systems, and two-factor authentication (2FA) to protect electronic records and transactions.
* **Monitoring and Testing:** Routine monitoring of access and activities on the institution’s network, combined with penetration testing and vulnerability assessments.

**Incident Response Plan:** In the event of a data breach or attempted compromise, CEI will activate its **Incident Response Plan [See Appendix B]**. This plan includes immediate reporting of incidents, investigation procedures, mitigation efforts, and notification of affected individuals in compliance with applicable laws.

**3. Third-Party Service Providers**

CEI will ensure that any third-party service provider that has access to NPI will also comply with the GLBA Safeguards Rule. This includes:

* Requiring third parties to implement and maintain appropriate security measures.
* Conducting due diligence and requiring signed contracts that stipulate their responsibilities in protecting NPI.
* Periodic review of third-party compliance and updating agreements as necessary.

**Privacy of Consumer Financial Information**

CEI complies with the Privacy Rule of GLBA by:

* Providing privacy notices to all individuals whose financial information is collected and explaining how this information is used and shared.
* Offering individuals the opportunity to opt-out of sharing their information with non-affiliated third parties, where applicable.
* Limiting access to sensitive financial data to only those employees who need it to perform their duties.

**Training and Awareness**

All CEI employees who handle or may come into contact with NPI will receive annual training on information security, privacy practices, and GLBA compliance. This training will include:

* Recognizing phishing and other common cyber threats.
* Proper handling and disposal of sensitive information.
* Reporting suspicious activity or data breaches immediately to the Information Security Officer (ISO).

**Continuous Improvement**

CEI is committed to continuously improving its security measures by:

* Staying updated on best practices in information security and evolving threats.
* Engaging with IT security consultants as needed.
* Regularly reviewing and updating the security policy to reflect changes in technology, regulations, and institutional practices.

 **Contact Information**

 For any questions regarding this policy, or to report a data breach or concern, please contact:

* **Information Security Officer**: [Kent Blacker, kent.blacker@cei.edu, 208 535-5464]
* **GLBA Compliance Coordinator**: [Stephen Brown, steve.brown@cei.edu, 208 535 5435]

**Appendix A**

Below is a comprehensive **Information Security Plan** (ISP) tailored for the College of Eastern Idaho (CEI). This plan aligns with regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA), and includes administrative, technical, and physical safeguards to protect sensitive information and ensure compliance with federal and state regulations.

**College of Eastern Idaho**

**Comprehensive Information Security Plan**

**1. Introduction**

The College of Eastern Idaho (CEI) is committed to protecting the security and confidentiality of sensitive and nonpublic information. This **Information Security Plan (ISP)** is established to safeguard against unauthorized access, disclosure, theft, or destruction of such information. The ISP applies to all systems, staff, contractors, and third-party service providers who access, process, or store CEI's sensitive data.

This plan addresses the following key elements:

* Risk identification and assessment
* Implementation of security controls
* Continuous monitoring and improvement
* Incident response and reporting procedures
* Employee and contractor training
* Third-party risk management

**2. Scope**

This plan covers all sensitive and nonpublic information (NPI) collected, stored, processed, or transmitted by CEI. This includes, but is not limited to:

* Financial information (student loan details, payment records, etc.)
* Personally Identifiable Information (PII) such as Social Security numbers
* Health information covered under HIPAA
* Intellectual property and proprietary data
* Sensitive academic and employee records

**3. Information Security Roles and Responsibilities**

**3.1 Information Security Officer (ISO):** The ISO is responsible for overseeing the implementation and enforcement of this Information Security Plan. The ISO will conduct risk assessments, monitor security measures, and coordinate responses to security incidents.

**3.2 GLBA Compliance Coordinator:** This role ensures CEI's compliance with the Gramm-Leach-Bliley Act, working in collaboration with the ISO to safeguard financial information.

**3.3 IT Department:** The IT department will manage the technical security measures outlined in this plan, including network security, user access control, and system monitoring.

**3.4 Data Stewards:** Each department handling sensitive information will designate a Data Steward responsible for ensuring that data is handled in compliance with CEI's policies.

**4. Risk Assessment and Management**

CEI will perform regular risk assessments to identify internal and external risks to the confidentiality, integrity, and availability of sensitive data. The risk management process includes:

**4.1 Identifying Risks:**

* Unauthorized access to data (physical or digital)
* Data breaches and theft (cyber-attacks, malware, etc.)
* Insider threats (employee misuse or error)
* Equipment failure or loss (hardware theft, system crashes)
* Natural disasters and physical destruction

**4.2 Evaluating the Impact of Risks:** CEI will evaluate the potential damage from the identified risks to determine where improvements are necessary.

**4.3 Implementing Risk Mitigation Strategies:** Appropriate administrative, technical, and physical safeguards will be implemented based on the risk assessment findings.

**5. Administrative Safeguards**

**5.1 Security Policies and Procedures:** CEI will maintain up-to-date security policies and procedures that address the use, storage, and transmission of sensitive data.

**5.2 Employee Training and Awareness:** All employees, contractors, and third-party providers who handle sensitive information must undergo mandatory security training. Training will cover:

* Recognizing phishing and social engineering attacks
* Proper data handling and disposal techniques
* Secure password practices and multi-factor authentication (MFA)
* Incident reporting procedures

**5.3 Access Control Policy:** Access to sensitive data will be limited to authorized personnel based on their role. The principle of least privilege will be applied to minimize unnecessary access.

**6. Technical Safeguards**

**6.1 Encryption:** All sensitive data transmitted electronically (email, cloud storage, etc.) will be encrypted using industry-standard encryption protocols. Data at rest will also be encrypted in storage systems where possible.

**6.2 Network Security:**

* **Firewall Protections:** Firewalls will be installed to prevent unauthorized access to CEI’s network.
* **Intrusion Detection/Prevention Systems (IDS/IPS):** CEI will utilize these systems to monitor network traffic and detect suspicious activities.
* **Secure Remote Access:** Virtual Private Network (VPN) solutions and MFA will be used for any off-campus access to CEI's network or sensitive systems.

**6.3 Endpoint Protection:** All institutional devices, including laptops, desktops, and mobile devices, will have up-to-date antivirus software and endpoint protection solutions installed.

**6.4 Data Backup and Recovery:** Regular backups of critical systems and data will be maintained, ensuring secure storage of backup files both onsite and offsite. Backup systems will be tested periodically to ensure they are functioning properly in case of a data loss event.

**6.5 Patching and Updates:** CEI will apply regular software patches and updates to ensure that systems remain secure from vulnerabilities.

**7. Physical Safeguards**

**7.1 Physical Access Control:** Physical access to rooms containing sensitive information (e.g., server rooms, file storage areas) will be restricted through the use of locked doors, access badges, and security cameras.

**7.2 Paper Document Protection:** Sensitive paper documents will be stored in secure, locked cabinets. Documents that are no longer needed will be shredded before disposal.

**7.3 Device Security:** Institutional devices, including servers, workstations, and mobile devices, will be physically secured to prevent theft or tampering. Devices must be password-protected and locked when not in use.

**8. Incident Response Plan**

CEI has developed an **Incident Response Plan (IRP)** to manage and mitigate the effects of data breaches or security incidents. This plan includes:

**8.1 Reporting Incidents:** Employees must report any suspected security incident or data breach immediately to the Information Security Officer (ISO).

**8.2 Response and Containment:** The ISO and IT department will assess the incident and take immediate action to contain the breach. This may include shutting down affected systems, disabling compromised accounts, and notifying affected individuals.

**8.3 Notification Requirements:** In the event of a confirmed data breach, CEI will notify affected individuals, regulatory authorities, and third-party service providers in compliance with state and federal laws.

**8.4 Post-Incident Review:** After an incident, CEI will conduct a full review to understand the cause and determine corrective actions to prevent future occurrences.

**9. Monitoring, Testing, and Improvement**

**9.1 Regular Monitoring:** CEI will continuously monitor its network for suspicious activity, vulnerabilities, and potential threats.

**9.2 Vulnerability Assessments and Penetration Testing:** Annual penetration tests will be performed by qualified third-party security vendors to identify weaknesses in CEI’s security systems.

**9.3 Internal Audits:** Regular internal audits will be conducted to review the effectiveness of the ISP, identify gaps, and ensure compliance with policies.

**9.4 Continuous Improvement:** The ISP will be reviewed and updated annually, or as needed, to incorporate new security threats, technologies, and regulatory requirements.

**10. Third-Party Risk Management**

**10.1 Vendor Due Diligence:** CEI will conduct due diligence before engaging any third-party vendor that handles sensitive data. This includes reviewing the vendor’s information security practices and ensuring that they comply with CEI’s data security standards.

**10.2 Third-Party Contracts:** Contracts with third-party vendors will include provisions that require them to implement security measures in compliance with the GLBA and this ISP.

**10.3 Ongoing Vendor Monitoring:** CEI will periodically assess the security practices of third-party vendors and require corrective actions if deficiencies are identified.

**11. Compliance with Laws and Regulations**

CEI will comply with all applicable federal, state, and local regulations, including:

* Gramm-Leach-Bliley Act (GLBA)
* Health Insurance Portability and Accountability Act (HIPAA)
* Family Educational Rights and Privacy Act (FERPA)
* Idaho data breach notification laws

**12. Conclusion**

This comprehensive Information Security Plan ensures that CEI is proactive in protecting sensitive and nonpublic information, managing risks, and responding effectively to security incidents. The success of this plan relies on the commitment of all employees, contractors, and third-party providers to follow established security policies and procedures.

The Information Security Plan will be reviewed and updated annually to reflect evolving threats, technologies, and regulatory changes.