LSSU GLBA Compliance

The GLBA (Gramm-Leach-Bliley Act of 2003) requires that the University develop, implement, and maintain a comprehensive information security program containing the administrative, technical, and physical safeguards that are appropriate based upon the University's size, complexity, and the nature of its activities. A person must be designated to coordinate, evaluate and monitor the effectiveness of the safeguards employed and be empowered to change them as needed to meet threats. The data covered is any non-public personal data about any consumers of the University's services. Examples of covered data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable information.

Lake Superior State University's designated responsible person is the University chief financial officer (CFO).

Lake Superior State University's compliance with GLBA for covered data is obtained through a combination of policies and proceedures:

Technology policies: 3.3.1 (2) and procedures (GLBA Statement-see below),
Business Operations policy: Identity Theft (Red Flag) 3.7.16 (1)
FERPA (Family Educational Rights and Privacy Act) (lssu.ed/registrar/ferpa).

GLBA is the responsibility of all individuals or departments that have access to covered data including but not limited to:

- o Enrollment Management (Recruiting, Admissions, Applications Processing, Registrar, Financial Aid)
- o Finance, Business Office, Cashiering (and alternative collection points), Accounting, Accounts
  Payable, Collections, Vendor Management, Customer Management, Grants Management
- o Human Resources
- o Institutional Advancement
- o Continuing Education and Similar Programs and Offices
- o Student Affairs
- o Academic Affairs
- o Performing Arts Centers
- o Information Technology
- o Athletics

All areas of the University follow rigorous records disposal practices. Records containing sensitive or personal data are shredded; either in house or by commercial services utilizing locked bin/at-pick-up-shredding.

IT GLBA statement:
Lake Superior State University employs a layered system of technical and procedural controls throughout our operating processes relating to personal and financial records.

From an Administrative perspective, we have a designated IT security coordinator and other members of the IT security team that meet on a weekly basis to assess our security posture, as well as to identify potential internal and external threats to the security, confidentiality, and integrity of customer information and other sensitive data. Employees are subjected to a background check, and require training as part of their onboarding and approval process when their position requires access to sensitive personal or financial information.

Next, technical controls are implemented, including isolated networks for secure servers, encrypted VPN access control for the specific groups needing access to sensitive data, and physical controls for access to the datacenter servers. Data Center is located in secure area, access is restricted to IT personnel. Access for individuals outside of IT, will be chaperoned by and IT staff member. Vendors requiring data access are inventoried and regularly reviewed for compliance.

Preventative measures are also in place, including encrypted backups to secure isolated storage, redundant backups to secure cloud storage, EDR software on client endpoints, and a robust next-generation firewall with logging and reporting for suspicious activity.