LAKE SUPERIOR STATE UNIVERSITY PROCEDURES MANUAL
Administrative Policy

Section: Information Technology | Section Number: 3.3.5

Subject: Third-Party Partner Security Management | Date of Present Issue: 10/18/2024

Date of Previous Issues: None

Policy Statement:

Lake Superior State University (LSSU) recognizes the importance of maintaining the security and integrity of its information systems when working with third-party partners. This policy establishes the requirements for managing and securing interactions with third-party partners, ensuring that they adhere to LSSU's security standards and best practices to protect the university's data and resources.

Scope:

This policy applies to all LSSU departments, faculty, staff, and third-party partners who engage in activities involving the exchange, processing, or storage of LSSU data and access to LSSU's information systems.

Definitions:

- **Third-Party Partner:** Any external organization, vendor, contractor, or service provider that interacts with LSSU's information systems or handles LSSU's data.
- **Data Security Agreement (DSA):** A formal agreement between LSSU and a third-party partner outlining security responsibilities and expectations.(Cyber Insurance)
- **Risk Assessment:** A process to identify and evaluate risks associated with third-party interactions with LSSU's information systems.

Procedures:

1. **Third-Party Risk Assessment:**
   - Before engaging with a third-party partner, the requesting department must coordinate with IT to conduct a thorough risk assessment. This assessment will evaluate the potential security risks associated with the third-party's access to LSSU's data and systems.
   - The risk assessment will include an evaluation of the third-party's security controls, data protection measures, and compliance with relevant regulations and standards.
2. **Access Control:**
   - Third-party partners will be granted the minimum level of access necessary to perform their contracted services. Access to sensitive data and systems will be restricted based on the principle of least privilege. Systems support access will be controlled by the IT department.
3. **Security Controls and Compliance:**

- Third-party partners must implement and maintain security controls that meet or exceed LSSU's security standards. Third-party partners must comply with all applicable data protection regulations.

4. **Incident Response and Reporting:**
   - In the event of a security incident involving a third-party partner, the partner must notify LSSU IT immediately and cooperate fully in the investigation and remediation efforts.
   - Third-party partners must have an incident response plan in place and provide LSSU with timely updates on the incident's status and any actions taken to mitigate its impact.
5. **Termination of Access:**
   - Upon the termination of the partnership or completion of the contracted services, the third-party partner's access to LSSU systems and data must be promptly revoked. IT will ensure that all accounts, credentials, and access rights granted to the third party are disabled or removed.
   - Any LSSU data stored or processed by the third-party partner must be securely returned or destroyed, and a certificate of destruction must be provided to LSSU where applicable.
6. **Review and Audit:**
   - LSSU IT will conduct audits at least every 12 months of third-party partners to ensure ongoing compliance with the terms of the DSA and LSSU's security standards.
   - The performance and security practices of third-party partners will be reviewed periodically, and any identified deficiencies must be addressed by the partner within a specified timeframe.

Responsibilities:

- **LSSU IT:** Responsible for conducting risk assessments
- **Requesting Departments:** Responsible for initiating the third-party engagement process, ensuring the partner complies with their contract, and coordinating with IT for assessments and audits.
- **Third-Party Partners:** Responsible for adhering to the security requirements outlined in the contract and cooperating with LSSU in maintaining the security and integrity of LSSU's data and systems.

Review Cycle:

This policy will be reviewed annually by the IT Department to ensure its effectiveness and relevance to evolving security threats and university operations.