LAKE SUPERIOR STATE UNIVERSITY PROCEDURES MANUAL
Administrative Policy

Section: Information Technology | Section Number: 3.3.3

Subject: Workstation and User Security Risks Management | Date of Present Issue: 10/18/2024

Date of Previous Issues: None

Policy Statement:

Lake Superior State University (LSSU) is committed to safeguarding its digital assets and sensitive information by mitigating security risks associated with workstations and end-user devices. This policy outlines the requirements and best practices for securing all workstations and user devices connected to LSSU's network, ensuring they are protected against unauthorized access, malware, and other security threats.

Scope:

This policy applies to all LSSU faculty, staff, students, who use workstations, laptops, or other user devices that access LSSU's network and information systems.

Definitions:

- **Workstation:** Any desktop computer, laptop, or similar device used by end-users to access LSSU's network and systems.
- **User Device:** Any device used by an individual, including mobile devices, tablets, and personal computers, that connects to LSSU's network.
- **Malware:** Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
- **Endpoint Security:** Security measures designed to protect individual devices that connect to a network.

Procedures:

1. **Device Registration and Authorization:**
   - All workstations and university owned devices must be authorized and registered with LSSU IT.
2. **Security Configuration and Management:**
   - All workstations and user devices must comply with LSSU's security configuration standards, including:
     - Installation of university-approved antivirus software and regular updates.
     - Enabling and maintaining firewalls and encryption where applicable.
     - Applying security patches and updates promptly to the operating system and installed applications.
     - Ensuring strong, unique passwords or passphrases are used, and multi-factor authentication (MFA) is enabled where required.

- Users must lock or log off their workstations when unattended to prevent unauthorized access.

3. **Data Protection and Encryption:**
   - Users are prohibited from storing sensitive university data on unapproved personal devices or transferring such data via unencrypted channels.
4. **Access Control and User Privileges:**
   - Access to LSSU systems and data must be granted based on the principle of least privilege, ensuring users have only the minimum access necessary for their roles.
   - Administrative privileges on workstations should be restricted to IT staff or designated personnel, and users must not have local administrator rights unless specifically authorized.
5. **Monitoring and Incident Reporting:**
   - IT will implement and maintain endpoint monitoring tools to detect and respond to potential security incidents involving workstations and user devices.
   - Users must report any suspicious activity, security breaches, or unauthorized access to the IT Help Desk immediately.
6. **Training and Awareness:**
   - LSSU will provide regular security awareness training to all users, covering topics such as phishing, malware prevention, and safe computing practices.
   - Users are required to complete mandatory cybersecurity training as part of their annual training.
7. **Decommissioning and Data Sanitization:**
   - When a workstation or user device is decommissioned, IT must ensure that all data is securely wiped, and any sensitive information is removed according to LSSU's data sanitization guidelines.
   - Devices must be returned to IT for proper disposal or reassignment, and the device's removal from the network must be documented.
8. **Enforcement and Compliance:**
   - IT reserves the right to disconnect any workstation or user device from the network that poses a security risk until compliance is achieved.

Responsibilities:

- **LSSU IT:** Responsible for implementing, enforcing, and reviewing this policy, as well as providing support and guidance to users on maintaining workstation security.
- **Users:** Responsible for following the security guidelines outlined in this policy and promptly reporting any security incidents or vulnerabilities.

Review Cycle:

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