Information Technology Report

May 15, 2026

Agenda Item #1: Information Technology Update Report

☒ Information ☐ Action ☐ Discussion

Purpose:

To provide an update on recent Information Technology projects and operational improvements. These efforts enhance campus infrastructure, strengthen systems reliability, and support the academic and administrative needs of students, faculty, and staff.

Background:

Information Technology continues to support daily campus operations while advancing system reliability, user experience, and infrastructure improvements. Over this reporting period, efforts focused on maintaining service continuity during staffing gaps, completing key infrastructure work, improving enterprise processes, and enhancing the overall user experience for students, faculty, and staff.

Recent Highlights:

IT successfully supported graduation events, delivering a significantly improved audio-visual experience for both attendees and presenters. Systems operated reliably throughout the ceremony, ensuring clear communication and a smooth event.

IT maintained full operational support during a temporary staffing shortage, ensuring uninterrupted service across campus. At the same time, the team completed several infrastructure and facilities-related projects, including wiring for new workspaces in Norris Center, supporting fire panel upgrades across seven buildings, and coordinating technical work tied to robotics and specialized lab environments. Additional updates included replacement of a campus door access controller and deployment of a new server to support hockey statistics.

On the systems side, work focused on stabilizing and improving core services. This included rebuilding key systems such as the VPN environment and print monitoring software, resolving vendor-related network issues with Barnes & Noble, and restoring monitoring integrations to improve system visibility. These efforts improved system performance, reliability, and day-to-day operations.

Support for academic and student-facing systems also continued to improve. The Virtual Lab environment has been fully restored, and access to key resources such as Statistica has been

streamlined through single sign-on. Work is ongoing to further enhance performance and provide a smoother experience for students accessing applications such as SPSS.

IT also partnered with campus departments to improve business processes and data accuracy. Financial Aid processes were streamlined to reduce manual review of award communications, and system updates were implemented to eliminate the need for annual configuration changes. Reporting improvements corrected duplicate data issues and improved accuracy for key administrative users, while ongoing collaboration with Institutional Research is standardizing reporting across departments.

In addition, following a recent federal update to the Integrated Postsecondary Education Data System (IPEDS), the Institutional Research team worked with campus partners to compile five to seven years of admissions, financial aid, and completer data within a three-month timeframe. This was a significant reporting effort completed to ensure compliance with new federal reporting requirements.

System maintenance and upgrades were completed to ensure stability and performance. Banner patching and database upgrades were successfully applied across test and production environments, including Oracle updates from version 19.26.0 to 19.30.0. These updates delivered important system improvements while keeping core systems current and minimizing disruption to campus operations.

IT staff also continued professional development in cybersecurity, AI, and data governance to stay current with emerging technologies and risks. As part of this effort, Sara Devaprasad presented at the AI Connect Conference in Sault Ste. Marie, sharing practical applications of AI tools to support teaching, content creation, and day-to-day workflows.

These updates reflect IT’s ongoing commitment to providing a secure, reliable, and user-focused technology environment. By addressing immediate needs while advancing strategic projects, we are positioning campus systems to better support teaching, learning, and operations.

Suggested Action/Motion:

N/A

President’s Recommendation:

N/A

LAKE SUPERIOR STATE UNIVERSITY

Information Technology Report

May 15, 2026

Agenda Item #2: **Information Technology Security**

☒ Information ☐ Action ☐ Discussion

Purpose:
To provide an update on cybersecurity operations, recent improvements, and ongoing efforts to strengthen institutional security and reduce risk.

Background:
Information Technology continues to build on the security improvements implemented following the recent cyber incident. The focus has shifted from recovery to ongoing monitoring, proactive risk reduction, and strengthening access controls across campus systems.

The work completed during this period represents a shift from reactive security measures to a more proactive and structured cybersecurity framework.

Recent Highlights:

Over this reporting period, cybersecurity operations have remained stable, with monitoring and alerting processes providing improved visibility into system activity. Alerts are now being identified and investigated more efficiently, allowing for faster response and better coordination with external partners.

A notable event during this period was identified by the LSSU network team through routine log monitoring. Within minutes, Merit SOC analysts joined to assist in real-time analysis. The activity was determined to be a potential risk, and traffic to the identified IP address was proactively blocked across all participating universities. This early detection and coordinated response prevented further impact and reflects the effectiveness of current monitoring and partnerships.

Overall activity levels remained relatively low, with no critical alerts reported and only a small number of active alerts requiring attention. This indicates a more controlled and stable security environment compared to previous periods.

A detailed summary of monitoring activity, response times, and threat landscape trends is included in the attached Merit Security Operations Center report.

LSSU continues to participate in regional cybersecurity collaboration through the Eastern Upper Peninsula Information Security Advisory Council (EUPISAC). This group includes IT and security representatives from Cloverland Electric, the Eastern Upper Peninsula Intermediate School District, Chippewa County, and LSSU, and provides shared situational awareness and coordinated response capabilities across the region.

As part of this partnership, LSSU will host a FEMA-supported cybersecurity training (MGT303 Cybersecurity Vulnerability Assessment) on campus in July. This opportunity reflects the value of regional collaboration while reinforcing LSSU's commitment to supporting cybersecurity awareness and preparedness across the local community.

Next Steps:

IT will continue strengthening monitoring and incident response processes while expanding cybersecurity awareness and training opportunities across campus. Efforts will also remain focused on improving authentication and access controls and maintaining strong collaboration with regional partners. These efforts continue to strengthen LSSU's cybersecurity environment, with improved visibility, more consistent monitoring, and the ability to identify and address potential risks earlier.

Suggested Action/Motion:

N/A

President's Recommendation:

N/A

Information Technology Report

May 15,2026

Agenda Item #3: Website Improvements Updates

☒ Information ☐ Action ☐ Discussion

Purpose:
To provide an update on recent website improvements completed over the summer and outline ongoing and upcoming enhancements. These efforts continue to support recruitment, accessibility, and operational goals across the university while improving user experience.

Background:
The university website remains a key tool for student recruitment, campus communication, and community visibility. Current efforts continue to focus on accessibility compliance, platform modernization, and improving how users locate and interact with information.

Major Improvements:

- Accessibility Enhancements: The main LSSU website currently maintains an accessibility score of approximately 94%, well above commonly accepted minimum standards. Work is ongoing to address remaining items including missing alt text, inaccessible form fields, color contrast issues, keyboard navigation, and page structure. These efforts ensure readiness for updated accessibility standards that went into effect in April.
- Platform Modernization (WordPress 7.0): Preparations are underway for the WordPress 7.0 update; the most significant platform and user interface change in over a decade. Work is being completed to ensure compatibility and a smooth transition when implemented.

Ongoing Improvements:

- Content Updates: Content updates continue across multiple departments, including CFRE, the Arts Center, and Purchasing.
- Website restructuring efforts are underway to improve navigation and reduce buried content, making key information easier for users to find.
- Continued focus on improving usability and overall site organization**.**

Coming Soon:

- WordPress 7.0 deployment

- Orphaned page identification and cleanup.
- Light/Dark mode functionality to enhance user experience.

Recent Site Performance (Last 60 Days):

- 6.2% decrease in active users compared to previous 60 days
- 7.3% decrease in new users compared to previous 60 days
- 6.8% decrease in total page views (Traffic came from 179 countries, with the highest activity in: United States, Singapore, China, Canada, , and Vietnam) in that order.
- **Top Visited Pages:**
    - Homepage (34,000 views)
    - Directory (31,000 views)
    - Library (6,700 views)
    - Banished Words (3,300 views)
- **Traffic Sources:**
    - 81,000 direct URL entries
    - 21,000 sessions from organic Google search
    - 5,8200 referrals from other sites
    - 1,392 from social media

The website continues to move toward a modernized, efficient, and recruitment-focused design. Security has improved, content accuracy is increasing, and ongoing accessibility and usability enhancements are helping create a more consistent and user-friendly experience.

Suggested Action/Motion:

N/A

President's Recommendation:

N/A

Merit SOC Security Operations Monthly Report

Lake Superior State University | April 2026

Generated April 20, 2026

This report provides an overview of our cybersecurity operations over the past month, showcasing how we protect Lake Superior State University and provides insights into the broader cybersecurity landscape.

LAKE SUPERIOR STATE	MERIT SOC
64.3 TB DATA INSPECTED	**2,060.0 TB** DATA INSPECTED
430,422 SECURITY EVENTS	**780,371,065** SECURITY EVENTS
4 ACTIVE ALERTS	**811** ACTIVE ALERTS
14 NEW MONTHLY ALERTS	**142** NEW MONTHLY ALERTS
0 CRITICAL ALERTS	**0** CRITICAL ALERTS

ACTIVE ALERTS BY TYPE

LAKE SUPERIOR STATE	TYPE	MERIT SOC
2	Sensitive Port	74
1	Spyware	17
1	Open Vulnerability	248
0	Zero-Day Malware	6
0	Merit Darknet	2
0	External Report	1
0	Malware Sinkhole	16
0	Malware Honeypot	3
0	Network Exploit	421
0	Phish Report	23

INCIDENT RESPONSE TIMES

Average	3.6 min
95th Percentile	3.1 min
Maximum	5.3 min

ALERT STATUS SUMMARY

Open Alerts	3
New (30 Days)	1
Resolved (30 Days)	13

OPEN ALERT SEVERITY

Low	0
Medium	3
High	0
Critical	0

EXECUTIVE SUMMARY

Overall activity for the reporting period remained relatively quiet, with the Merit SOC team primarily responding to a small number of CrowdStrike-related alerts and inquiries. The most significant accomplishment was the rapid, coordinated response to a potential security event on April 17, where both the Lake Superior State University and Merit SOC teams worked in close partnership. Following a firewall alert, the teams quickly triaged the activity, collected and analyzed relevant network data, and confirmed that no data loss or compromise had occurred. Appropriate blocking measures were implemented, along with continued monitoring and alerting to ensure ongoing visibility and protection.

Merit SOC Security Operations Monthly Report

Lake Superior State University | April 2026

Generated April 20, 2026

NETWORK DENIAL OF SERVICE (DDOS) ATTACK MITIGATIONS

LAKE SUPERIOR STATE

0

Mitigations

MERIT SOC

859

Total Mitigations

TOP MITIGATIONS THIS MONTH

No events requiring mitigation occurred.

PROACTIVE THREAT HUNTING

THREAT HUNTING

94

Hours

WHAT WE FOUND

Proactive threat hunting this period included identifying and resolving artifacts that were left behind by Windows Defender, as well as identifying and blocking malicious files related to the November 2025 ransomware event. Additionally, network packets and indicators are being actively searched for BPFDoor malware which has become more prominent globally.

CROWDSTRIKE EDR STATUS

881

Covered Endpoints

13

Cases Opened (30 days)

13

Cases Closed (30 days)

MERIT SOC CYBERSECURITY PROTECTION ACTIONS

20

Detailed Attack Analyses

47

Malware Detonations

720

URL Detonations

426

Threat Intelligence Searches

GLOBAL CYBERSECURITY LANDSCAPE

PRIORITY KNOWN EXPLOITED VULNERABILITIES (KEVS)

3

New This Month

→

15

Total Active KEVs Globally

PRIORITY COMMON VULNERABILITIES & EXPOSURES (CVES)

115

New This Month

→

1,728

Total CVEs Globally

CURRENT THREAT LANDSCAPE

The cybersecurity threat landscape in April 2026 continues to pose significant challenges to higher education institutions. Ransomware groups are actively targeting universities due to valuable research data, student records, and typically constrained cybersecurity budgets. Nation-state actors, particularly those aligned with China and Russia, have intensified espionage activities targeting academic research in STEM fields, healthcare, and emerging technologies. Additionally, the education sector remains the top target for credential phishing attacks, with threat actors exploiting the open nature of academic networks and high student device turnover.