UtahStateUniversity

OFFICE OF THE PRESIDENT
Elizabeth R. Cantwell

MEMORANDUM

Date: March 8, 2024

RE: Unifying and Standardizing USU IT Support and Computer Management

USU is a dynamic and innovative institution, rapidly expanding our influence in the state and nation. As we grow, we bear a heightened responsibility to our constituents and research sponsors to do so in a scalable, compliant, secure way. Over the next year, USU will standardize IT support, processes, and cybersecurity controls for all university-owned computers and data processing and storage systems. We need to ensure that 100% of these computers and systems are in a managed, configurable, secure, and electronically auditable state by summer 2025. This will shift computer management from a decentralized state of "asking and assuming" to a unified state of "knowing and ensuring."

Upon the recommendation of the Trustees, Vice Presidents for Research and Legal Affairs, Deans Council, and the Senior Risk Management Committee, President Cantwell and USU's CIO have tasked USU IT to complete this work. We will therefore unify and standardize IT computer support efforts, including staffing, tools, policy, and process under USU IT, creating dual reporting lines where appropriate (without reallocating budgets) for fully embedded, unit-funded IT staff. We understand that this represents a significant change compared to the individualized and decentralized approaches to IT support and computer acquisition, deployment, and management that are in place now. However, in an environment of rapidly increasing regulation and evolving threats, we must move now and we must move expeditiously.

Why is this necessary?
These foundational efforts enable USU compliance with required portions of CIS, CMMC 2.0, NIST, and NSPM-33 standards that represent best practices for cybersecurity, enable USU to receive federal contracts and grants, and to comply with USHE policy, state, and federal law. This effort will also ensure greater protection of institutional data, including student and employee records.

What does this mean to me?
Your IT support staff will do most of the work, configuring each of your computers to ensure a baseline security level, including certain required applications are installed and updated (like SentinelOne, a FEDramp certified anti-malware/anti-virus software). It will not prevent access to the software you need to do your job, nor track day-to-day activity or web browsing. It will ensure that the operating system is installed, patched, and up to date, verify appropriate hard drive encryption, and configure certain system, applications, and access controls as necessary, and allow USU and your IT support staff to ensure the state of such electronically.

When will this happen?
This will start with each computer being evaluated and configured or reconfigured manually over the next year or so. Your IT support staff will work with each of you individually to schedule time to make the change. In some cases, your device may already be correctly configured and part of this new system, as piloting and testing is already underway.

An informational website, including FAQs, scheduled webinars, and process detail is forthcoming.

Thank you,

Elizabeth Cantwell, President
Eric Hawley, CIO