Appendix B – Standards and Guidelines

In compliance with the USHE Policy R345-4.1, Weber State University (WSU) will strive to implement the Center for Internet Security (CIS) critical security controls (CSCs) as a minimum information security standard unless otherwise required to implement a different standard required by contract or law. The links to these requirements will be updated as needed.

Appendix B constitutes WSU's information security plan to implement the CIS CSCs. The IT Division and the Information Security Office (ISO) are responsible for implementing this information security standard. The IT Division and ISO may require the university community to comply with more granular requirements consistent with implementing this information security plan or as required by contract or law. The university may enhance the CIS CSCs with different security frameworks. The IT Division and ISO will review the implementation of these CSCs and, as appropriate, update them annually at a minimum.

CIS CSC 1: Inventory and Control of Enterprise Assets
The university will strive to actively manage (inventory, track, and correct) all university assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to its infrastructure physically, virtually, remotely, and those within cloud environments and accurately know the totality of assets that need to be monitored and protected within the university.

CIS CSC 2&15: Software Asset & Service Provider Management
The university will actively manage all software on the network, including operating systems and applications, by maintaining an inventory, tracking usage, and ensuring only authorized software is installed and executed. Unauthorized or unmanaged software will be identified and prevented from installation or execution. Additionally, the university will establish a process to evaluate service providers that handle sensitive data or manage critical IT platforms and processes, ensuring they implement appropriate protections for these assets.

CIS CSC 3: Data Management
The university will strive to operate processes and tooling to control, handle, retain, and dispose of the university's data.

CIS CSC 4: Secure Configuration of Enterprise Assets and Software
The university will strive to establish and maintain the secure configuration of university assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

CIS CSC 5 & 6: Account Management/Access Control Management
The university will strive to use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, service accounts, and university assets and software.

CIS CSC 7: Continuous Vulnerability Management
The university will strive to develop a plan to continuously assess and track vulnerabilities on all university assets within the university's infrastructure, to remediate and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

CIS CSC 8: Audit Log Management
The university will strive to collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

CIS CSC 9: Email and Web Browser Protections
The university will strive to improve the protection and detection of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

CIS CSC 10: Malware Defenses
The university will strive to prevent or control the installation, spread, and execution of malicious applications, code, or scripts on university assets.

CIS CSC 11: Data Recovery
The university will strive to establish and maintain data recovery practices sufficient to restore in-scope university assets to a pre-incident and trusted state.

CIS CSC 12: Network Infrastructure Management
The university will strive to implement and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

CIS CSC 13: Network Monitoring and Defense
The university will strive to operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the university's network infrastructure and user base.

CIS CSC 14: Security Awareness and Skills Training

The university will strive to establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the university.

CIS CSC 16: Application Software Security
The university will strive to manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the university.

CIS CSC 17: Incident Response Management
The university will strive to establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to attacks.

CIS CSC 18: Penetration Testing
The university will strive to test the effectiveness and resiliency of university assets by identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Revision History
Creation Date: August 3, 2023
Amended: N/A