Ensuring Secure Access to Digital Systems

Digital systems are the home for nearly all critical UW administrative data and processes. Platforms like Microsoft Office, Canvas, and Workday store intellectual property, tuition and student academic accounts, budget information, health and research data, and more. The confidentiality, integrity, and availability of these assets is secure only with the use by individuals authorized to use them.

UW does not have a university-wide policy or standard that articulates who may access digital systems. Consequently, people who separate from the university, for any reason, may continue to access digital systems for months—or even years.

Who says this practice should change?

- **University Policy APS 47.2,** which stipulates that University facilities, systems, computers, and equipment may be used only to support University teaching, research, service, and administrative functions.
- **External auditor KPMG** (2024), who has called out the lack of a decommissioning policy numerous times, most recently in a 2024 audit finding.
- **UW Enterprise Risk Management Initiative #5** finds that immediate deprovisioning of user accounts and access when no longer needed prevents data exposure and breach of information.
- **The National Institute of Standards and Technology (NIST)**, the primary federal agency that articulates standards related to cybersecurity, including who may access digital systems (NIST SP 800-53).
- **Cyber-insurance providers,** who consider digital systems access management a top consideration in whether to grant applicants coverage.
- **State CIO Security Standard 141,** which requires agencies to remove access rights to information and information processing facilities upon termination or change in status of employees.

In addition to helping to meet these mandates, the standard will assist the UW in meeting security responsibilities for data protected under FERPA, HIPAA, and other privacy-related laws or regulations.

UW-IT is charged with the protection of digital systems

in Executive Order 63, and Administrative Policy statements 2.3, 2.5, and 2.6. To meet that obligation and consistent with its responsibility to set minimum security standards, UW-IT proposes to create the following standard for access to digital systems:

> *Only enrolled students and regular and contracted employees engaged in UW teaching, research, administrative, educational or other necessary functions are authorized to use UW information & technology systems, including but not limited to email, teleconferencing, data management, learning management systems, and finance and human resources systems.*
>
> *Separation from the University shall coincide with termination of access to digital University systems and use of University information technology equipment.*

Draft Implementation Timeline

- **April 1 – May 1, 2025**: Address HR concerns for providing benefits and tax documents to individuals after they separate; solicit stakeholder feedback/concerns.
- **May 1 through Sept. 30, 2025:** Communicate new access standard to the university community.
- **June 1 through June 30, 2025**: Phase 1 of implementation, which includes only UW Medicine Employees.
- **July 1 – October 30, 2025:** Phase 2 expands scope of implementation to UW Academy Employees.