January SYS Institution Policy Distribution and Medical Withdrawal Policy Approval

UW System Administrative Policies <SYSPolicies@uwsa.edu>
Fri 1/22/2021 6:46 PM

January Policy Distribution

This email is going to Provosts, CBOs, SSAOs, CDOs, CIOs, Senior Strategic Enrollment Officers, Financial Aid Directors, Shared Governance Representatives, the Technology and Information Security Council, and Designated Institutional Policy Contacts. Please distribute to others as needed.

The one policy and one procedure in the January Policy Distribution are listed below:

- SYS 1042, Information Security: Threat and Vulnerability Management

Click on the links from the "January Distribution Policies" button to view the drafts and ensure that your feedback is captured for review during the post-comment period. Comments can include attachments, including word documents and PDFs.

Below find brief summaries of the policies. Complete summaries are located at the top of the draft policy pages.

Submit feedback for the policies by Friday, February 5, 2021.
SYS 1042, Information Security: Threat and Vulnerability Management

This policy will be effective February 1, 2022.

The purpose of SYS 1042, Information Security: Threat and Vulnerability Management is to establish the minimum requirements for vulnerability management, vulnerability scanning, patch management, threat intelligence and penetration testing of University of Wisconsin (UW) System information technology (IT) assets.

- All University-owned or leased IT assets must have an operational process and technical enforcement for discovering, reviewing, reporting, and remediating vulnerabilities.

- Institutions shall report and confirm compliance with this policy on an annual basis.


This procedure will be effective February 1, 2022.


- Automated vulnerability scanning tool(s) must be run against University-owned or leased IT assets on a periodic basis commensurate with asset risk profile.

- Penetration testing of University owned information systems, services, and supporting infrastructure containing high risk data must be conducted on a regular basis and such testing must be performed by a qualified assessor.

- UW Institutions must conduct routine threat Intelligence gathering and sharing.

- UW institutions are responsible for maintaining a documented patch management program.

- UW institutions are responsible for reporting and preparing documented vulnerability and patch management metrics.
Tuition & Fees Policy Approved

On January 19, 2021, President Thompson approved the new system administrative policy SYS 807, Medical Withdrawal Policy. For more information on the SYS policy revision, see below.

SYS 807, Medical Withdrawal Policy

This policy will be effective September 1, 2021.

Summary of Policy

· This policy outlines provisions with respect to medical withdrawals and refunds beyond the 100% refund date.

· Requires that one central office must administer the policy, and one central and secure database house all of the medical withdrawal documents.

· Requires that the policies and associated campus procedures be made available to students as a part of the Registrar’s polices and procedures for all students.

· Lists the supporting documentation requirements for a medical withdrawal approval.

· If the policy has been revised, identify the places within the document that the policy revisions occur. When at all possible, list the specific section, subsection, and paragraph number for each revision.

· Provides the timeline in which students may request a withdrawal and how to calculate the timeframe on transcripts and for repayments.

· Provides a tuition and fee refund schedule based on course length.

· Specifies how this policy should be integrated with related campus processes.

Affected Areas on Campuses

· This policy applies to the institutional Registrar’s Offices and Offices of Financial Aid, as well as the office designated to administer the policy.

Campus Implementation

· Institutions must adhere to the provisions of this policy, and must develop their own procedures to operationalize this policy. Institutions may also develop guidance to support this policy.

Additional Communication
· Additional communication will be provided prior to the effective date.

Stay updated with the policy development process by subscribing to an RSS feed [here](https://outlook.office.com/mail/inbox/id/AAQkADkyYmQ0ZGM5LTJkNzQtNDg4Yy04MTJmLTZkNTUwZGUwN2ZiZgAQPHMLMcivkC8kZB3s2kmFtk%3D). You can use this feed with your favorite RSS reader or subscription service.