January SYS Policy Distribution

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

As a reminder, there are one policy and one procedure in the January SYS Policy Distribution, 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 policy and procedure. Complete summaries are located at the top of the draft policy and procedure 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
Stay updated with the policy development process by subscribing to an RSS feed [here](#). You can use this feed with your favorite RSS reader or subscription service.