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

March Policy Distribution Reminder

As a reminder, the four policies in the March Policy Distribution are listed below:

- SYS 236, Utilization of Independent Contractors
- SYS 350, Payment Card Integrity Policy
- SYS 1228, Telecommuting

The policies above have a two-week comment period. Submit feedback for the policies above by Friday, April 2, 2021.

- SYS 138, Award of Credit by Prior Learning Assessment

The policy above has a 60-day comment period. Submit feedback for the policy above by Tuesday, May 19, 2021.

Click on the links from the "March 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.
SYS 236, *Utilization of Independent Contractors*

*This policy will be effective upon approval.*

This policy establishes the requirements associated with UW institutions use of independent contractors and the processes that may be used for payments related to their services. Revisions align the policy with current procurement practices.

SYS 350, *Payment Card Integrity Policy*

*This policy will be effective upon approval.*

This policy provides guidance and procedures to prevent loss or disclosure of cardholder data. Proposed revisions to the policy incorporate the most current version of PCI DSS requirements and add in directives for compliance assessments.

SYS 1228, *Telecommuting*

*This policy will be effective upon approval.*

This policy enables, but does not require, UW System Institutions to establish telecommuting arrangements with employees when appropriate and desirable for the institution and the employee. Telecommuting arrangements are permitted when approved by the employee and their immediate supervisor with notice of the agreement provided to the appropriate Vice Chancellor/Vice President or designee; when it is feasible that an employee could fulfill their job duties from an alternate location for the period covered by the arrangement; and when the telecommuting arrangement does not disrupt the operations of the UW System.
SYS 138, *Award of Credit by Prior Learning Assessment*

*This policy will be effective upon approval.*

This is a new policy and represents the elevation of a section of SYS 135 to a separate policy, set of procedures, and guidance. The policy outlines the definitions, evaluation and documentation practices for prior learning assessments.

## Information Security Policy and Procedures Delayed Effective Date

On April 24, President Thompson approved a technical revision to *SYS 1039, Information Security: Risk Management.*


The technical revisions delay the effective date of the policies and procedures until **January 1, 2022.** See a detailed summary of the revisions below:

*SYS 1039, Information Security: Risk Management*

*This policy and these procedures will go into effect on January 1, 2022*

**Summary of Policy and Procedures**

- This policy and procedures have been developed to establish expectations for Information Security Risk Management activities, as described below:
  - **SYS 1039:** The policy provides a formal structure for the management of information security (IS) risks occurring within the University of Wisconsin (UW) System.
  - **SYS 1039.A:** This procedure establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin (UW) System.
  - **SYS 1039.B:** This procedure defines the specific method and information required to document, track and provide notification of risk acceptance of information security-related requirements throughout the University of Wisconsin (UW) System.
  - Due to delays in the implementation of ERM and the requested security actions from President Thompson to address cyber
security incidents, the effective date of this policy and procedures is delayed.

- The policies and procedures will now go into effect on January 1, 2022.
- The policy scheduled review date is one year from the effective date, in January 2023.

**Affected Areas on Campuses**

- Each institution’s information technology office, led by its Chief Information Officer (CIO), is responsible for communicating this policy and associated procedures to its community of constituents.
- This policy and associated procedure documents are applicable to all institutions, schools, departments and employees of UW System, including academic staff, university staff, faculty, student employees, and researchers, as well as third-parties, such as authorized contractors and vendors, who have access to UW System data and/or systems.

**Expectation of Campuses on UWSA Policy Reporting**

- It is expected that the identified institution’s Chancellor or their designee will regularly report to UWSA on the implementation status of this policy and the associated procedures.

**Additional Communication**

- The UW System Office of Information Security will ensure information security risk management training materials are made available to UW System leaders, managers, system developers and users.
- Further reminder communications will be sent prior to the effective date.

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.

Unsubscribe