UNIVERSITY OF WISCONSIN SYSTEM

Stefan Fletcher
Director, Administrative Policies & Special Projects
Suite 209, 780 Regent St.
Madison, WI 53715
(608) 262-8939
sfletcher@uwsa.edu
http://www.wisconsin.edu

November 16, 2020

Below please find a listing of all approved System Administrative policies and procedures taken from October 12, 2020 through November 13, 2020.

I. New System Administrative Policies

SYS 540, *Non-Competitive Procurement Contracts* (Approved October 26, 2020)

- This policy defines when a non-competitive negotiation can be used to award a contract. It also identifies the dollar thresholds at which an additional level of approval must be sought.
    - Purchasing Directors may sign non-competitive contract up to $149,999.
    - The Vice Chancellor must approve non-competitive contracts over $150,000. At UW Madison and UW Milwaukee the Associate/Assistant Vice chancellor can approve contracts over $150,000.
    - Non-competitive contracts, with private, profit-making organizations , valued over $1,000,000 must be approved by UW System institution's Vice Chancellor, the UW System Office of Procurement, reviewed by the UW System Office of General Counsel, and approved by the Board of Regents prior to execution.
        - If federal dollars are used a Cost Analysis must also be performed, per federal regulations.

SYS 1000, *Information Security: General Terms and Definitions* (Approved October 13, 2020)

- The purpose of this policy is to provide a list of general terms and definitions that are used in the 1000 series of the UW System Administrative policy set as well as additional definitions, as required, to provide clarity and consistency across all UW System Administration information security policies, documents and systemwide initiatives.
- New definitions, and material edits to existing definitions, will be circulated for institutional vetting prior to addition to this policy.

SYS 1039, *Information Security: Risk Management* (Approved October 13, 2020)

- The policy provides a formal structure for the management of information security (IS) risks occurring within the University of Wisconsin (UW) System.
    - Establishes standard methods for Information security risk management associated with all institution owned or leased information systems that process, maintain, transmit or store data used to accomplish UW System research, teaching and learning, or administration.
    - Establishes standard methods to ensure that the likelihood and impact of threats and vulnerabilities are understood and minimized to the furthest extent practical.
    - Creates a repository known as the Risk Register, for the identification, management, reporting, and tracking of implementation of controls, in relation to Information security risks and the assessment of those risks.
    - Documents accepted risks in situations in which a UW institution does not implement a standard control or process.
    - Establishes responsibility for ensuring information security risk management training materials are made available to leaders, managers, system developers and users.

SYS 1040, *Information Security: Privacy Policy* (Approved November 13, 2020)

- This policy has been developed to establish expectations for the handling and protection of UW System community member's personal data, set the tone and foundation for a systemwide Privacy Program, and address core privacy ideologies and expectations of our students and staff. This policy has also been developed to ensure UW's compliance with current and future privacy legislation. Core components of this policy include:
  - Limiting the collection, use, sharing and storage of personal data to that which reasonably serves the institution's academic, research, administrative functions, or other required purposes. If data is collected that does not fall within these limits, institutions are required to provide opt-in capabilities for data subjects to control their processing preferences;
  - Requirement to notify data subjects, prior to collection, what personal data is being collected, how it is being processed, and who it will be shared with;
  - Requirement to allow data subjects to review their own personal data and request corrections when inaccuracies are found;
  - Requirement for institutions to identify a Privacy Officer, who will act as the primary point of contact for privacy related matters;
  - Requirement for UW System to appoint a Chief Privacy Officer to develop and lead a systemwide Privacy Program;
  - Outlines a reasonable expectation of privacy, consistent with RPD 25-3, *Acceptable Use of Information Technology Resources*;
  - Reporting requirements for suspected violations or breaches of privacy; and
  - Requirement for the publication of a Website Privacy Statement for each institution's website.

II. New System Administrative Procedures

SYS 1039.A, *Information Security: Risk Management Procedure* (Approved October 15, 2020)

- This procedure establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin (UW) System.
  - Establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin.
  - Enables UW System institutions to proactively assess, mitigate, and manage information security risk throughout the enterprise.
  - Enables UW System institutions to capture information security risks in a formal, standardized manner.
  - Assigns formal information security risk ownership, treatment and validation.
  - Establishes a formal method for the assessment of likelihood, impact and resulting overall information security risk(s) throughout UW System.

SYS 1039.B, *Information Security: Notification of Risk Acceptance* (Approved October 13, 2020)

- 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.
  - 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.

SYS 1040.A, *Information Security: Privacy Procedure* (Approved November 13, 2020)

- This procedure has been developed to establish expectations for the handling and protection of UW System community member's personal data, set the tone and foundation for a systemwide Privacy Program, and address core privacy ideologies and expectations of our students and staff.
  - Core components of this procedure include those listed in the policy section above.

III. Substantively Revised System Administrative Policies

SYS 1, *Development, Revision, and Approval of UW System Administrative Policies, Procedures, & Guidelines* (Approved November 11, 2020)

- The revisions implement a formal interim policy and procedure framework for the UW System Administrative (SYS) policy series.
- A definition was added for "Interim Policy/Procedure Action."
- The formal interim policy practice is as follows:
  - An interim policy/procedure action will either:
    - draft a new interim SYS policy or procedure to address an emergency, where an interim policy/procedure action addresses a high-level concern that requires clarification sooner than would be allowed by the full SYS policy review process (e.g., furloughs to address financial challenges of COVID-19), with the intention that a normal SYS policy or procedure will be drafted and reviewed to replace the interim policy action; or
    - amend or waive provisions of an existing policy or procedure during the course of an emergency situation, if the action is only temporarily necessary (e.g., one-time extension of the due date of a required report).
  - All interim policy/procedure actions will include an expiration date, which can be no longer than one year after the policy action is approved. An interim policy/procedure action may only be extended beyond a one-year period from the original issuance date under extraordinary circumstances. The policy owner must provide justification in writing, and that justification must be approved by the relevant UW System Vice President(s) and the UW System President prior to any extension taking effect.
  - An interim policy/procedure action that is originally published with an expiration date of less than a year from its original issuance date may be extended up to a year from its issuance date upon approval by the UW System President.
  - All interim policy/procedure actions must be approved by the UW System President.
  - If an interim policy/procedure action addresses a need in the UW System that will exist beyond one year or the original justified effective period, a related draft SYS policy or procedure will be created and sent through the SYS policy review process.

IV. Substantively Revised System Administrative Procedures

SYS 175.A, *Accreditation Visits and Reports Procedures* (Approved November 5, 2020)

- These procedures state the actions required for regional accreditation and the role of the UW System Administration in the review.
  - Removes the requirement for the UW System President and Associate Vice President of Academic Programs & Faculty Advancement to receive a copy of an institutional self-study prior to accreditation team visits.
  - Requires that a representative from the Office of Academic and Student Affairs meets with the accreditation team, along with the UW System President.
  - Specifies that the UW System President and Vice President of Academic and Student Affairs must receive a copy of the accrediting team's report ***at least one week in advance of the visit.***

V. Technically Revised System Administrative Policies

SYS 1030, *Information Security: Authentication* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.
- Updated **section 9, Scheduled Review** dates in a few policies to ensure a consistent review strategy within the 1000 series of policies. New policies and procedures going forward will be reviewed within one year from *effective date*, and within a maximum of two years thereafter.
  - Changed from September 2020 to March 2021 (one year from effective date)

SYS 1031, *Information Security: Data Classification and Protection* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.
- Updated **section 9, Scheduled Review** dates in a few policies to ensure a consistent review strategy within the 1000 series of policies. New policies and procedures going forward will be reviewed within one year from *effective date*, and within a maximum of two years thereafter.
    - Changed from April 2021 to June 2022 (two years from last revision)

SYS 1032, *Information Security: Awareness* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.

SYS 1033, *Information Security: Incident Response* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.

SYS 1035, *Information Security: IT Asset Management* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.
- Updated **section 9, Scheduled Review** dates in a few policies to ensure a consistent review strategy within the 1000 series of policies. New policies and procedures going forward will be reviewed within one year from *effective date*, and within a maximum of two years thereafter.
    - Changed from August 2021 to September 2022 (one year from effective date)

VI. Technically Revised System Administrative Procedures

SYS 1030.A, *Information Security: Authentication Procedure* (Approved November 13, 2020)

- Updated section 5, Definitions, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.

SYS 1031.A, *Information Security: Data Classification* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.

SYS 1031.B, *Information Security: Data Protections* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.

SYS 1035.A, *Information Security: IT Asset Management Standard* (Approved November 13, 2020)

- Updated **section 5, Definitions**, to reference the newly created SYS 1000, *Information Security: General Terms and Definitions* policy. Terms found within this section remain.