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

March 18, 2022

Below please find a listing of all new and revised Regent Policy Documents and UW System Administrative policies and procedures approved from February 11, 2022, through March 17, 2022.

I. New UW System Administrative Policy Approval

- SYS 625, *Youth Protection and Compliance* (approved March 10, 2022; effective March 1, 2023)
    - This policy establishes the minimum standards for the protection of Youth engaged in Covered Activities throughout the University of Wisconsin System (UW System). The policy outlines each of the components to be included in UW System institutions' policies related to protection of Youth engaged in Covered Activities. The policy applies to all UW System institutions, and the scope of the policy is limited to Youth Participants in Covered activities.
    - Institutions are charged with centrally documenting all youth participants data.
    - All covered activities shall be centrally registered and properly insured.
    - All youth serving staff, whether an employee or volunteer shall be screened, vetted, and centrally registered.
    - All independent contractors with access to youth need to be screened accordingly and centrally documented.
    - Prior to working with a minor all staff without interruptions in service shall contact their institution's Human Resources department to disclose the intent to work with minors and confirm they have the appropriate screening for the capacity in which they will be involved with youth.
    - All covered activities shall have safety/emergency procedures that specifically addresses youth.
    - All Third Parties will be required to sign a contract with the institution which clearly outlines the responsibilities and requirements of the Third Party under the policy.
    - Institutional youth protection policies will specifically address athletic recruitment that is in alignment with current Safe Sport recommendations.

II. Revised UW System Administrative Policy Approvals

- SYS 920, *Standards Manual for UW Managed Capital Projects* (approved February 17, 2022; effective July 1, 2022)
    - The policy establishes the requirement that the Capital Planning & Budget (CPB) department create, manage, and regularly update a standards manual for guiding the project delivery of UW Solely Managed (UW-managed, also known as Gift & Grant) capital projects for the University of Wisconsin System. The policy notes

salient aspects of UW-managed projects that the manual will include and establishes the rationale for having the manual. The policy also establishes the expectation for applicable employees and third parties to adhere to the provisions of the manual. Institution Comments and Concerns
    - There were no comments submitted during the distribution feedback period.
    - After distribution, the policy effective date was updated to July 1, 2022, to align with the publication of the Standards Manual to which the policy refers.
- SYS 1000, *Information Security: General Terms and Definitions* (approved and effective as of March 8, 2022)
    - 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. Revisions to the policy include:
    - Updated policy and procedures links to Related Documents in section 7
    - Added definitions from SYS 1037, SYS 1041, and SYS 1042 to section 5.
    - There were no comments submitted during the distribution feedback period.
- SYS 1036, *Information Security: Endpoint Protection* (approved February 17, 2022; effective February 17, 2023)
    - The purpose of this policy is to provide structure for the deployment and management of endpoint protection systems and controls used to mitigate Information Security threats throughout the University of Wisconsin. This policy only applies to UW System owned or leased endpoints.
    - Where technically feasible, institutions are expected to deploy malware protection software, maintain supported operating systems, adhere to principles of least privilege, and employ controls to prevent unauthorized physical and logical access to endpoints.
    - Institution Comments and Concerns
    - The policy team received significant feedback on both the policy and procedure throughout the development process. All feedback was taken into consideration during final revisions and significant changes were made to both the policy and procedure documents. This resulted in the removal of entire policy segments, which changed the formatting and numbering of policy and procedure statements.
    - If institutions have any questions regarding how their specific feedback was considered, please send an email to informationsecurity@uwsa.edu with your name, the institution you represent, and a copy of the submitted feedback you would like to discuss.
    - Please also see the related, revised system administrative procedure:
        - SYS 1036.A, *Information Security: Endpoint Protection Standard*
- SYS 1037, *Information Security: IT Disaster Recovery* (approved and effective as of March 8, 2022)

- This policy establishes the minimum requirements for an Information Technology (IT) Disaster Recovery (DR) Plan for University of Wisconsin (UW) institutions and is designed to assist in executing recovery processes in response to a disaster or significant IT disruption. Revisions to the policy include:
- Moved following definitions in section 5 to SYS 1000 and updated standard definition section language:
  - Data Backup
  - Disaster Recovery (DR) Plan
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- There were no comments submitted during the distribution feedback period.

- SYS 1041, *Information Security: Logging and Monitoring* (approved March 8, 2022; effective July 1, 2022)
  - The purpose of this policy is to establish a consistent expectation of security logging and monitoring practices across the University of Wisconsin (UW) System to aid in the early identification and forensics of security events. Revisions to this policy include:
  - Moved following definition from section 5 to SYS 1000:
    - High Impact System
  - Removed definition for IT Asset
  - There were no comments submitted during the distribution feedback period.
- SYS 1042, *Information Security: Threat and Vulnerability Management* (approved March 8, 2022; effective April 1, 2022)
  - This policy establishes the minimum requirements for vulnerability management, vulnerability scanning, patch management, threat intelligence and penetration testing of University of Wisconsin (UW) System information technology owned or leased IT assets. Revisions to the policy include:
  - Moved the following definitions from section 5 to SYS 1000:
    - Vulnerability Scanning
    - Vulnerability Management
    - Patch Management
    - Penetration Testing
    - IT Asset Owner
  - There were no comments submitted during the distribution feedback period.

III. Revised UW System Administrative Procedure Approvals

- SYS 1030.A, *Information Security: Authentication* (approved and effective as of March 2, 2022)

- This procedure describes the minimum authentication standards that must be met by University of Wisconsin (UW) System institutions. Revisions to the procedure include:
- In section 5 (Related Documents), updated NIST 800-53v4 reference to NIST 800-53v5
- There were no comments submitted during the distribution feedback period.

- SYS 1031.A, *Information Security: Data Classification Procedure* (approved and effective as of March 2, 2022)
  - This procedure outlines a method to classify data according to risk to the University of Wisconsin System and assign responsibilities and roles that are applicable to data governance. Revisions to this procedure include:
  - In subsection 4.C, updated financial account number language to be consistent with Wis. Stats. § 134.98
  - Added link to Information Security Compensating Control Request Form to section 5, Related Documents.
  - There were no comments submitted during the distribution feedback period.
- SYS 1036.A, *Information Security: Endpoint Protection Standard* (approved February 17, 2022; effective February 17, 2023)
  - This procedure provides a formal structure for the deployment and management of endpoint protection systems and controls used to mitigate Information Security (IS) threats throughout the University of Wisconsin (UW) System.
  - For more information, please see the summary of SYS 1036, *Information Security: Endpoint Protection* above.
- SYS 1039.A, *Information Security: Risk Management Procedure* (approved and effective as of March 2, 2022)
  - This Information Security Risk Management (ISRM) procedure establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin (UW) System. Revisions to the procedure include:
  - Updated NIST 800-53v4 reference in section 1 (Policy Purpose) and section 2 (Related Documents) to NIST 800-53v5
  - There were no comments submitted during the distribution feedback period.
- SYS 1042.A, *Information Security: Threat and Vulnerability Management Standard* (approved March 8, 2022; effective April 1, 2022)
  - The purpose of this procedure is to establish the minimum requirements for vulnerability management, vulnerability scanning, patch management, threat intelligence and penetration testing of University of Wisconsin (UW) System owned or leased information. Revisions to this procedure include:
  - Updated definition section language to conform with rest of the SYS 1000 series policies
  - There were no comments submitted during the distribution feedback period.

IV. Upcoming Policy Effective Date Reminders

The following policy and procedure will go into effect on **April 1, 2022.**

- SYS 1042, *Information Security: Threat and Vulnerability Management*
- SYS 1042.A, *Information Security: Threat and Vulnerability Management Standard*

V. Policies in the Final Stages of Revision

The following policies were distributed for comment in prior months and are currently being revised by the policy owners:

- Rescission of SYS 150, *The Application of Job Market and Placement Information to Academic Planning*
- SYS 822, *Student Services Funding*