The University of Wisconsin Oshkosh
Procedure # UWO.IT.1033.A
Information Security: Incident Response

Original Issuance Date:	September 14, 2016
Last Revision Date:	September 14, 2016
Next Review Date:	March 2017

1. PURPOSE

The purpose of these procedures is to define the steps required to respond to an information security incident at UW Oshkosh.

2. RESPONSIBLE OFFICER

Chief Information Officer

3. SCOPE

These procedures apply to all incidents involving information not classified as low risk data regardless of form. These procedures also include requirements for other computer system and network related incidents that do not involve the potential unauthorized disclosure or use of information.

4. BACKGROUND

The President of the University of Wisconsin System is empowered to establish information security polices under the provisions of Regent Policy Document 25-5 (https://www.wisconsin.edu/regents/policies/information-technology-information-security/). The UW System and UW Oshkosh are committed to a secure information technology environment in support of institutional mission. These procedures are designed to help ensure effective and consistent information security incident response throughout the University of Wisconsin System.

5. DEFINITIONS

Employees: All faculty, staff, and student-workers.

High Risk Data: Data assets classified as high risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

Individuals: All faculty, students, and staff.

Institutions: All four year campuses of the UW System, UW Colleges, the University of Wisconsin- Extension, and UW System Administration.

Low Risk Data: Data assets classified as low risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

Moderate Risk Data: Data assets classified as moderate risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

6. PROCEDURES

1. Any individual who suspects that an information security incident has likely occurred, shall report the incident through email or phone call to any of the following:
    a. Chief Information Officer (CIO).
    b. Information Security Officer (ISO).
    c. Information Technology Helpdesk.
    d. University Police.
2. Helpdesk personnel and University Police shall immediately inform the CIO or ISO of the incident reported.
3. Unless otherwise delegated, the CIO is the Incident Commander overseeing all incident response teams and actions.
    a. In the absence of the CIO, the ISO is the default Incident Commander overseeing all incident response teams and actions.
4. The Incident Commander shall convene appropriate incident response teams and roles, depending on the circumstances of the incident, with the following responsibilities:
    a. Incident Management Team: Information Technology leaders shall direct the work of the Incident Containment Team and Incident Communications Team.
    b. Incident Containment Team: Information Technology specialists appropriate to the circumstances of the incident shall work on containing the spread of damage and to the extent possible reducing or controlling existing damage.
    c. Incident Communications Team: Information Technology leaders and University Communications specialists shall develop and execute communications according to the circumstances of the incident.
    d. All teams under direction of the Incident Commander shall consult with Subject Matter Experts as needed, such as Risk Management, UW System Legal Counsel, etc.
5. The Incident Commander shall assign a severity level to the incident of High, Medium, or Low depending on the risk level of the data involved, as well as the breadth and depth of the incident and other risk factors associated with the incident.

6. Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for the initial investigation into an alleged incident.
7. Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for containment of a confirmed incident commensurate with the severity level and circumstances of the incident.
8. Under the oversight of the Incident Commander, the Incident Management team shall determine the steps for communication of a confirmed incident commensurate with the severity level and circumstances of the incident.
9. Under the oversight of the Incident Commander, the Incident Management team shall determine the appropriate escalation path of a confirmed incident commensurate with the severity level and circumstances of the incident.
    a. An incident assigned a severity level of High or Medium shall be reported to University Police, University Risk Management, UWSA Risk Management, UWSA Chief Information Officer and UWSA Legal Counsel if needed.
10. In consultation with University Police, University Risk Management, UWSA Risk Management, UWSA Chief Information Officer and UWSA Legal Counsel if needed, the Incident Commander shall determine the requirements for internal notification and external reporting and notifications.
11. Under the oversight of the Incident Commander, the Incident Management team shall determine the documentation and evidence to be collected according to the circumstances of the incident.
12. Under the oversight of the Incident Commander, the Incident Management team shall conduct an after-action debriefing session to evaluate the incident and the incident response for purposes of gleaning lessons learned to prevent future incidents or improve future incident responses.
13. All documentation and evidence collected in response to the incident will be kept in secure storage until the Incident Commander determines it can be released.

7. REFERENCES

UW System Administrative Policy 1031, Information Security: Data Classification
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/

UW System Administrative Policy 1031, Information Security: Data Classification
(https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/)

UW System Administrative Procedure 1032.A, Information Security: Awareness
(https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)

UW System Administrative Procedure 1034, Information Security: Acceptable Use (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-acceptable-use/)

UW System Operational Policy GEN 13 Layoff for Reasons of Budget or Program (https://www.wisconsin.edu/ohrwd/download/policies/ops/gen13.pdf)

Regent Policy Document 25-5, Information Security (https://www.wisconsin.edu/regents/policies/information-technology-information-security/)

Wisconsin Administrative Code s. 35.93, Chapter UWS 4, Procedures for Dismissal (http://docs.legis.wisconsin.gov/code/admin_code/uws/4.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 11, Dismissal of Academic Staff for Cause (http://docs.legis.wisconsin.gov/code/admin_code/uws/11.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 17, Student Nonacademic Disciplinary Procedures (http://docs.legis.wisconsin.gov/code/admin_code/uws/17.pdf)

8. POLICY

These procedures fulfill the requirements of Policy # UWO.IT.1033 Information Security: Incident Response.

9. REVISION HISTORY

09/14/2016	Effective date of UW System policy
06/30/2017	Effective date of UWO Procedures.