

**The University of Wisconsin Oshkosh**  
**Policy # UWO.IT.1033**  
**Information Security: Incident Response**



---

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

## **1. PURPOSE**

The purpose of this policy is to require the creation of an information security incident response procedure at each UW System institution. This policy facilitates the consistent implementation of the procedures necessary to detect and react to information security incidents, determine their scope and risk, respond appropriately to the incident, mitigate the risks, communicate the results to all stakeholders, and reduce the likelihood of the incident from reoccurring. This policy identifies those elements that should be contained in the information security incident response procedures. This policy also defines the requirements for notification of incident information between UW System institutions and University of Wisconsin System Administration.

## **2. RESPONSIBLE OFFICER**

Chief Information Officer

## **3. SCOPE**

This policy applies to all information not classified as low risk data regardless of form at each University of Wisconsin System institution. This policy also includes requirements for procedures 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 policies 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. This policy is designed to help ensure effective and consistent information security incident response procedures 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. POLICY STATEMENT

1. Any individual who suspects that an information security incident has likely occurred, shall report it to the appropriate institution personnel.
2. The Office of the CIO shall maintain and enforce an information security response procedure that includes:
  - a. Procedures for submitting information of a potential incident to appropriate incident response personnel.
  - b. Identification of specific position(s) and/or team(s), and their roles and responsibilities, for those involved in incident response. This may include management, departmental representatives, IT response staff, institutional risk management, university communications, and legal advice.
  - c. Procedures for initial investigation and assignment of severity for a potential incident.
  - d. Procedures for investigation of a confirmed incident.
  - e. Procedures to identify actions to be taken in response to an incident.
  - f. Procedures that identify an appropriate escalation path for the incident based on severity.
  - g. Procedures for meeting the requirements for internal notification and legal requirements for external reporting and meeting notification periods.
  - h. Identification of documentation to be collected during the response to the incident.

- i. Procedures for close-out of incidents.
  - j. Procedures for the tracking and management of incident related information.
  - k. Procedures for notification to the UW System CIO within one business day if a confirmed incident involves the reasonable likelihood of a compromise of high or moderate risk data.
  - l. Procedures for updating the UW System CIO of the resolution of the incident.
3. The Chief Information Officer shall annually review and approve the incident response procedures.

## 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 Procedure 1031.A, Information Security: Data Classification

(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/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](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](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](http://docs.legis.wisconsin.gov/code/admin_code/uws/17.pdf))

**8. PROCEDURES**

Procedure # UWO.IT.1033.A Information Security: Incident Response

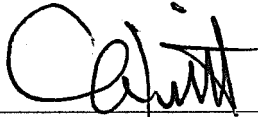
([http://it.uwosh.edu/wp-content/uploads/2015/07/PROC\\_1033.A\\_IncidentResponse\\_20170621.pdf](http://it.uwosh.edu/wp-content/uploads/2015/07/PROC_1033.A_IncidentResponse_20170621.pdf))

**9. REVISION HISTORY**

09/14/2016	Effective date of UW System policy.
06/30/2017	Approved by Chancellor Leavitt.

---

**APPROVED BY:**



---

Chancellor Andrew Leavitt