Authority

The Information Incident Response Procedure (IIRP) is authorized under the UWM Information Security Policy S59; section III-D (http://www4.uwm.edu/secu/policies/saap/index.cfm), which provides for the development of campus-wide procedures to help departments control risk.

This procedure was developed in partnership with UWM Office of Legal Affairs, UWM Risk Management, UWM Information Security Office, and UWM Internal Audit. This document will be reviewed and updated annually, by April 15th, by core members of the Information Incident Response Team.

Purpose

An IIRP is required in order to bring necessary resources together in an organized manner to deal with adverse events related to the security of UWM’s information assets. Adverse events are incidents that potentially compromise the confidentiality, integrity or availability of UWM data. Examples include malware attacks, lost/stolen property containing UWM data, unauthorized third party access to UWM systems or data and loss or compromise of paper records.

This procedure is designed to address numerous legal requirements which obligate entities to take certain actions as a result of suspected unauthorized acquisition of confidential information.

Goals

The primary goals of the IIRP are to:

1. Provide a consistent method and repeatable process to respond to information incidents.
2. Document the incident including the investigatory process, mitigating steps, conclusions and required follow-up.
3. Identify and adhere to specific record retention and disposal procedures including location, timeframe and types of documents.
4. Identify and assign appropriate campus wide roles and responsibilities.
5. Meet state, federal, UW-System, UWM and contractual requirements for information security, privacy and compliance incidents.
**Reporting**

Users of UWM information resources must report information incidents involving possible or suspected unauthorized access of UWM confidential information to the UWM Information Security Office. Reportable incidents are defined as any incident that could potentially result in unauthorized access to confidential UWM information. The following scenarios are provided as examples:

1. Loss or theft of computer systems, devices or media, where it is reasonable to believe the following:
   a. that confidential information was present at the time of loss and
   b. that unauthorized persons could access that information (for example, the information was not encrypted);
2. Intrusion by malware or other unauthorized access via any network into computer systems or devices, where it is reasonable to believe that confidential information was accessed by unauthorized persons;
3. Unauthorized entry into offices or work areas, where is it reasonable to believe that confidential information was accessed by unauthorized persons; or
4. Any other circumstances where it is reasonable to believe that confidential information may have been accessed by unauthorized persons.

Under this procedure it is not necessary to report “incidental access” by employees or other trusted persons where no harm is likely to result.

Individual departments or units may institute additional requirements or procedures; this procedure sets forth the minimum required process at UWM.

**Scope**

The intent of this procedure is to address incidents where it is reasonable to believe that unauthorized disclosure of confidential electronic or paper information has occurred. Confidential information is defined in the [ISSA Data Classification and Criticality Standards](http://www4.uwm.edu/itsecurity/).

This procedure is limited to the scope defined above and is not intended to address information threats such as denial of service, copyright violations, policy violations, spam activity, phishing, vulnerabilities resulting from missing computing system patches, virus infections and web defacement unless such activity results in the unauthorized disclosure of confidential electronic or paper information.