WAYNE STATE
UNIVERSITY
Computing & Information Technology

Standard for Incident Response

Purpose

This policy establishes the need for the University to utilize standard and documented procedures for identifying, evaluating, and responding to reported data breaches and violations of IT Security policy.

Scope

The scope of this policy covers University data being stored, processed, or transmitted on any component of IT infrastructure at Wayne State University, whether managed by central IT, distributed IT, or as part of an off-site managed service. This policy covers data as it resides on any desktop, laptop, server, hosted service, or media device.

Roles and Responsibilities

University staff members will be aware of computing events or activities that have the potential to result in disclosure of University data or system compromise, reporting them to the Information Security Office per reporting procedures.

University IT staff will be aware of system indicators or red flags that systems under their control have a potential breach of the confidentiality, integrity, or availability of University data. Furthermore, University IT staff should have the technical proficiency to assist the C&IT Information Security Office in obtaining and analyzing logs and information from systems under their control during a security incident.

University management will provide resources and support during security investigations, as well as ensuring staff have necessary resources to identify and report suspected security incidents.

The C&IT Information Security Office will act as the central organization for receiving reports of security incidents, analyzing responding to incident reports, and reporting the results of these investigations to University leadership.

Compliance

All university units are required to be in compliance with this policy and any associated standards. Any exceptions to this policy must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Incident Response Standards, Procedures, and Guidelines
Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office outlining the specific incident response controls to be implemented, along with appropriate guidance. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination
The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this policy and related standards, taking it into consideration during periodic policy review. This policy and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Standards for Incident Response

The University must use and maintain the following controls to protect against and minimize the impact of security incidents:

1. Incident Response Plan. The C&IT Information Security Office maintains a Security Incident Response Plan (SIRP) which formally defines a security incident, states the roles and responsibilities of individuals during the course of a security incident, and provides a process for these individuals to follow during incident investigation and resolution. The SIRP is updated as necessary due to technology changes or lessons learned from prior incidents, reviewed at a minimum of an annual basis, and distributed to C&IT Risk and Security Oversight members annually or when changes are made.

2. Incident Reporting. Employees report suspected incidents via one of the following means:
    a. To the C&IT Help Desk via phone call at 313-577-4357;
    b. To the C&IT Information Security Office email account at abuse@wayne.edu;
    c. To C&IT Information Security Office staff members directly via email, phone call, or in-person;
    d. To their local university IT support professional via email, phone call, or in-person. The IT support professional will then gather information and report the incident to C&IT via one of the other above means.

3. User Training. Employees and other information system users must be trained on what their role is and what they are expected to do during a suspected or actual security incident:
    a. Users must be able to identify suspected incidents and report them via established reporting channels;
    b. IT staff must be able to perform basic diagnosis and troubleshooting on information systems under their control, as well as isolate potentially impacted systems from causing further damage;
    c. Any employee, or delegate. that fulfils a role identified in the SIRP must be able to perform responsibilities as outlined in the plan;
    d. C&IT Information Security Office staff must be able to triage and diagnose security incidents, create forensic copies of data for further analysis, and execute the Security Incident Response Plan during an incident.
4. Training and information on the above topics must be provided to employees within 60 days of joining one of the above roles and every subsequent calendar year. Training must also be

provided in the event that information system changes substantially alter any of these capabilities.

5. Incident Handling. The C&IT Information Security Office is responsible for addressing reported suspected incidents and responding to them according to established procedure and the Security Incident Response Plan. Suspected incidents may be reported by a user or as a result of an automated process, script, or program that monitors for suspicious activity.

6. Incident Response Automation. Automated processes may be used to parse, identify, and respond to high volume, low impact incidents. Any incident handled by an automated process must still be recorded and tracked accordingly.

7. Incident Response Testing. A simulation or tabletop exercise is performed on an annual basis to test the effectiveness and applicability of existing incident response controls. For maximum effectiveness, testing occurs on a central information system that processes or stores confidential information.

8. Incident Response Assistance. The C&IT Information Security Office provides may provide advice, guidance, and assistance to identified affiliates of Wayne State University for reporting suspected incidents and gathering necessary information for analysis, triage, and classification.

9. External Incident Response. Upon approval of the CISO, members of the Wayne State Incident Response team may participate in State, City or Higher Education incident response consortiums and may use any processes and techniques developed by Wayne State University for this purpose.

Non-Compliance

The C&IT Information Security Office may limit access to or from a system if it does not meet the above guidelines.

Exceptions

Exceptions to these standards may be granted by the Information Security Office given business justification and a satisfactory risk assessment. In such cases, the system owner shall acknowledge the risk and take responsibility for any breaches, incidents, or compromises that occur as a result of not utilizing a supported operating system.