University of CINCINNATI	*Policy Title:* **Information Security Incident Management and Response**	*Policy Number:* **9.1.8**
Category: Information Technology	**Effective Date:** 01/23/2019	**Policy Owner:** VP & CIO UC Information Technologies
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** NA	**Responsible Office(s):** IT@UC Office of Information Security

Background

This policy forms a part of the university's data governance framework and supplements existing information security policies. It applies to information security events and incidents affecting any university information asset or information system. This policy provides direction in determining the appropriate response to a misuse of university information technology (IT) resources from within or outside the university.

The university recognizes the importance of and is committed to effective information security incident management in order to help protect the confidentiality and integrity of its information assets, availability of its information systems and services, safeguard the reputation of the university, and fulfill its legal and regulatory obligations.

Policy

This policy applies to all of the following:

- Information – whether in printed, verbal or digital form – created, collected, stored, manipulated, transmitted or otherwise used in the pursuit of University of Cincinnati (UC) mission, regardless of the ownership, location or format of the information.
- Information systems used in the pursuit of UC mission irrespective of where those systems are located.
- Individuals encountering such information or information systems regardless of affiliation.

The duty to immediately report information security events and incidents is in force at all times; whether the university is open or closed, regardless of the time of day. Faculty, staff, students, visitors and contractors must immediately report the following information security events and incidents to the IT@UC Office of Information Security (OIS) at abuse@uc.edu.

- All suspected information security events or incidents impacting the confidentiality, integrity or availability of university data.
- Suspected or actual security breaches of restricted information as defined in the Data Governance & Classification Policy – whether in printed, verbal or electronic form – or information systems used in the pursuit of the university's mission.
- Abnormal systematic unsuccessful attempts to compromise restricted information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission.
- Suspected or actual weaknesses in the safeguards protecting information or availability of information – whether in printed, verbal or electronic form – or information systems used in the pursuit of the university's mission.

IT@UC Office of Information Security will:

- Isolate from the university network information systems which are known to be, or suspected of being compromised until the incident has been investigated, resolved and risks sufficiently mitigated.
- Communicate with the Department of Enterprise Risk Management in the event of a suspected security event or incident impacting the confidentiality, integrity or availability of university data, entities affiliated with the university or using university technology resources.
- Maintain incident command and communicate with appropriate internal and external entities for incident investigation and resolution.
- Oversee and lead the incident management process to promote a coordinated, consistent, efficient and effective response.
- Leverage and coordinate with the experience, expertise and resources of other university units including applicable compliance offices and officers as necessary and appropriate.
- Immediately report and coordinate with the Department of Enterprise Risk Management and any insurance carrier regarding privacy breach response services to maximize efficiency and utility of response to significant incidents.
- Assess information security events and incidents according to the Incident Response Procedure.
- Immediately report incidents that involve personal safety or criminal activities to UC Police Department (UCPD).

- Report incidents involving regulatory matter or restricted data to the appropriate university unit.

In cases of incidents classified as High per the Incident Response Procedure, or those that may cause disruption to business services or financial loss, it is the sole responsibility of the CIO in collaboration with key university stakeholders to issue an all-clear and return of affected resources to normal operation.

Information Security Incident Response Team (ISIRT)

The ISIRT refers to members of OIS who have been identified to be the first responders for information security incidents and will act as the point of contact for information security incidents. The ISIRT will be responsible for the initial response, mitigation support and (where appropriate) escalation of information security incidents. The primary roles and responsibilities for the ISIRT are as follows:

- Incident Handler - Responsible for the overall management of the incident. Additionally, the Incident Handler will be responsible for fostering cross-team collaboration and keeping other university officials informed of the situation as appropriate.
- Incident Analyst - Responsible for overseeing the technical aspects of the response.

Upon declaration and classification of an incident, ISIRT will notify and escalate information pertaining to the incident. ISIRT will collaborate with other teams and members of the university community for incident mitigation and resolution.

Incident Response

The lifecycle of information security incident response and handling is outlined as follows:

- Preparation – writing of incident response policies, training, preparation of appropriate tools, and anything that may be required to handle an information security incident.
- Identification – when events are analyzed in order to determine whether those events might compromise an information security incident.
- Containment – the attempt to keep further damage from occurring as a result of the incident.
- Eradication – the process of understanding the cause of the incident so that the system can be reliably cleaned and ultimately restored to operational status in the following step.
- Recovery – cautiously restoring the system or systems to operational status.

- Lessons Learned – provide a final report on the incident, which will be delivered to management.

Related Links

Data Governance & Classification Policy
Information Security Incident Response Procedure
Information Security Incident Escalation Guideline

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

History

Issued: 01/23/2019