	Policy Title:	*Policy Number:*
University of CINCINNATI	**Information Security Incident Management and Response**	**9.1.8**
Category: Information Technology	**Effective Date:** 09/03/2021	**Policy Owner:** VP & CDO, Digital Technology Solutions
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** NA	**Responsible Office(s):** Office of Information Security

Background

This policy applies to information security events and incidents affecting any university data information asset or information system. The policy provides direction in determining the appropriate response to a misuse of university information technology (IT) resources from within or outside the university.

Policy

This policy applies to all 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 information security events and incidents to the Office of Information Security (OIS) at abuse@uc.edu. Incidents include but are not limited to:

- All suspected information security events or incidents impacting the confidentiality, integrity or availability of university data.
- Suspected or actual security breaches of Controlled Unclassified Information and 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.
- Unauthorized access and/or perusal of systems or data, outside of authorized duties and without business need. This could include “shoulder surfing”.

The Office of Information Security will:

- 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.

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 CDO in collaboration with key university stakeholders to issue an all-clear and return of affected resources to normal operation.

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