Information Security Incident Response

Policy Number	4-015
Responsible Authority	Vice President and CIO
Initiating Authority	Vice President and CIO
Effective Date	7/15/2021
Date of Origin	7/15/2021

APPLICABILITY/ACCOUNTABILITY

This policy applies to all members of the University community.

BACKGROUND INFORMATION

Cloud computing is an application or infrastructure resource that users access via the internet. Although they may be convenient, cloud computing services can bring risks such as data disclosure, data loss, or data compromise. The acquisition and use of a cloud-based service requires a detailed review by the Information Security Office and the Office of the General Counsel. This policy establishes the requirements and procedures necessary to ensure associated risks are managed appropriately.

POLICY STATEMENT

Federal and state regulations require the university to take reasonable measures to protect and secure electronic data containing personal information and provide swift notice to individuals of data security breaches.

It is the policy of the university to require all members of the university community to immediately report confirmed or suspected data security incidents to the Security Incident Response Team (SIRT) using the procedures outlined in this policy. Furthermore, where applicable, departmental information security, privacy, or compliance liaisons or designees are to be notified along with SIRT.

Supervisors have an elevated responsibility to ensure all individuals under their supervision have the necessary knowledge, skills, and training to follow the procedures listed in this policy.

Any violation of this policy and its procedures may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on university owned computers or university supported internet sites. In addition to these corrective actions, failure to comply with this policy and its procedures may result in disciplinary action, up to and including termination.

DEFINITIONS

Computing Resource. Personal computers, laptops, and portable computing and communication devices, such as tablets, smartphones, servers, mainframes, data storage systems, and similar equipment capable of processing, accessing, displaying, storing, or communicating electronic information.

Data. Alphanumerical or other information represented either in a physical form or digital form suitable for electronic processing or storage.

Data Custodians. Individuals or groups that are considered owners of a particular set of data that may have special or elevated requirements for their protection. Data Custodians are especially important when their data has contractual requirements mandated by a third party, such as data breach notification requirements. Examples of Data Custodians include, but are not limited to, Principal Investigators (PIs) or units that share UCF data with partner universities.

Electronic Information Resource. Data or information in electronic format and the computing and telecommunications resources through which such resources are accessed or used.

Highly Restricted Data. Any data that is strictly controlled, and protected by laws, regulations, contracts, or policies. Highly Restricted Data requires the highest level of access control and security protection, both in storage and in transit. The loss of confidentiality, integrity, or availability of Highly Restricted Data could have a significant adverse impact on the university's mission, safety, finances, or reputation. (For an extended definition, characteristics, and examples, see UCF Policy 4-008 Data Classification and Protection.)

Restricted Data. Institutional Data not identified as Highly Restricted Data, and data that may be protected by state or federal regulations, such as the Family Educational Rights and Privacy Act (FERPA.) Restricted Data must be protected to ensure that they are not disclosed in public records requests and are only disclosed as required by law and to authorized individuals only. (For an extended definition, characteristics, and examples, see UCF Policy 4-008 *Data Classification and Protection.)*

Security Event. Any suspicious act that potentially violates federal or state laws, regulations or contracts, or UCF information security policies and computer security standards.

Security Incident. Any act that violates federal or state laws, regulations or contracts, or UCF information security policies and computer security standards. Examples of security incidents include, unauthorized attempts (either failed or successful) to gain access to a computing resource, system, or data; unwanted disruption or denial of service; unauthorized use of an electronic information resource or system for processing or storing data; inappropriate usage according to UCF Policy 4-002 *Use of Information Technologies and Resources*; or the theft or loss of university restricted data as defined by UCF Policy 4-008 *Data Classification and Protection* policy.

Security Incident Response Team (SIRT). The responsible authority for all information security related events at the University of Central Florida. SIRT will establish protocols to adequately respond, handle, and make appropriate recommendations on the reporting of those incidents within the university's purview. Responsibilities of the SIRT include, but are not limited to, continually updating the security incident response plans, policies, and procedures, maintaining systems for discovering and documenting security incidents, assessing threats, processing security complaints, and handling and escalating (if necessary) security incidents. SIRT provides guidance on information and computer security incidents that impact university IT resources or threatens the confidentially, integrity, and availability of university information.

Security Incident Response Committee (SIRC). A select and diverse group of executive and technically proficient university employees, each with specific knowledge and skills, who work collaboratively to respond to and set policies and procedures for information security incidents. Responsibilities of the SIRC include, but are not limited to, continually monitoring and governing the security incident response policies and processes, providing leadership and measured responses to security incidents and public notifications of data breaches, and managing, and if necessary, escalating security incidents to senior executives.

Telecommunications Resource. Wired or wireless voice or data communications circuits or networks and associated electronic equipment.

Unauthorized Access. Any action or attempt to utilize, alter, or degrade an electronic information resource in a manner inconsistent with university policies and procedures.

Unrestricted Data. Data that is not protected by law or contract, and the disclosure of which is not reasonably expected to cause harm to the university or to the affected parties. (For an extended definition, characteristics, and examples, see UCF Policy 4-008 *Data Classification and Protection.)*

PROCEDURES

The following procedures describe how to report and respond to security incidents and events.

Mandatory Reporting Responsibilities and Response Procedures

1. **Reporting**
   Individuals working on or behalf of the university must report suspected or confirmed security incidents immediately through the following channels:

   1.1. All suspected or confirmed security incidents must be immediately reported to SIRT by emailing sirt@ucf.edu, by calling the UCF IT Support Center at (407) 823-5117, or by submitting a ServiceNow ticket located on the UCF Information Security Office website. Please keep in mind that a potentially compromised computer resource may not be reliable or suitable for reporting a security incident. Please use a system where there is no doubt of its integrity.
   1.2. All security incidents involving protected health information (PHI) or research governed data must be immediately reported to the applicable corresponding departmental information security, privacy, or compliance liaisons or designees in addition to SIRT. All individuals reporting security incidents involving these areas must review and adhere to the university's policies and procedures governing protected health information or research governed data.
   1.3. Do not include Highly Restricted Data (e.g., PII, ePHI, account credentials with passwords, etc.) when contacting SIRT via phone, email, or ticket. SIRT may request additional sensitive information through secure channels.
   1.4. Data Custodians are responsible for maintaining their own records of any contractual relationship with a third party that requires notification of a data breach to the third party, or any other data breach responsibilities placed on UCF in agreements or contracts.
      1.4.1. In the event of a breach, Data Custodians are responsible for immediately notifying SIRT of any of these requirements, enabling SIRT to invoke the security incident response plan.
      1.4.2. Data Custodians are responsible for informing SIRT of a breach of data either at UCF or a breach involving a third party/parties.
      1.4.3. SIRT will perform an analysis or an investigation and advise the Data Custodian on next steps consistent with this policy. Once SIRT has investigated, the Data Custodian may be responsible for passing on the notification of data breach, with SIRT's input, to third party, and to liaise with the third party in general. This contact with the third party should occur only after SIRT has been consulted and provided approval.
   1.5. Exception: Some security incidents may involve violation of federal and/or state law, in which case, SIRT will work with the UCF Police Department and other law enforcement agencies as necessary.

2. Security Incident Response

SIRT will address the security incident based on this policy and the severity of the incident. Incident severity takes several factors into account: sensitivity of the data involved, number of end users impacted, and its overall impact on the ability of the university to fulfill its mission.

2.1. SIRT may detect or be informed of a security incident and will investigate security events to determine whether an incident has occurred, the extent involved and impact of the incident.

2.2. SIRT will be involved in the containment and remediation of security incidents and may authorize and expedite changes to information systems and/or implement network security controls as necessary and appropriate to contain the incident.

2.3. In the course of an investigation, SIRT is authorized to access, retrieve, and monitor relevant university information resources and user's computer activities without notice or further approval and in compliance with all other university policies.

2.4. SIRT will determine the level of each security incident based on all evidence and reports, and escalate the incidents, as needed, to the SIRC and the Emerging Issues and Crisis Response Team.

2.4.1. For security incidents involving Unrestricted Data, where the impact is deemed low, SIRT will invoke the incident response plan and direct the user(s) to take corrective action to handle the security incident.

2.4.2. For security incidents involving Highly Restricted Data or Restricted Data, individuals will work with SIRT to determine if a breach has occurred. In the event of a confirmed data breach, responsible parties, under SIRT's direction, will follow the security incident response plan to meet the appropriate data breach notification and reporting laws and regulations in handling the incident.

2.5. For security incidents involving Highly Restricted Data, Restricted Data, or Unrestricted data, SIRT will conduct an initial investigation of the security incident, determine the potential risk and impact to the university, and when appropriate, convene the SIRC to determine next steps, such as determining a data breach situation based on legal and regulatory requirements, engagement of third party security, legal or cyber liability firms for further investigation, and making decisions on how to publicize security incidents per regulatory or contractual requirements.

2.6. SIRT is authorized to share indicators of compromise and security incident information, excluding personally identifiable or university system information, with partner institutions, law enforcement, government agencies, and information sharing centers, such as Multi-State Information Sharing & Analysis Center, Research and Education Networks Information Sharing & Analysis Center, etc.

2.7. Any disclosure of information regarding an information security incident must be reviewed and approved by the CIO and SIRC.

RELATED INFORMATION OR DOCUMENTS

Florida Statutes 501.171 *Security of Confidential Personal Information* (Florida Information Protection Act of 2014 (FIPA))

UCF Security Incident Response Plan

UCF Policy 4-002 Use of Information Technologies and Resources

UCF Policy 4-008 Data Classification and Protection

CONTACTS

Information Security Office, Chief Information Security Officer, infosec@ucf.edu, 407-823-3863

Security Incident Response Team (SIRT), sirt@ucf.edu
UCF IT Support Center, itsupport@ucf.edu, 407-823-5117

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-015

Initiating Authority: ma184583 Digitally signed by ma184583 Date: 2021.07.12 13:59:15 -04'00' Date: _____

University Policies and Procedures Committee Chair: Date: 6/30/21

President or Designee: Michael Johnson Digitally signed by Michael Johnson Date: 2021.07.15 15:31:11 -04'00' Date: _____