COLLEGE POLICY: 469

INFORMATION TECHNOLOGY INCIDENT RESPONSE

A. Purpose

It is vital to the UA Cossatot community that computer security incidents that threaten the security or privacy of confidential information are properly identified, contained, investigated, and remedied.

The purpose of these Guidelines is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information. The Incident Response Guidelines provide a process for documentation, appropriate reporting internally and externally, and communication to the community as part of an ongoing educational effort. Finally, these Guidelines establish responsibility and accountability for all steps in the process of addressing computer security incidents.

B. Scope

The Incident Response Guidelines (Guidelines) applies to all members of the UA Cossatot community (hereafter described as the "UAC community"). The UAC community includes faculty and staff members, students, alumni, guests, and contractors. These guidelines also include computing or network devices owned, leased, or otherwise controlled by UAC. Additionally, incidents involving confidential information apply to any computing or network device, regardless of ownership, on which confidential or restricted information is stored or by which access to confidential or restricted information might be gained. (Examples include but are not limited to a home computer containing confidential data, a mobile device on which credentials are stored which could be used to access confidential data, a server housed in an off-site facility.)

C. Process

Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the University must be reported to the Department of Information Systems Support. Anyone with knowledge, or a reasonable suspicion, of an incident which violates the confidentiality, integrity, or availability of digital information, makes an immediate report to the following e-mail address: diss@cccua.edu.

Arkansas Act 260 of the 2021 Regular Session states a public entity, or contractual provider of a public entity, must disclose, in writing, an initial report of the known facts of the security incident to the Legislative Auditor within five (5) business days after learning of the security incident. Additionally, the public entity shall provide regular updates. A report, update, notification, or list created or maintained under this section is exempt from FOIA as a security function under Ark. Code Ann §25-19-105(b)(11).

The Director of Information Systems Support, in collaboration with other appropriate staff, determines if a reported incident is or is not a confidential information security incident.

If the incident is not considered a confidential information Security Incident, the incident is referred to a Systems Administrator who will ensure that the incident is handled in accordance with the procedures described herein. The Director of Information Technology informs the Chancellor's Cabinet.

If the Director of Information Systems Support, in collaboration with other appropriate staff, determines that the incident IS a confidential data security incident, an Incident Response Team is formed. The purpose of the Incident Response Team is to determine a course of action to appropriately address the incident. The Director of Information Systems Support designates the membership of the Incident Response Team. Normally, membership includes appropriate individuals from Information Services and offices with primary responsibility for the compromised data.

It is the responsibility of the Incident Response Team to assess the actual or potential damage to UA Cossatot caused by the Confidential Data Security Incident, and to develop and execute a plan to mitigate that damage. Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

The Incident Response Team reviews, assesses, and responds to the incident for which it was formed according to the following factors, in decreasing order of priority:

- Safety - If the system involved in the incident affects human life or safety, responding in an appropriate, rapid fashion is the most important priority.
- Urgent concerns - Departments and offices may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Appropriate Information Services staff are available for consultation in such cases.
- Scope - Work to promptly establish the scope of the incident and to identify the extent of systems and data affected.
- Containment - After life and safety issues have been resolved, identify, and implement actions to mitigate the spread of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the network.
- Preservation of evidence - Promptly develop a plan to identify and implement steps for the preservation of evidence, consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information. Preservation of evidence should be addressed as quickly as possible to restore availability of the affected systems as soon as practicable.
- Investigation - Investigate the causes and circumstances of the incident and determine future preventative actions.
- Incident-specific risk mitigation - Identify and recommend strategies to mitigate the risk of harm arising from this incident.

- Documentation – All incidents will be documented using the Incident Response Form.

If, in the judgment of the Director of Information Systems Support, the incident might reasonably be expected to cause significant harm to the subjects of the data or to UA Cossatot, the Director of Information Systems Support may recommend to the Chancellor that a response team be established. The response team is comprised of senior-level administrators designated and recommended by the Director of Information Systems Support. The response team determines whether the UA Cossatot should make best efforts to notify individuals whose personally identifiable information might have been at risk due to the incident. In making this determination, the following factors are considered:

- Legal duty to notify
- Length of compromise
- Human involvement
- Sensitivity of compromised data
- Existence of evidence that data were compromised
- Existence of evidence that affected systems were compromised for reasons other than accessing and acquiring data
- Additional factors recommended for consideration by members of the Incident Response Team or Senior Response Team

Information Systems Support maintains a log of all confidential information Security Incidents, recording the date, type of confidential information affected, number of subjects affected (if applicable), summary of the reason for the breach, and corrective measures taken. Information Systems Support issues a report for every confidential information Security Incident describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.

D. Definitions

Confidential Information - Sensitive personally identifiable information (PII) that must be safeguarded to protect the privacy of individuals and the security and integrity of systems and to guard against fraud. This includes, but is not limited to:

- Social Security numbers
- Credit and debit card numbers
- Bank account or other financial account numbers
- FERPA protected information
- HIPAA protected information
- Passwords, passphrases, PIN numbers, security codes and access codes
- Tax returns
- Credit histories or reports
- Background check reports

Additionally, proprietary information, data, information, or intellectual property, in which the college has an exclusive legal interest or ownership right may also be considered confidential information. Examples include, but are not limited to:

- Financial information
- Business planning data
- Data, software, or other material from third parties which the college has agreed to keep confidential

Malware - Any software designed with malicious intent. Examples include, but are not limited to:

- Viruses
- Worms
- Trojan horses
- Spyware
- Ransomware

Security Incident - Any event that threatens the confidentiality, integrity, or availability of college systems, applications, data, or networks. Examples of college systems include, but are not limited to:

- Servers
- Desktop computers
- Laptop computers
- Workstations
- Mobile devices
- Network equipment

Examples of Security Incidents include, but are not limited to:

- Unauthorized access
- Intentionally targeted but unsuccessful unauthorized access
- Accidental disclosure of Confidential Data
- Infection by malware
- Denial-of-service (DoS) attack
- Theft or loss of a college system
- The theft or physical loss of computer equipment known to store SSNs
- Loss or theft of tablets, smartphones or other mobile device
- A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party
- A firewall accessed by an unauthorized entity
- A DDoS (Distributed Denial of Service) attack
- The act of violating an explicit or implied security policy

- A virus or worm uses open file shares to infect from one to hundreds of desktop computers
- An attacker runs an exploit tool to gain access to a college server's password file

Sensitive Personal Information - An individual's first name or first initial and last name combination with any one or more of the following data elements (when the name or data element is not encrypted):

- Social security number
- Driver's license or government issued identification number
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Does not include publicly available information that is lawfully made available to the general public from the Federal government or a state or a local government" (2-3).

E. Enforcement

Any behavior in violation of these Guidelines is cause for disciplinary action. Violations will be adjudicated, as appropriate by UA Cossatot. Sanctions as a result of violations of these Guidelines may result in, but are not limited to, any or all of the following:

- Attending a class or meeting on Security Incident issues, as well as successful completion of a follow up quiz;
- Loss of computing, email and/or voice mail privileges;
- UA Cossatot judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement or other appropriate sources;
- Suspension or expulsion from the college;
- Prosecution under applicable civil or criminal laws;
- Employees may be subject to disciplinary action.

F. Violations

Reports of data and systems compromises, and the exposure of personal and restricted information should be immediately reported to: diss@cccua.edu

Policy History:

May 2, 2022

PROCEDURE: NONE