UADA Policy 930.1
Division Information Technology Security:
Incident Response Policy

Purpose

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

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

Scope

This policy applies to all members of the UADA workforce:

- Employees (including faculty and staff)
- Volunteers
- Students and residents
- Extra help workers
- Contingent workers

Definitions & Terms

Data Breach - A security or privacy incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Identifiable Information (PII) or Personal Data transmitted or stored.

Escalation - Arrange additional resources to resolve or provide the status regarding an incident.

Incident Response/Incident Management - Process for detecting, reporting, assessing, responding to, dealing with, and learning from Security Incidents.

Information Security - The protection of confidentiality, integrity, and availability of information and the equipment, devices, or services containing or providing such information.

Personal Data - Any information relating, directly or indirectly, to an identified or identifiable data subject or individual, where such information is protected under applicable data protection or privacy law.

Personal Identifiable Information (PII) - Any information that (a) can be used to identify the PII principal or individual to whom such information relates, or (b), might be directly or indirectly linked to a PII principal or individual.

Privacy Event - A situation where PII or Personal Data is possibly processed in violation of one or more relevant privacy principles under UADA's internal privacy policies or procedures.

Privacy Incident - A situation where PII or Personal Data is processed in violation of one or more relevant privacy principles under UADA's internal privacy policies or procedures.

Security Event - An identified occurrence of a system, service, or network state indicating a possible breach of information security policy, potential exploitation of a Security Vulnerability or Security Weakness, or a previously unknown situation can be security-relevant.

Security Incident - A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.

Incident Response Team (IRT) - A predefined group of individuals responsible for responding to an incident, managed by Information Technology. During an incident, the IRT is responsible for the communication and coordination of other internal and external groups.

Security Vulnerability - A weakness of an existing asset or control that can be exploited by one or more threats.

Security Weakness - A weakness that results from the lack of an existing, necessary control.

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 the UADA mission, regardless of the ownership, location, or format of the information.
- Information systems used in the pursuit of the UADA 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 or privacy events and incidents is always in force; whether the organization is open or closed, regardless of the time of day. Faculty, staff, students, visitors, and contractors must immediately report the following information security or privacy events and incidents to the UADA Office of Information Technology (OIT) at abuse@uada.edu.

- All suspected information security/privacy events or incidents impacting the confidentiality, integrity, or availability of organization data.
- Suspected or actual security breaches of restricted information as defined in the Data Lifecycle – whether in printed, verbal or electronic form – or information systems used in the pursuit of the organization'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 organization'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 organization's mission.

UADA Office of Information Technology (OIT) will:

- Isolate from the UADA 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 UADA Legal Counsel in the event of a suspected security event or incident impacting the confidentiality, integrity, or availability of organization data, entities affiliated with the organization, or using organization 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 organization units including applicable compliance offices and officers as necessary and appropriate.
- Immediately report and coordinate with the UADA Legal Counsel regarding privacy breach response services to maximize efficiency and utility of response to significant incidents.
- Assess information security/privacy events and incidents according to the Incident Response Procedure.
- Immediately report incidents that involve personal safety to the relevant local police departments.
- Immediately report incidents that involve criminal activities to the UADA Legal Counsel so that they can contact the relevant local police departments.
- Report incidents involving regulatory matters or restricted data to the appropriate organizational 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 Associate Vice President for Finance and Administration (AVPFA) in collaboration with key organization stakeholders to issue an all-clear and return of affected resources to normal operation.

Incident Response Team (IRT)

The IRT refers to members of OIT 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 IRT will be responsible for the initial response, mitigation support, and (where appropriate) escalation of information security incidents. The primary roles and responsibilities of the IRT 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 organization 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, IRT will notify and escalate information pertaining to the incident. IRT will collaborate with other teams and members of the organization community for incident mitigation and resolution.

Members of the IRT

- UADA Chief Information Officer
- CES Director of Information Technology (DIT) (IRT Primary Lead)
- AES Director of Information Technology (DIT) (IRT Primary Lead)
- CES Data Protection Officer (DPO)
- AES Data Protection Officer (DPO)
- Information owner
- Vice President for Agriculture, Senior Associate VP's - AES and CES
- Office of Legal Counsel (OLC)
- Human Resources
- End-User Support
- Technical Services Staff (Assigned)
- Building and/or facilities management staff
- Other personnel involved in the security or privacy incident or needed for resolution
- Contractors (as necessary)
- Chief Communication Officer

Incident Response

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

- Detection – identification of a security or privacy event that may result from potential exploitation of a security vulnerability or a security weakness, resulting from an innocent error.
- Analysis – determining whether a security or privacy event is an actual security or privacy incident.
- Containment – attempts to limit the impact of a security or privacy incident before an eradication and recovery event.
- 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.
- Post-Incident Activities – provide a final report on the incident, which will be delivered to management.

Refer to the Information Security Incident Response Procedure for more details and instructions on the lifecycle stages of the incident response process.

Related Links

Data Lifecycle Policy
Incident Response Procedure
Incident Escalation Guideline
Breaches of Privacy & Security of Protected Health Information (PHI) Policy and Procedures (UADA)