INCIDENT RESPONSE POLICY & PROCESS

PURPOSE OF INCIDENT RESPONSE

This policy's objective is to ensure a consistent and practical approach to the management of Security and Privacy Incidents, including the identification and communication of Security and Privacy Events and Security Weaknesses. Furthermore, this document defines the policy for addressing Security and Privacy Incidents through appropriate Incident Response.

TERMS & DEFINITIONS

Term/Acronym	Definition
Data Breach	A Security or Privacy Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PII or Personal Data transmitted, stored
Data Controller	The person or organization that determines the purpose and means of the processing of Personal Data.
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.
Personnel	UAPB employees (full time and extra help)
Privacy Event	A situation where PII or Personal Data is possibly processed in violation of one or more relevant privacy principles under UAPB'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 UAPB'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 the Technical Services. 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.

INCIDENT RESPONSE POLICY

The Incident Response policy is as follows:

- Ensure a quick, effective, and orderly response to Security Incidents with assigned responsibilities and procedures.
- Ensure that those responsible for Security Incident management understand the university's priorities for handling Security Incidents.
- Security Events reported through the appropriate management channels as quickly as possible.
- Personnel and contractors using the organization's information systems and services must note and report any observed or suspected Security Weakness or Vulnerability in systems or services.
- Security and Privacy Events should be evaluated, and then decided if they are to be classified as Security or Privacy Incidents.
- Security and Privacy Incidents should be responded to following documented Incident Response procedures.
- Knowledge gained from analyzing and resolving Security and Privacy Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures will be used to define and apply for identifying, collecting, acquiring, and preserving information, serving as evidence.
- Execution of the incident response policy and expectations
- Reporting of Security and Privacy Incidents
- Contact (s) for reporting incidents will be the communication team
- The communication team consists of assigned UAPB Technical Services Personnel, Vice-Chancellor for Finance and Administration, Chancellor, and other UAPB Personnel.
- In the event of a Security or Privacy Incident, Data Controllers, university officials and other necessary parties should be notified in a reasonable timeframe and comply with regulatory and other applicable requirements and guidance.
- No interference of an investigation into security or privacy events or incidents be unreasonably blocked.
    - Any impediment of an investigation into a security or privacy event or incident must immediately be reported to university leadership for resolution.
    - Obstruction of an investigation may result in disciplinary action, up to and including termination.

INCIDENT RESPONSE PROCEDURES

The purpose of this document is to define the Incident Response procedures followed by UAPB in the event of a Security and Privacy Incident. A step-by-step guide to re-establish normal operations from the original Protection and Privacy Case and Incident Identification.

Both Security and Privacy Incidents are detected, analyzed, contained, and eradicated to avoid any other Security and Privacy Incidents. Where required or appropriate, such notice shall be given to the workers and/or involved parties and law enforcement authorities, if required.

TERMS & DEFINITIONS

Term/Acronym	Definition
Abnormal Activities	Unsuccessful attacks that appear particularly significant based on UAPB understanding of the risks it faces.
Data Breach	A Security or Privacy Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PII or Personal Data transmitted, stored or otherwise processed.
Data Controller	The person or organization that determines the purpose and means of the processing of Personal Data.
Escalation	Arrange additional resources to resolve or provide the status regarding an incident.
GCO	University of Arkansas System's General Counsel's Office
Incident Record	Generated at the time a Security or Privacy Incident is initially recognized. Contains all relevant information about the Security or Privacy Incident.
Incident Response/Incident Management	Process for detecting, reporting, assessing, responding to, dealing with, and learning from incidents.
Information Security	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) is or might be directly or indirectly linked to a PII principal or individual.
Personnel	UAPB employees (full time and extra help).
Privacy Event	A situation where PII or Personal Data is potentially processed in violation of one or more relevant privacy principles under iCIMS' 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 iCIMS' internal privacy policies or procedures.
Security or Privacy 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 or Privacy Incident	A single or series of unwanted or unexpected Security or Privacy Events that compromise business operations with an impact on Information Security.
Security or Privacy Incident Response Team (IRT)	A predefined group of individuals needed and responsible for responding to an incident, managed by the Information Security Department. During an incident, the IRT is responsible for the communication and coordination of other internal and external groups.
Sensitive Personal Information (SPI)	A form of Personal Data and means any information revealing a Data Subject's genetic or biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, and lifestyle, or criminal convictions or offenses
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.
Subscriber Data	Refer to UAPB Subscription Agreement(s).

SCOPE

This procedure covers the Incident Response process for all identified Security and Privacy Incidents. The content will cover the following actions:

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

The Incident Response process is considered complete once information confidentiality, integrity, and/or availability are restored to normal, and verification has occurred.

Roles and Responsibilities

Individuals needed and responsible for responding to a Security or Privacy Incident make up the IRT. Core members will include the following:

- Director of Technical Services (IRT Primary Lead)
- Data Protection Officer (DPO)
- Information owner
- Senior Leadership
- General Counsel's Office (GCO)
- 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)
- Communications Resources

Detection Phase

In the detection phase, the IRT, or an internal or external entity, identifies a Security or Privacy Event that may result from potential exploitation of a Security Vulnerability or a Security Weakness, resulting from an innocent error.

Immediately upon observation or notice of any suspected Security or Privacy Event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department at the following address:

Email: tottenw@uapb.edu

The detection of a Security or Privacy Incident can be made known in several ways, including the following.:

- Observation of suspicious behavior or unusual occurrences;
- Lapses in physical or procedural security;
- Information coming into the possession of unauthorized Personnel or Third Parties;
- Information is inappropriately exposed on a publicly facing website.

To assess whether a Security or Privacy Event must be reported, personnel shall consider whether there are indications that:

- Information was used by unauthorized Personnel or Third Parties;
- The information has been downloaded or copied inappropriately from UAPB's computer systems or equipment;

- Equipment or devices containing information have been lost or stolen;
- Equipment or devices containing information have been subject to unauthorized activity (e.g., hacking, malware).
- Personal Data has been inappropriately disclosed, accessed, or transferred.

In addition, protection or privacy incident notification shall be considered as the following cases:

- Ineffective security controls;
- Breach of information integrity, confidentiality, or availability expectations;
- Human errors (innocent or otherwise);
- Non–compliance with policies or standards;
- Breaches of physical security arrangements;
- Uncontrolled systems changes;
- Malfunctions of software or hardware;
- Access violations.

Even if personnel are not sure whether a Security or Privacy Event is an actual Security or Privacy Incident, they are still required to report it as provided herein. It is better to be cautious than to be compromised.

The IRT will usually require the reporter to supply further information, which will depend upon the nature of the Security or Privacy Event. However, the following details usually shall be provided:

- Contact name and information of the person reporting the Security or Privacy Event;
- Date and time the Security or Privacy Event occurred or was noticed;
- Type and circumstances of the Security or Privacy Event;
- The type of data, information, or equipment involved;
- Location of the Security or Privacy Event, data or equipment affected;
- Whether the Security or Privacy Event puts any person or other data at risk; and
- Any associated ticket numbers, emails, or log entries related to the Security or Privacy Event.

IRT Primary Lead will ensure that the IRT is promptly engaged once such notice is received. The following steps will also be taken:

The IRT, under the leadership of the IRT Primary Lead, shall use reasonable efforts to analyze the matter within four (4) hours of notice and decide whether to proceed with the Analysis Phase of the Incident Response Procedures.

- Immediately, the decision to initiate the Analysis Phase must be taken so that personnel can make an initial determination as to the urgency and seriousness of the situation.
- Upon deciding to begin the Analysis Phase, if the IRT suspects that the Security or Privacy Event may damage the reputation of UAPB or legal liability, the GCO shall initiate a legal assessment of actual or potential legal issues.

Analysis Phase

The initial response to the detection of a Security or Privacy Event is typically the Analysis Phase. *In this phase, the IRT determines whether a Security or Privacy Event is an actual Security or Privacy Incident.* The following considerations apply to determine if a Security or Privacy Event is a Security or Privacy Incident:

1. Leverage diagnostic data to analyze the Security or Privacy Event using tools directly on the operating system or application. This may include, but not be limited to:

    (i) Taking screenshots, memory dumps, consult logs and network traces;

(ii) Performing analysis on the information being collected;

(iii) Analyzing the precursors and indications;

(iv) Looking for correlating information; and

(v) Performing research (e.g., search engines, knowledgebase).

2. Identify whether the Security or Privacy Event resulted from an innocent error or a potential attacker's actions. If the latter, effort shall be made to identify who the potential attacker maybe, by:

(i) Validating the attacker's IP address;

(ii) Researching the attacker through search engines;

(iii) Using incident databases;

(iv) Monitoring attacker communication channels, if possible; and

(v) In unique cases, and with the approval of legal counsel, potentially scanning the attacker's system.

Assume the IRT has determined that a Security or Privacy Event has triggered a Security or Privacy Incident. In this situation, the appropriate IRT team members will be engaged appropriately, and the IRT will begin to record the investigation and collect evidence. The type of Security or Privacy Incident is based on the nature of the event. Example types are listed as follows:

- Data exposure.
- Unauthorized access/Inappropriate role-based access.
- Distributed Denial of Service/ Denial of Service (DDoS/DoS).
- Malicious code.
- Improper usage.
- Scans/Probes/Attempted access.

If it is determined that a Security or Privacy Incident has not been triggered, additional activities noted under "Post-Incident Activities" may be initiated under the IRT direction.

The Security or Privacy Incident's potential impact on UAPB and/or its Subscribers shall be evaluated, and the IRT shall assign an initial severity classification of a low, medium, high or critical to the Security or Privacy Incident. To analyze the situation, scope, and impact, the IRT shall:

- Define and confirm the severity level and potential impact of the Security or Privacy Incident.
- Identify which resources have been affected and forecast which resources will be affected.
- Estimate the current and potential effect of the Security or Privacy Incident.

The IRT shall attempt to determine the scope of the Security or Privacy Incident and verify if the Security or Privacy Incident is still ongoing. Scoping the Security or Privacy Incident may include collecting forensic data from suspect systems or gathering evidence that will support the investigation. It may also include identifying any potential data theft or destruction. New investigative leads can be generated as the data collected is analyzed. If the Security or Privacy Incident involves malware, the IRT shall analyze it to determine its capabilities and potential impact on the environment. Based on the evidence reviewed, the IRT will determine if the Security or Privacy Incident requires reclassification as to its severity or cause (e.g., if it was initially thought to be a malicious actor's action but turned out to be an innocent error or vice versa).

As indicated above, a Security or Privacy Incident may require evidence to be collected. The gathering of such evidence shall be done with due diligence, and the following procedures shall apply:

1. Gathering and handling of evidence (forensics) shall include:

(i) Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer);

(ii) Name, title, and phone number of everyone who collected or handled the evidence during the investigation;

(iii) Time and date (including time zone) of each occurrence of evidence handling;

(iv) Locations where the evidence is stored, and conditions of storage (e.g., locked spaces, closely monitor or observe areas); and

(v) Reasonable efforts to create backups of the affected system(s) allow one to be used as evidence, and one is to be used as a source of additional backups.

2. To ensure that evidence is not destroyed or removed, where any Personnel is suspected of being responsible for a Security or Privacy Incident, UAPB shall, consistent with its procedures, use reasonable efforts to place monitoring and forensics agents and/or confiscate all computer/electronic assets that have been assigned to him or her.

    (i) This task may be done secretly and shall be completed as quickly and in as non-intrusive a manner as possible.

    (ii) The IRT shall consider restricting access to the computers and attached peripherals (including remote access, secure remote system access, etc.), pending the outcome of its examination.

3. Where applicable, and depending upon the seriousness of the Security or Privacy Incident, items, and areas that shall be secured and preserved in an "as was" condition include:

    (i) Work areas (including wastebaskets);

    (ii) Computer hardware (keyboard, mouse, monitor, CPU, etc.);

    (iii) Software;

    (iv) Storage media (disks, tapes, removable disk drives, CD ROMs, etc.);

    (v) Documentation (manuals, printouts, notebooks, notepads);

    (vi) Additional components as deemed relevant (printer, cables, etc.);

    (vii) In cases of damage, the computer system and its surrounding area, as well as other data storage devices, shall be preserved for the potential collection of evidence (e.g., fingerprinting);

    (viii) If the computer is "Off," it shall not be turned "On." For a stand-alone computer system, if the computer is "On," the Information Security and IT Departments will be contacted.

4. It is vital to establish who was using the computer system at the time of the Security or Privacy Incident and/or in the immediate area. The IRT shall obtain copies of relevant records (e.g., access logs, swipe card logs, closed-circuit television ("CCTV") recordings) as part of the investigation.

5. Based on the severity level and the Security or Privacy Incident categorization, the proper team or personnel shall be notified and contacted by the IRT.

6. Until the IRT, with UAPB senior management's approval, makes the Security or Privacy Incident known to other personnel, the preceding activities shall be kept confidential to the extent possible.

If it is determined that a Security or Privacy Incident has occurred and may significantly impact UAPB or its Subscribers. In that case, the IRT shall determine whether additional resources are required to

investigate and respond to the Security or Privacy Incident. The extent of the other resources will vary depending on the nature and significance of the Security or Privacy Incident.

Abnormal Activities Notification:

The IRT recognizes that many attempts to gain unauthorized access to, disrupt, or misuse information systems and the information stored. UAPB's information security program will thwart many of these attempts. In general, the IRT will not report unsuccessful attacks on customers. For example, the IRT would generally *not* be required to report to a Data Controller or customer if it makes a good faith judgment that the unsuccessful attack was of a routine nature.

However, the IRT will take reasonable steps to notify customers or Data Controllers of any identified Abnormal Activities. For example, in making a judgment about whether an unsuccessful attack shall be reported, UAPB might consider whether handling the attack required measures or resources well beyond those ordinarily used, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps. In cases of identified Abnormal Activities, the Data Controller or customer would be notified by means agreed upon by UAPB and the Data Controller or customer within twenty-four (24) hours upon UAPB becoming aware of the Abnormal Activity.

Data Breach Notification:

If it is determined during the analysis phase, a Security or Privacy Incident has occurred that constitutes a Data Breach, with notification obligations based on applicable legislation, regulation, or similar jurisdictional requirements. In that case, notification of such Data Breach shall be handled by the IRT and provided to the impacted Data Controller by email, telephone, or other appropriate means agreed upon by UAPB and the Data Controller, within twenty-four (24) hours upon UAPB the IRT becoming aware of the Data Breach. Additional activities noted under 'Post-Incident Activities' may also be initiated under the direction of the IRT.

Containment Phase

The Containment Phase mitigates the root cause of the Security or Privacy Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Security or Privacy Incident before an eradication and recovery event. During this phase, the IRT may implement controls, as necessary, to limit the damage from a Security or Privacy Incident. If a Security or Privacy Incident is determined to be caused by innocent error, the eradication phase may not be needed. For example, after reviewing any information that is collected investigating the Security or Privacy Incident, the IRT may:

1. Secure the physical and network perimeter.
    i. For example, shutting down a system, disconnecting it from the network, and/or disabling certain functions or services.
2. Connect through a trusted connection and retrieve any volatile data from the affected system.
3. Determine the relative integrity and the appropriateness of backing the system up.
4. If appropriate, back up the impacted system.
5. Change the password(s) to the affected system(s). Personnel, as appropriate, shall be notified of the password change.
6. Determine whether it is safe to continue operations with the affected system(s).
    i. If it is safe, allow the system to continue to function, in which case the IRT will:
        a. Update the Incident Record accordingly; and
        b. Move to the Recovery Phase.

ii. If it is not safe to allow the system to continue operations, the IRT will discontinue the system(s) process and move to the Eradication Phase.

iii. The IRT may permit continued operation of the system under close supervision and monitoring if:

1. Such activity will assist in identifying individuals responsible for the Security or Privacy Incident;
2. The system can generally run without risk of disruption, compromise of data, or severe damage; and
3. The consensus reached within the IRT before taking the supervision and monitoring approach.

7. The final status of this stage shall be appropriately documented in the Incident Record.
8. The IRT shall apprise senior management of the progress, as appropriate.

During the Analysis and Containment Phases, the IRT shall keep notes and use the appropriate chain of custody procedures to ensure that the evidence gathered during the Security or Privacy Incident can be used successfully during prosecution, if applicable.

Recovery Phase

The Recovery Phase represents the IRT's effort to restore the affected system(s) to operation after the problems that gave rise to the Security or Privacy Incident and the consequences of the Security, or Privacy Incident have been corrected. Recovery events can be problematic depending on the Security or Privacy Incident type and require full project management plans to be effective.
Although the specific actions taken during the Recovery Phase can vary depending on the identified Security or Privacy Incident, the standard process to accomplish this shall be as follows:

1. Execution of the following actions, as appropriate:
    - Installing patches
    - Rebuilding systems
    - Changing passwords
    - Restoring systems from clean backups
    - Replacing affected files with clean versions
2. The determination whether the affected system(s) has been changed in any way:
    a. If the system(s) has changed, the system is restored to its proper, intended functioning ("last known good").
        i. Once restored, the system functions are validated to verify that the system/process functions as intended. This may require the involvement of the business unit that owns the affected system(s).
        ii. If the operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline), it shall be restored and validated, and the system(s) shall be monitored for proper behavior.
    b. If the system(s) has not been changed in any way but taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
3. Implementation of additional monitoring and alerting may be done to identify similar activities.
4. Update the Incident Record with any details determined to be relevant during this phase.

5. Apprise senior management of progress, as appropriate.

Post-Incident Activities

In addition to the Data Breach and Abnormal Activities notification requirements identified in the analysis phase above, and after verification of a successful containment and any necessary eradication, the IRT shall take the following post-incident activities, as may be required:

II. Communications

A. Notification

After consulting with senior management, when warranted or required by judicial action, applicable law, regulation, or like legal decisions requirement, UAPB shall use reasonable efforts to provide notice to personnel and/or affected parties about a Security or Privacy Incident or Data Breach involving the Sensitive and/or Confidential information of such stakeholders. For example:

1. Where it is determined, or the IRT and senior management reasonably believe, that there has been unauthorized access to or release of unencrypted data;
2. Where a Security or Privacy Incident has compromised the security, confidentiality, or integrity of Confidential Information.

Upon deciding to notify and before notifying law enforcement or other governmental authority (if necessary), the IRT (in consultation with senior leadership) shall use reasonable efforts to provide notice and disclosure to personnel and/or affected parties within twenty-four (24) hours and, subject to applicable law, regulation, or like jurisdictional requirement before notification of law enforcement personnel. Delayed notification may occur when required or authorized by applicable law, regulation, or court of competent jurisdiction. For example, notification disclosure might be delayed if notice would impede a criminal investigation or if time is required to restore reasonable integrity to UAPB's information systems.

Notification of a Data Breach or Abnormal Activities will occur within twenty-four (24) hours of identification, as noted in the 'Abnormal Activities Notification' and 'Data Breach Notification' sections above in alignment with regulatory requirements.

If appropriate, the IRT may:

3. Prepare a general notice and arrange for providing the information to personnel and/or affected parties;
4. Prepare a FAQ based on the notice and arrange to have it posted to the UAPB website after the message has been sent;
5. Identify a point a contact for personnel and/or affected parties to contact if further information is needed; and
6. Establish a toll-free number for use by stakeholders.

UAPB's objective is to provide notice in a manner designed to ensure that Personnel and/or affected parties can reasonably be expected to receive the disclosure.

The notification's form and content may either be by letter (first class mail) or by email sent to an address where Personnel and/or affected parties can reasonably be expected to receive the disclosure or other similar means.

The notification, in clear and understandable language, may contain the following elements:

1. A description of the Security or Privacy Incident, Privacy Incident or Data Breach that includes as much detail as is appropriate under the circumstances;
2. The type of information that was impacted (e.g., number of individuals or records concerned) subject to unauthorized access and any foreseeable, likely consequences;
3. Measures were taken by UAPB to protect the Information of Personnel and/or affected parties from further impact;
4. A contact name and a toll-free number that personnel and/or affected parties may use to obtain further information;
5. A reference to the page on the UAPB website where updates may be attained;
6. A reminder to guard against possible identity theft by being vigilant concerning banking or credit activity for twelve to twenty-four months;
7. Contact information for national credit reporting agencies;
8. Other elements may be required by applicable law or whose inclusion the IRT may otherwise consider appropriate under the circumstances.

B. Cooperation with External Investigators

Suppose the IRT considers it appropriate to inform law enforcement authorities or retain forensic investigators or other external advisors. In that case, the following information shall be collected to provide to such officers or investigators:

1. To the extent known, details of the:
    a. Security or Privacy Incident (date, time, place, duration, etc.);
    b. Person(s) under suspicion (name, date of birth,address, occupation/position, employment contracts, etc.);
    c. Computer and network log files about the Security or Privacy Incident(s);
    d. "Ownership" details of any Information that is allegedly stolen, altered, or destroyed;
    e. The access rights to the computer system involved of the person(s) under investigation;
    f. Information obtained from access control systems (e.g., computer logs, CCTV, swipe card systems, attendance logs, etc.); and

g. The IT department took any action about the computer systems concerned, including the date and time.

2. A copy of applicable UAPB Data Privacy and Security Statement ("Statement") in force at the time of the incident (if applicable); and

3. Any other documentation or evidence relevant to the internal investigation of the Security or Privacy Incident.

C. Information Sharing and Media Relations

Security or Privacy Incident-specific information (e.g., dates, accounts, programs, systems) must not be provided to any unknown individuals making such requests by telephone or email. Any release of Security or Privacy Incident-specific information shall only be to individuals previously identified by the IRT. All requests for information from unknown individuals shall be forwarded to the IRT. If there is any doubt about whether data can be released, contact the GCO.

The GCO shall only make contact with law enforcement authorities in consultations with the IRT and senior management.

In the event of a Security or Privacy Incident, where members of the media make inquiries, personnel must be aware that all requests for the release of information, press releases, or media interviews must be submitted to the GCO.

The GCO, in consultation with the IRT and senior management, shall determine whether it is appropriate to issue a media statement, hold a press briefing, or schedule interviews.

If Sensitive and/or Confidential Information has been compromised and a significant number of individuals, as identified by the IRT, are affected and/or suspected of being involved, the GCO, subject to applicable law, shall use reasonable efforts to contact appropriate consumer reporting agencies before sending notices to the affected person and/or affected parties.

Certain jurisdictions where UAPB does business or where UAPB's stakeholders reside mandate additional disclosure or notification obligations. Additionally, advice from both inside and outside counsel is required before communication occurs with credit reporting agencies.

D. External Incident Communications

After a Security or Privacy Incident, information may be required to be shared with outside parties, following emergency response procedures as necessary, including:

- Law enforcement/incident reporting organizations
- Affected external parties
- The media
- Other outside parties

1. UAPB will seek to ensure its obligations are fulfilled by quickly and professionally taking control of communication early during significant events. Accordingly, the IRT will:
    - Designate a credible, trained, informed spokesperson to address the media;
    - Determine appropriate clearance and approval processes for the media;
    - Ensure the organization is accessible by media, so they do not resort to other (less credible) sources for information;
    - Emphasize steps being taken to address the Security or Privacy Incident;
    - Tell the story quickly, openly, and honestly to counter falsehoods, rumors, or undue suspicion.
2. When publicly disclosing information of a Security or Privacy Incident, consider the following:
    - Was Personal Data compromised?
    - Was Subscriber Data compromised?
    - Did the Security or Privacy Incident invoke legal and/or contractual obligations?
    - What is the organization's strategy moving forward?

E. Internal Incident Communications

1. Where warranted, the IRT will ensure that open communication is maintained within the organization to ensure relevant parties are informed of facts, reminded of responsibilities, and capable of dismissing rumors and speculation.
2. Aggregate documentation from post-mortem/follow-up reviews into the Security or Privacy Incident record and create a formal report of the Security or Privacy Incident to share with senior management, as necessary.

III. Follow Up

The Follow-up Phase represents the Security or Privacy Incident review to look for "lessons learned" and to determine whether the process that was followed could have been improved in any way. Security or Privacy Events and Security or Privacy Incidents shall be reviewed after identification resolution to determine if improvements can be made to the response.

The IRT will meet to review the Security or Privacy Event or Security or Privacy Incident record created, as necessary, and perform the following:

i) Determine the root cause of the Security or Privacy Incident and what must be done to ensure that the root cause has been addressed

ii) Create a "lessons learned" document and include it with the Incident Record.

iii) Evaluate the cost and impact of the Security or Privacy Event or Incident to the organization using applicable documents and any other resources.

iv) Determine what could be improved.

v) Communicate these findings to senior management for approval, as necessary, and implement any recommendations made post- review of the Security or Privacy Event or Incident.

vi) Carry out recommendations approved by senior management while ensuring that sufficient time and resources are committed to this activity.

vii) Close the Security or Privacy Event or Incident.

A. Retention and Review of Security or Privacy Incident Record & Documentation

It shall be the IRT's responsibility to investigate the Security or Privacy Incident and establish an incident record. The incident record shall be verified during the follow-up process to ensure that it documents:

1. Relevant factual information or evidence;
2. Consultations with personnel and external advisors; and
3. Findings resulting from the collection of factual information or evidence obtained.

The rationale for creating an incident record is that law enforcement authorities may be informed of Security or Privacy Incidents, or UAPB may take legal action if individuals causing a Security or Privacy Incident can be identified. The consequences of each Security or Privacy Incident are not always evident in the beginning, or even during, the Security or Privacy Incident course. For that reason, information must be documented, and associated information system events logged.

The incident record may be in written or electronic form. If it is an electronic form, appropriate protections must be applied to guard against the incident record's alteration or deletion.

The information to be reported will vary according to the specific circumstances and availability of the information, but may include:

1. Dates and times when incident-related events occurred;
2. Dates and times when incident-related events were discovered;
3. Dates and times of incident-related conference calls;
4. A description of the Security or Privacy Incident, including the systems, programs, networks or types of information that may have been compromised;
5. The root cause(s) of the Security or Privacy Incident(s), if known, and how they have been addressed;

6. An estimate of the amount of time spent by personnel working to remediate incident-related tasks;
7. The amount of time spent by Third Parties working on incident-related tasks, including advice from outside counsel;
8. The names and contact information of all individuals providing information in connection with the investigation;
9. Measures engaged to prevent future Security or Privacy Incidents, taking into consideration root causes, along with any remediation costs incurred by UAPB; and
10. If applicable, the date and time of law enforcement involvement.

All personnel has an affirmative obligation to use reasonable efforts to respond to all inquiries for information and cooperate in all investigations. Obstruction of Security or Privacy Event and Security or Privacy Incident investigations may lead to disciplinary actions, up to and including termination.

Review of the incident record and documentation shall include the following:

1. Review tracked documents of the Security or Privacy Incident to evaluate the following:
    - The causes of the nonconformity;
    - Whether similar nonconformities exist or could potentially occur;
    - The effectiveness of the corrective action taken; and
    - The effectiveness of the Incident Response process.
2. Learn from Security or Privacy Incidents and improve the response process. Security or Privacy Incidents must be recorded, and a post-incident review conducted. Identify the impact of Security or Privacy Incidents and outline pain points for future security investments. The following details must be retained:
    - Types of Security or Privacy Incidents
    - Volumes of Security or Privacy Incidents and malfunctions
    - Costs incurred during the Security or Privacy Incidents, where possible.

B. Retention and Review of Data Breaches Record & Documentation

It shall be the UAPB Privacy's responsibility, under IRT oversight, to notify impacted parties about a Data Breach and establish a record of the Data Breach with sufficient information to provide a report for regulatory and/or forensic purposes. The Data Breach record shall be verified during the follow-up process to ensure that it documents:

- A description of the Security or Privacy Incident and/or Privacy Incident;
- The time period;
- The consequences of the Security or Privacy Incident;
- The name of the reporter;
- To whom the Security or Privacy Incident was reported;
- Document the steps to resolve the Security or Privacy Incident (including the person in charge and the data recovered); and
- The fact that the Security or Privacy Incident resulted in unavailability, loss, disclosure, or alteration of Personal Data and/or PII.

C. Periodic Evaluation of the Program

The processes surrounding incident response shall be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to Security or Privacy Events and Incidents and the training of the general population regarding the organization's expectation of them, relative to security responsibilities.

Security or Privacy Events and Incidents shall be documented for tracking, analysis, and reporting purposes. The following metrics shall be considered to assess the overall Security or Privacy Incident management program:

- The overall reduction in time spent responding to Security or Privacy Incidents
- Reduction of the impact of specific Security or Privacy Incidents.
- Overall reduction of the occurrence of Security or Privacy Incidents.
- Period in-between to analysis
- Period in-between to resolution

REFERENCES AND RELATED DOCUMENTS

Researched on the internet and reviewed various policies online.

POLICY INFORMATION

Continuous improvement. This document's content is subject to regular review based on UAPB Technical Services staff and the campus community's input. Recommendations for development should be submitted to the Director of Technical Services.