
# Incident and Breach Response Policy

## Florida International University

FIU FLORIDA INTERNATIONAL UNIVERSITY

# Table of Contents

## The purpose of this document

This document is intended to set institutional standards for an incident and breach response plan ("Plan") that is designed to support, and should be read in conjunction with FIU's Policies on Information Security and Acceptable Use.

The purpose of setting institutional standards is to ensure that certain types of incidents, including breaches of privacy are properly documented, communicated and elevated by the department, division or unit that is responsible for applying policies and procedures in order to protect the confidentiality of Private information on FIU Systems. The use of this plan is not necessarily for every privacy and data incident, because many incidents are small and routine, requiring only a single responder.

Each department, division or unit shall identify a designee ("Responding Party"), responsible for reporting Privacy Breaches (see the definition below) to FIU's Incident Response Team (as defined in appendix A, below). Responding Parties are expected to seek guidance in accordance with this document, and to fully cooperate with FIU's Incident Response Team (defined in appendix A, below).

If there are inconsistencies between this Policy and other FIU policies, such discrepancies should be reported to the Director of IT Security and the University Privacy Officer.

## The Primary Audience

The primary audience for this Plan includes the Responding Party; however, many FIU faculty and employees should find this document useful, including Business Unit Leaders, Information Security Officers and Privacy Officers responsible for providing direct support to their Unit or Division.

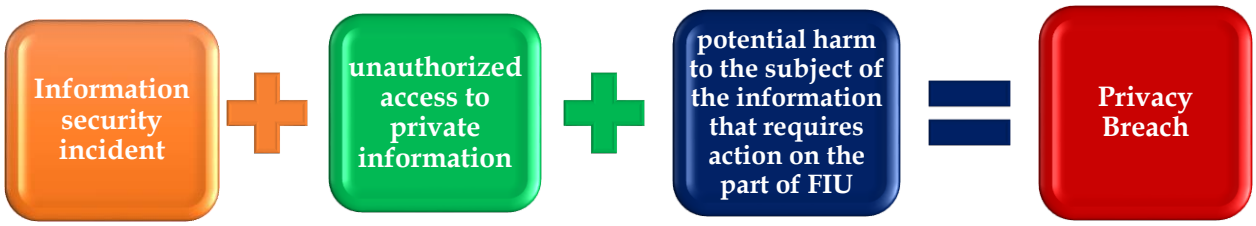
## When and how this Plan should be used

This Plan should be used by a Responding Party whenever he or she develops a reasonable basis to anticipate that an incident or a series of incidents may have resulted in a Privacy Breach. **The Incident Response Team should be notified as soon as possible, but no more than 24 hours after discovery**. In the event that the Responding Party needs to address immediate concerns related to the Privacy Breach, it shall be within the discretion of the Responding Party to modify the timelines in order to protect the individuals impacted by the Privacy Breach; however, there is no Privacy Breach scenario that bypasses the requirement to notify the Incident Response Team. Florida has a 30-day notification requirement, so timely engagement of the Incident Response Team is critical. Further, communications should be limited to the Incident Response Team and others on a need to know basis only with careful consideration as to what should be communicated verbally or documented in writing.

## The difference between an Information Incident and a Privacy Breach

**Information Incidents** are a single or series of unwanted or unexpected events that threaten privacy or information security. They can be accidental or deliberate and include access, theft, loss, alteration or destruction; however, it is important to remember that not all incidents are privacy breaches.

**Privacy Breach** occurs when there is an actual disclosure (access or use) of personal information, whether accidental or deliberate, that is not authorized under law, regulation, contract or policy. Final determination must be made by University Counsel.




**Private Information -** Personal information about an individual for which the individual can reasonably expect will not be made available to the public. This type of information includes personally identifiable information (a category of private information regulated by federal and state laws), as well as other non-public private information that would adversely impact an individual if inappropriately used or disclosed. Examples of private information includes, but is not limited to the following:

Medical Information (Protected Health Information (PHI) - See HIPAA policy)

Private information of an FIU employee, contractor, donor or volunteer (Personal Information)

Non-directory Education Records (Personally Identifiable Information (PII) - See FERPA policy)

Financial Information (Account & Credit Card Information and PII - See GLBA and PCI policy)

**Public Records Law -** Please note that Florida's public records law requires that all information received in connection with state business, be made available to anyone for inspection and copying upon request, unless the information is subject to a specific statutory exemption. (See § 119.071, Fla. Stat.)

## When Notification Is Required

The impact of any incident should be analyzed by the Responding Party in collaboration with the Incident Response Team. Some breaches (after final determination by legal counsel) may require notification to individuals and/or others based on contractual commitments or applicable laws and regulations. In the event that a regulatory agency must be notified about a breach, the Responding Party will submit any proposed notification to the Office of the General Counsel for approval prior to delivering notification to any individual or regulatory agency.

The following is a list of the types of incidents that may require notification:

A user (faculty, staff, contractor, or third-party provider) has obtained unauthorized access to private information maintained in either paper or electronic form.

An intruder has broken into database(s) that contains private information on an individual.

Computer equipment such as a smartphone, workstation, laptop, CD-ROM, or other electronic media containing private information on an individual has been lost or stolen.

A department or unit has not properly disposed of records containing private information on an individual.

A third party service provider has experienced any of the incidents above, affecting the organization's data containing private information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the Responsible Party can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps were taken to safeguard the information pertaining to affected individuals:

The Responsible Party is able to retrieve private information on an individual that was stolen, and based on the investigation in conjunction with the IRT, reasonably concludes that retrieval took place before the information could have been accessed by another person who could misuse it.

The Responsible Party determines that private information on an individual was improperly disposed of, but can establish that the information was not accessed before it was properly destroyed.

An intruder accessed files that contain only individuals' names and addresses.

A laptop computer is lost or stolen, but the data was encrypted and could only have been accessed with a secure token or similar access controlling device.

## Incident & Breach Response Cycle

The level of support needed and provided by the Incident Response Team will vary. The following graphic and text is intended to provide a general progression of incident and breach response events.


**Stage 1**: Detect & Report –Potential first responders (e.g. Managers, Privacy, Security or IT professional) should be made aware that if they suspect an Incident involving private information, that first responder should immediately report his/her suspicions to the Responding Party designated by the Department or Division.

The Responding Party shall do the following:

- Verify that an Incident occurred.
- Determine whether the Incident involved private information.

- Consider what immediate steps should be taken to mitigate harm (e.g. remote wipe a lost or stolen device, or contact a recipient to arrange for destruction of material sent in error.
- Take the lead, and direct others to gather and preserve FIU information and records needed for General Counsel to make a final breach determination.
- Notify the Incident Response Team by contacting the FIU Security Officer and/or the Compliance/Privacy Officer within 24 hours of verifying the incident involving private information.

## Stage 2: Analyze, Contain & Validate

The Incident Response Team shall support the Responding Party by doing the following:

- Assist with developing or approve the temporary work plan
- Provide guidance on documenting repeatable processes and establishing a chain of custody for any evidence to support breach determination
- Review how the Incident involved private information
- Estimate velocity of potential impact
- Determine whether specialized resources (e.g. Forensics and Incident Response) resources are needed.
- Request breach determination from General Counsel

The Responding Party will do the following:

- Provide a frequent status updates to the Incident Response Team
- Execute the approved temporary work plan

## Stage 3: Eradicate and Enumerate

The Responding Party shall do the following:

- Remove any remaining threat (e.g. implement additional access control (firewall or local block, etc.), remote wipe, data destruction, removing viruses or other malware, etc.)
- Begin to develop a list of impacted parties and contact information for those that may need to be notified

## Stage 4: Recover and Notification

The Responding Party shall do the following:

- Assign resources to recover any lost IT, business or operational functionality
- Identify and retain internal and/or external resources to assist in providing notification as necessary, and with approval from the Incident Response Team
- Develop and execute the approved notification plan(s)
- Restore service and support the return to normal operations once the Privacy Breach has been mitigated

## Stage 5: After Action Review

The Responding Party shall do the following:

- Prepare and provide a final Incident Report to the Incident Response Team, using the basic template in appendix G.

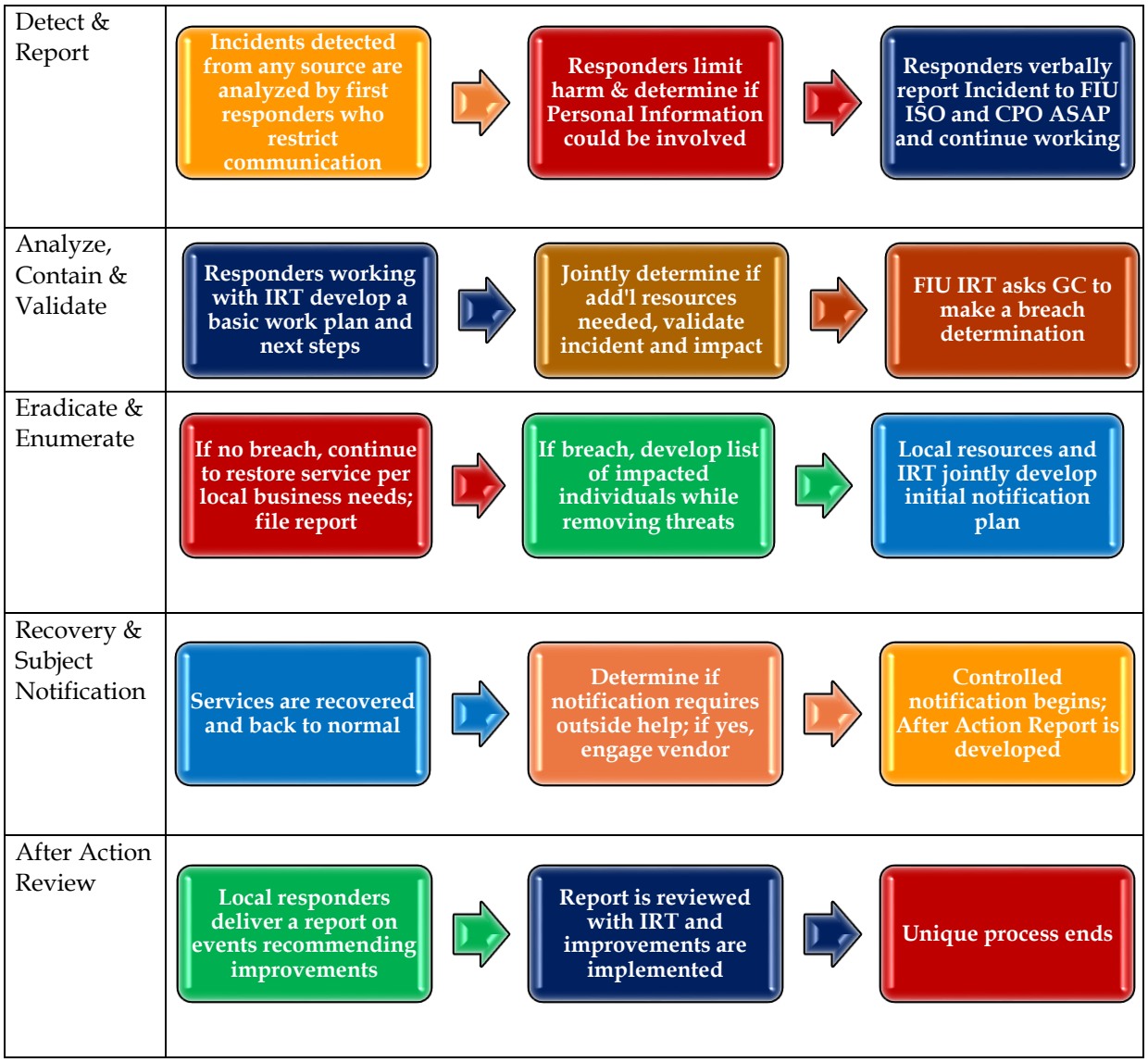
The Incident Response Team shall do the following:

- Work with the Responding Party to review the details of the Privacy Breach, and determine what improvements should be implemented.

# Appendix

## Incident & Breach Response Flow Chart at-a-glance

The chart below can be used to provide an overview on what to expect during the process. Flexibility is important since information may change or surface frequently.




### Device loss: Initial Incident & Breach Triage for user based computing endpoints (laptops, tablets, smartphones and other personal devices)

To facilitate initial intake for incidents (theft, loss, malware, hacking, etc.) involving computing endpoints (desktop, laptop, tablet, smartphone, etc.), the primary concern remains disclosure of institutional private information. Private information relating

only to the user (self, family, etc.) is a sensitive and personal user support problem, but one that can be dealt with on a case-by-case basis by unit management outside of this procedure. Identifying the likely presence of any FIU (e.g. institutional) information is key, so please perform initial triage by asking the following four questions:

Note: If a device (smartphone, etc.) is reported lost or stolen, and it uses Active Sync to retrieve FIU mail it may be remotely wiped by the user via self service in Outlook Web Access, or by an IT Administrator. This can eliminate harm before it occurs or limit additional harm, perhaps preventing a privacy breach. Consider this response without delay and contact DoIT Email administration / Windows Enterprise Systems if you need assistance.

## Question 1: Does the FIU community member currently work in a "high information risk" department or organization?

"High risk" includes departments that normally process significant quantities of private information within their daily activities directly and on the device in question. Examples include groups that process personnel, financial, medical, alumni or student records, usually with full Social Security numbers. Relevant to the problem, try to determine what practices the department uses to manage institutional private information, especially email use.

## Question 2: Is the FIU community member working in a "high information risk" role?

Although a department may (or may not) typically process large quantities of private information on a day-to-day basis, the unique business role carried out by certain individuals within each department may itself involve regular collection, use or other access to such data. Often, a community member within a department has a legitimate business need to collect or use institutional private information. If so, these community members may have records containing private information directly on the endpoint device. These roles usually involve sensitive personnel activities such as hiring, financial, student record, or payment processing. Try to determine if the community member is in one of these roles and what practices he or she uses to manage FIU's private information.

## Question 3: Has the community member previously collected Private information?

As roles change, community members who may have once processed private information directly on the device may no longer do so today. However, legacy data is often unwisely copied over to new devices. FIU's DLP is designed to alert on this, and if

the community member no longer needs data previously collected but has retained it anyway, try to determine what practices he or she used or uses to manage it. Regardless of the outcome, encourage the user to destroy or remove (e.g. to scrub) private information, consistent with FIU Records Management guidance.

### Question 4: Has the community member used their FIU mail account to send and receive private information, and do they use that FIU account on this device?

A community member may believe they have no private information stored on a lost or stolen device, but may have old attachments in emails which have been inadvertently copied onto the device through mail client synchronization. Often, older messages are not synchronized in an effort to save space. Try to determine this by reviewing mail still accessible for review here at FIU. Do not destroy evidence (delete mail or empty trash, etc.) during this process.

**Any positive (yes) answers to these four triage questions will require immediate verbal internal notification to the FIU Security and Privacy Officer and further analysis. If the community member responds negatively (no) to all four questions, please report this information to the FIU Privacy and Security Officers and include it in your final report.**

## Incident & Breach Triage for other items

Because other items are not as common, they will need to be handled on a case-by-case basis. Please immediately report Incidents with impact for privacy to the FIU Privacy and Security Officers so the IRT can assemble and begin to evaluate work planning and next steps.

## General Terms

**Privacy** is the decision making process guiding the collection of information, and determining which disclosures or uses of such private information are authorized (and therefore what is an unauthorized disclosure) under various circumstances.

**Security** refers to the management process of preventing unauthorized disclosures, as well as detecting and responding to them if they occur.

**Compliance** is the process of continually demonstrating institutional conformance with applicable policies, laws and regulations. Finally, while information is made useful by modern technology, and security, privacy and compliance activities may benefit

from an understanding of key technical aspects, managing these activities is not itself a technical activity.

## A. FIU Incident Response Team Roles and Responsibilities

The Incident Response Team ("IRT"), shall consist of a core team of central administration with the ability to oversee the management of, or directly manage incidents, as may be required. This includes performing triage effectively, controlling all internal and external communications, reducing duplicative efforts, making a final decision on validating the breach and bringing in additional team members and external resources who may be engaged to support the entire process as needed.

| Function Represented | Role In Incident Response |
|---|---|
| Privacy/Compliance | • Help lead the IRT and manage incidents<br>• Investigate privacy policy violations<br>• Conduct training and document compliance with university-wide privacy policies<br>• Develop privacy monitoring tools<br>• Approve privacy policy exceptions |
| Information Security | • Help lead the IRT and manage incidents<br>• Investigate privacy/security related violations<br>• Conduct training and document compliance with university information security policies<br>• Provide subject matter expertise to the units/departments |
| Information Technology | • Manage IT infrastructure and applications as part of response process<br>• Assist with system outages caused by the incident or by recovery actions<br>• Coordinate information delivered via the Service Center |
| Legal | • Provide legal guidance to all aspects of FIU's response proceedings<br>• Make all final breach determination(s)<br>• Approve all proposed subject notification<br>Identify and file required contractual or regulatory submissions (e.g. OCR, Florida A.G., Granting Agency, etc.) |

| | |
|---|---|
| External Relations | • Is informed of incidents to respond to media inquiries |
| Internal Audit | • Investigate the effectiveness of internal controls and suspicions of internal fraud and abuse |
| FIU Police Department | • Implement law enforcement including loss of physical property (systems) or aid in investigations, coordination with external law enforcement activities, etc. |
| Privacy Liaisons, IT Administrators and other responders (working closely with the IRT) | • Assess and manage the incident response process at the unit level, and provide status updates and reports to the IRT through the Responding Party<br>• Coordinate outreach involving business unit staff/faculty and any 3rd party stakeholders (ex. a vendor or partner of the affected unit)<br>• Manage the local call center process |
| Risk Management | • Review coverage with the IRT and facilitate claim activity with FIU's insurer(s) and subcontractors. Participate in process after-action reviews to ensure FIU's coverage remains adequate |

## B. Local Responder Roles and Responsibilities

Responding Parties are also supported by internal team members working to resolved incidents within their department, division or unit as they occur (and immediately reporting those that could lead to a determination of a Privacy Breach to the FIU IRT). The Responding Party should consist of resources that understand local information

management practices and are capable of event and incident administration with the ability to oversee, or directly manage incidents, as may be required. As resource constraint varies at FIU, additional resources may be required and will be procured to assist or manage the incident as may be or become necessary.

| Function Represented | Role In Incident Response |
|---|---|
| Business Unit/Division Leader | • Ensure local processing activity conforms to this procedure<br>• Oversee timely communication with FIU IRT<br>• Liaise with vendors if issues under review are outsourced<br>• Participate in customization or development of notification message to those impacted, and sign letters<br>• Report uninsured financial losses to CFO |
| Responding Party | • Receive delegations from Business Unit Leader as appropriate<br>• Assess and manage the incident response process at the unit level, and provide status updates and reports to the IRT<br>• Coordinate outreach involving business unit staff/faculty and 3rd party stakeholders<br>• Work with the Office of the General Counsel to obtain approval for individual and regulatory notification<br>• Manage the local call center process |
| Information Technology | • Help lead the technical aspects of local investigation of incidents and suspected breaches<br>• Provide technical expertise to the unit/department<br>• Manage local IT infrastructure and applications as part of response process<br>• Assist with efficient system recovery actions |

## C. Incident / Breach Severity Level Matrix

If an incident with impact such as a breach has been confirmed, and with authorization from the IRT, the following matrix can be used to guide FIU management in establishing initial estimations of severity.

| Severity | Negligible | Low | Medium | High |
|---|---|---|---|---|
| Privacy impact to people | No impact | Impact to 10 people or less | Impact to 10-499 people<br><br>Regulatory agency notification required | Impact to 500 people or more |
| Financial risk | No financial exposure | Financial exposure is less than $25,000.00 | Financial exposure is $25,000.00 – 75,000.00 | Uninsured financial exposure exceeds $75,000.00 |

## D. Incident / Breach Internal Communication Matrix

The Incident Response Team will inform the appropriate parties if an incident is being analyzed which has potential to be declared a breach by General Counsel. Additionally, if an incident with a breach has been confirmed, and with authorization from the IRT, the following FIU management elements will be informed that victim notifications are expected to come from the business unit where the breach occurred and that documenting the breach and response is expected.

| | | | | |
|---|---|---|---|---|
| Level of internal reporting required beyond IRT | VP or Dean to report to OPS, DAC, President/Chief of Staff | VP or Dean to report to OPS, DAC, President/Chief of Staff | VP or Dean to report to OPS, DAC, President/Chief of Staff and Provost | VP or Dean to report to Chief of Staff, OPS, DAC, Provost, President |
| Level of additional or external notification | N/A; internal notification intended to effect improvements. | Once approved, VP or Dean to notify affected individuals and staff. General Counsel to notify any FIU partners (on a need to know basis) | Once approved VP or Dean to notify affected individuals and staff. OGC to notify partners and regulatory agencies if required | Notification strategy to be determined by IRT. OGC to notify partners and regulatory agencies if required |

## E. Periodic Testing

The incident and breach response procedure will be tested and reviewed annually unless an incident takes place where the procedure is used.. The test should include a walk-through of the plan components, and the actions and that would be taken in the test scenario(s), and a review of the test to determine how the systems or processes should be improved. Improvements should also come from actual use and lessons learned.

## F. Initial Report Checklist

| Information | Description |
|---|---|
| **Initial Estimated Severity Level** | Use the incident categories of Negligible, Low, Medium or High to define *initial estimated severity level and velocity of impact* |

| | |
|---|---|
| **Type of Incident** | Describe how it initially appears the incident may have occurred<br>• Unknown<br>• Human error<br>• Physical loss or theft<br>• Compromised Device or System<br>• Compromised User Credentials<br>• Social Engineering (or Phishing) |
| **Incident Timeline** | Date/time that the incident was discovered/reported<br>Date/time that the incident was reported to FIU Security/Privacy Officers<br>Date/time or data range that the incident occurred (if known) |
| **If external notification, who or what reported the event** | Contact Information for the Incident Reporter: full name, relationship to organizational unit/division, email address, phone number, and location (mailing address, office number). |
| **Additional Contact Information** | List contact information for any other parties involved in the incident |
| **Detailed description of the events so far** | Include as much information as possible such as:<br>Description of the incident (how it was detected, what occurred)<br>Description of the affected resources<br>Description who or what is impacted<br>Summary of response actions performed<br>Other organizations that may need to be contacted<br>Cause of the incident if known (misconfigured app, unpatched host, etc.)<br>List of evidence gathered<br>Total hours spent on incident handling and/or additional non-labor costs involved in handling (estimate)<br>Incident Handler Comments |
| **Identification of the devices(s)** | Source of the Incident: List of sources Host name/IP Address<br>Target of the Attack: Host Name/IP Address (note: Target of the attack should not be listed for incidents involving protected health information or sensitive student information) |
| **Additional details** | • Is external assistance required<br>• Status of media inquiries, if known<br>• Other pertinent summary items |

## G. After Action Review Items

| | |
|---|---|
| **Assessment of collected data on** | What was the scope of the incident and when did it occur? How did the incident evade controls? |

| | |
|---|---|
| **incident source** | |
| **Incident root cause analysis** | What vulnerabilities led to the incident occurring?<br>Could the incident have been prevented through existing processes? |
| **Assessment of collected data on incident response process** | How well did staff perform in their incident response? Were the documented procedures followed? |
| Incident response program analysis | Are there different actions that should be taken in the future? |
| **Assessment of collected data on incident's impact?** | What was the incident's hard cost (actual monetary loss)?<br>What were the incident's soft costs (inefficiencies, downtime, etc.)? |
| **Determination of concrete next steps** | What additional tools or resources are needed to mitigate future incidents?<br>What changes need to be made to policies, IT systems or procedures to prevent recurrence? |

**H.** Using this template and taxonomy, the FIU IRT can begin to develop a root cause analysis as part of the after action review.

| | | |
|---|---|---|
| **1. Breach as a Result of a Physical Loss** | 1.1. Documentation | Loss of control over documentation includes paper or other physical sensitive information. |
| | 1.2 Media and Portable Devices | Loss of control over media is where the data are in electronic form for use by a computing device, but the computing device is not part of what was lost; includes portable media such as CDs, hard drives, and memory sticks. |
| | 1.3 Hardware | This category includes all types of computing devices with sensitive data on their connected storage facilities (e.g., PDAs, smartphones, laptops, desktops.) |
| **2. Breach as a Result of Deliberate Act** | 2.1. Insider Action | This category includes instances where someone with legitimate access to sensitive information intentionally abuses it, thus causing a loss of control. Insiders can include employees, contractors, partners, vendors, customers, consumers, students, and outsiders with proximity to the organization. |
| | 2.2. Compromise | This loss of control of sensitive information results from the exploitation of vulnerability in an information system as a compromise (e.g., a computer virus or worm). |
| **3. Breach as a Result of a Procedural Failure** | 3.1 Processing Errors | This category includes errors in legitimate and normal business activity that result in a loss of control over sensitive information, such as exposing sensitive information, in a visible location (e.g., a document visible through an envelope window, a file or photo published on a website, a misprinted document). |
| | 3.2 Disposal | Improper disposal of information or the media that store it lead to this type of exposure. For example, Instances where sensitive information is carelessly thrown away and Computer equipment, desks, and filing cabinets being released though a surplus process. |

## After Action Review Questions

Incident and Privacy breach postmortem meeting agenda

Participants: IRT members, Business Unit Leadership

1. Assessment of Collected Data on Breach Source

What was the scope of the breach, and when did it occur? How did the breach evade security controls?

2. Breach Root-Cause Analysis

What vulnerabilities led to the breach? Could the breach have been prevented through existing processes?

3. Assessment of Collected Data on Breach Response Process

How well did various staff members perform in their breach response roles? Was the documented procedure followed?

4. Breach Response Program Analysis

Were any actions taken that might have delayed our response or inhibited recovery? Are there different actions that should be taken in the future?

5. Assessment of Collected Data on Breach's Impact

What was the breach's final actual impact (actual monetary loss)? What were the breach's soft costs (e.g., inefficiencies, downtime)?

6. Determination of Concrete Next Steps

What changes, or additional tools or resources are needed to mitigate or better respond to future breaches? What changes need to be made to IT systems or procedures to prevent recurrence?

## I. Incident Response Team At-A-Glance RACI Chart Template

The role of each member of the data breach response team is delineated below.

R=Responsible, A=Accountable, C=Consulted, I=Informed

| Role/Player | Privacy | CIO | CISO | Media Relations | Legal | Ofc. Of President | Stakeholder |
|---|---|---|---|---|---|---|---|
| Incident Intake | I | I | CI | N/A | I | N/A | RA |
| Declare a Privacy Breach | RC | I | IC | I | A | I | I |
| Convene Breach Response Team | RA | I | RA | I | I | I | I |
| Identify Affected Systems | I | I | CI | N/A | I | I | RA |
| Assess the Impact of the Breach | RA | I | RA | IC | A | I | CI |
| Contact Third-Party Experts for Support (e.g., OC, Forensics Experts) | I | I | RA | N/A | I | I | CI |
| Perform Forensic Analysis | I | I | IC | I | I | I | I |
| Draft Customer Notification Message(s) | RCI | I | I | RCI | A | I | RC |
| Liaise with the Media | CI | CI | CI | RA | I | I | CI |
| Conduct Postmortem Analysis | RA | RA | RA | CI | CI | I | CI |
| Report to Senior Executives | RA | RA | RA | RC | AR | I | AR |

**HISTORY**

Initial Effective Date: October, 2016
Review Dates (review performed, no updates): N/A
Revision Dates (updates made to document): February 3, 2025.