**I. INTRODUCTION TO THE INCIDENT RESPONSE PLAN.**

A.PURPOSE.

This Incident Response Plan (“IRP”) has been designed for data privacy-related incidents reported at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Organization”). While each data privacy-related incident has unique aspects, this plan gives the Incident Response Team (“IRT”) overall guidelines for its responsibilities and actions.

B.OBJECTIVES. The IRP enables the Organization to respond to most privacy-related incidents in an efficient and cost-effective manner that:

1. Avoids or minimizes damage to individuals whose Personally Identifiable Information (“PII”) or Protected Health Information (“PHI”) may have been compromised.

2. Avoids or minimizes short and long-term business losses resulting from a privacy-related data breach.

3. Meets industry and regulatory requirements and avoids breach-related penalties.

4. Minimizes the risk of class-action litigation resulting from a breach.

5. Minimizes the risk of similar breaches in the future.

C. IRP Requirements. The following requirements must be met to help ensure the effectiveness of the IRP:

1. The IRP must be approved by the Board of Trustees.

2. IRT members must be trained in their IRP roles and responsibilities.

3. The IRP must be tested and reviewed regularly.

4. The IRP must cover all foreseeable data breach incidents/types.

5. The IRP must outline how to assist administration, staff, faculty, employees, students, alumni, parents, donors and vendors in the event of a data breach.

6. The IRP must also cover interactions with vendors, contractors and strategic partners.

**II. INCIDENT RESPONSE TEAM AND OTHER CONTACTS**

A.OVERVIEW.

1. The Incident Response Team (“IRT”) typically operates under the authority of the Board of Trustees of the Organization to ensure data breach preparedness is a continuing priority for the entire Organization. The IRT is responsible for all phases of response to a privacy-related incident. The IRT is comprised of both team members internal to the Organization and those contracted by the Organization.

2. There are four phases to the Incident Response Process:

a. **1)**  **DISCOVERY** – occurs when an incident is reported.

b. **2)** **INVESTIGATION** – occurs when the Discovery phase establishes a likelihood that the incident is an actionable data breach.

c. **3) RESPONSE** – occurs when a data breach requires the Organization take further action to protect the organization and affected individuals whose Personal Information (PII) and/or Protected Health Information (PHI) is at risk or has been compromised.

d. **4) CLOSURE** – occurs after the Response phase where the IRT has the opportunity to review the incident, the actions taken, the effectiveness of the IRP and the reaction from affected individuals.

3. To be successful, the IRT members must have the expertise and training to respond to and manage privacy-related incidents, they must have the full support of the Board of Trustees, and they must have access to relevant data, tools and incident reports.

B.ROLES OF THE IRT.

1. IRT Leader

a. The IRT Leader is an individual from an internal or external legal department or a Chief Privacy Officer .

b. The IRT Leader should be able to:

i. Manage and coordinate the overall response efforts and IRT.

ii. Act as an intermediary between Board of Trustees and other IRT members to report progress and problems.

iii. Identify key tasks, manages timelines and documents all response efforts from beginning to end.

iv. Outline the budget and resources needed to handle a breach.

v. Assign the “Threat Level” of an incident (with assistance from IT).

vi. Summarize the steps needed to assess the scope of a breach.

vii. Ensure the contact lists remain updated and IRT members remain ready to respond.

viii. Analyze response efforts post-breach to better prepare the Organization and team for the next incident.

2. Executive Leaders

a. The Organization’s key decision makers should be included as advisors to the IRT to ensure you have the needed leadership, backing and resources to properly develop and test the IRP.

3. Insurance & Risk

a. Internal and external insurance and risk managers are critical to the incident responses process and should be notified immediately. Your insurance contacts will need to:

i. Determine whether the Organization carries insurance coverage for the specific type of privacy event;

ii. To the extent coverage exists, make certain to place all appropriate insurance brokers and carriers on notice to ensure the maximum amount of coverage for all phases of the incident and/or breach.

4. Legal

a. Rely on internal and external legal, privacy and compliance experts to shape the Organization’s data breach response and help minimize the risk of litigation and fines. Your legal representatives will need to:

i. Determine whether it is necessary to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers.

ii. Review and stay up to date on both state and federal laws governing data breaches in the industry.

iii. Oversee the Discovery and Investigation phases from an evidentiary perspective and maintain attorney-client privilege.

iv. Coordinate with internal and external legal teams as needed.

v. In conjunction with other members of the IRT, draft notification letters to affected individuals, notifications to applicable state and federal regulators, media notices and call center Frequently Asked Questions (FAQs).

5. IT & Security

a. Members from IT & Security should:

i. Train personnel in data breach response, including securing the premises, safely taking infected machines offline and preserving evidence.

ii. Work with a Forensic firm to identify the compromised data and delete hacker tools without compromising evidence.

iii. Coordinate with IT organizations to provide needed information during the Investigation phase and implement actions to prevent similar future incidents.

6. Public Relations / Crisis Management

a. Depending on the size of a data breach and the type of information at risk (or compromised), the Organization may need to report the breach to the media and/or notify affected individuals and/or state attorneys general offices. It is critical that the PR members of the IRT, while working with a Crisis Management firm, be able to:

i. Identify the best notification and crisis management tactics before a breach ever occurs.

ii. Handle any information leaks regarding a breach.

iii. Prepare and issue holding statements, press releases or statement to media, as needed and required.

iv. Track and analyze media coverage (including social media activity) and quickly respond to any negative press during and after a privacy incident or data breach.

7. Human Resources

a. Data breaches may affect administration, staff, faculty, employees, students, alumni, parents, donors and/or vendors, so the IRT should include representatives from student affairs and HR to provide needed support. Your representatives should:

i. Create simulation training for your employees that demonstrates how their roles would change during a data breach.

ii. Outline a plan for setting up a data breach hotline for administration, staff, faculty, employees, students, alumni, parents, donors or vendors if a breach occurs. Determine in advance if you will use internal or external resources.

iii. Coordinate with student affairs team to prepare for response after notification letters are sent out or PR announcements are made.

iv. Work with appropriate managers and employees to correct performance or improve processes or training (if employee performance is a factor in the incident).

v. Work with appropriate managers and legal representatives to take appropriate employment action (i.e., termination of employment) and legal action (if employee misconduct is a factor in the incident).

8. Finance

a. A representative from the Office of the CFO or finance department should be a part of the IRT and be responsible for:

i. Evaluating financial liability and business risks related to a breach incident.

ii. Conducting cost/benefit analysis for breach response planning.

iii. Gaining budget approval for data breach responses.

9. Data Breach Notification Vendor

a. An outside data breach notification vendor should also be a member of the Organization’s IRT. Given timing, it is best to contract with a data breach notification vendor in advance of a breach to secure the best rates. Such vendor will be able to:

i. Print and address breach notification letters.

ii. Timely and accurately mail the notifications to affected individuals (and verify delivery).

iii. Manage address lists and search for updated addresses when letters are returned to sender.

iv. Manage call centers after notifications are sent.

10. Law Enforcement

a. Depending on the severity of a data breach or privacy incident, you may need to involve law enforcement. Take time to collect all of the appropriate contact information now so you can act quickly if a breach does occur.

i. Identify which state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.

ii. During a breach, be sure everyone on the IRT is aware of any law enforcement directives so the investigation is not interrupted.

iii. If law enforcement believes that notice of the breach would impede a pending investigation, then Organization must receive a written stay of notice from law enforcement. ***Currently***, certain state Attorneys General require proof of stay of notice be produced if notice to state residents will be delayed.

C.INTERNAL IRT CONTACT LIST.

1. IRT Leader

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *IRT Leader – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *IRT Leader – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

2. Executive Leaders

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Executive Leader – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Executive Leader – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

3. Insurance & Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Insurance & Risk – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Insurance & Risk – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

4. Legal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Legal – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Legal – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

5. IT & Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *IT & Security – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *IT & Security – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

6. Public Relations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Public Relations – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Public Relations – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

7. Human Resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Human Resources – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Human Resources – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

8. Finance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Finance – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Finance – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

D.EXTERNAL IRT CONTACT LIST.

1. External Insurance & Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *External Insurance & Risk – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *External Insurance & Risk – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Mobile Phone: | Home Phone: | | Office Phone: | Email: |

2. External Legal Counsel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *External Legal Counsel – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *External Legal Counsel – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

3. Forensic Firm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Forensics Firm – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Forensics Firm – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

4. Public Relations / Crisis Management Firm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Public Relations /*  *Crisis Management Firm – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Public Relations /*  *Crisis Management Firm – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

5. Data Breach Notification Vendor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Data Breach Notification*  *Vendor – Primary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Data Breach Notification*  *Vendor – Secondary* | | Organization: | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

6. Law Enforcement and Government Agencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Police Department* | | | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Secret Service* | | | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *FBI* | | | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *State Attorney General* | | | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *U.S. Department of Education* | | | | |
| Name: | | Title: | | |
| Work Mobile Phone: | Personal Mobile Phone: | | Office Phone: | Email: |

E. THIRD PARTIES CONTACT LIST. Key vendors and business partners with whom the Organization shares PII/PHI, such as payment processors, marketing agencies, business partners or third-party service providers.

1. Business Partners

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Business Partners* | | | | |
| Organization | Contact | Mobile Phone | Office Phone | Email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

2. Vendors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Vendors* | | | | |
| Organization | Contact | Mobile Phone | Office Phone | Email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

3. Card Processors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Card Processors* | | | | |
| Organization | Contact | Mobile Phone | Office Phone | Email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4. Media

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Media* | | | | |
| Organization | Contact | Mobile Phone | Office Phone | Email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**III. DEFINITIONS AND POLICIES**

A.definitions.

1. **Personally Identifiable Information (PII)** – PII is confidential information and includes an individual’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual (depending on the State(s) statute(s) at issue: Social Security number; Diver's license number or state-issued identification card number; Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account; Passport number; Medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or health insurance information; or Username or email address coupled with a password or security question and answer that would permit access to an online account.

2. **Protected Health Information (PHI) –** PHI is confidential information and includes information that is created, received, and/or maintained by the Organization related to an individual’s health care (or payment related to health care) that directly or indirectly identifies the individual.

3. **Data Breach (Under State Law) –** the definition of a privacy-related data breach varies from state to state. The applicable state law is based on the current residency of each affected individual involved in the breach. Here are ***some current examples*** of the various risk of harm thresholds that trigger a “breach” (one or more of these thresholds may apply to your Incident):

a. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII;

b. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, that results or could result in identity theft or fraud;

c. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, unless PII is not used or subject to further unauthorized disclosure;

d. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, unless no misuse of PII has occurred or is not reasonably likely to occur;

e. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, unless no reasonable likelihood of harm to consumer whose PII was acquired has resulted or will result;

f. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, that has caused or is likely to cause loss or injury to a resident;

g. Unauthorized acquisition of PII that materially compromises the security, confidentiality or integrity of PII, that causes or is reasonably likely to cause substantial economic loss to the individual;

h. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, unless no reasonable likelihood of financial harm to consumer whose PII was acquired has resulted or will result;

i. Unauthorized access to and acquisition of PII where illegal use of the PII has occurred or is reasonably likely to occur and that creates a risk of harm to a resident;

j. Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII, unless technical breach does not seem reasonably likely to subject consumers to a risk of criminal activity.

4. **Data Breach (Under HIPAA/HITECH Final Rule) –** a “data breach” means an acquisition, access, use or disclosure of PHI that compromises the security or privacy of PHI.

a. A breach is *presumed* if there is an impermissible acquisition, access, use or disclosure of PHI unless the Organization (as either Covered Entity or Business Associate) demonstrates a low probability that PHI has been compromised, based on the following four (4) risk factors:

i. The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom disclosure was made;

iii. Whether PHI was actually acquired or viewed; and

iv. The extent to which the risk to PHI has been mitigated (i.e., obtaining reliable assurances by a recipient of PHI that the information will be destroyed or will not be used or disclosed).

B. TYPES OF DATA SECURITY INCIDENTS.

1. **Physical loss**: Stolen or lost laptop, PDA, thumb drive, or other portable media containing PII or other sensitive data, and hardcopies.

2. **Improper disposal**: Employees disposing of documents or records containing PII and/or PHI in the trash (without shredding paper or wiping disk drives).

3. **Misdirected communication**: Employee sending a fax, e-mail or snail mail with PII/PHI to the wrong recipient.

4. **Computer “glitch”**: A software issue or improper IT setting allowing unauthorized access or disclosure of PII or PHI.

5. **Database/server breach**: Unauthorized person accesses or hacks into a data server that stores personal or other sensitive data.

6. **Stolen Data by Otherwise Authorized Users**: Employee or other person with access downloads or sends personal or sensitive data to another unauthorized location for an improper purpose.

7. **Vendor Breach**: Negligence, physical loss, improper disposal, database/server breach or stolen data at a vendor’s location or server.

C. THREAT LEVELS.

1. **RED** – A data privacy incident where mission critical systems or resources are at risk, or after determination that confidential information, PII or PHI was, in fact, accessed, acquired, used or disclosed.

2. **YELLOW** – A data privacy incident where mission critical systems or resources may be at risk, if confidential information, PII or PHI may have been accessed, acquired, used or disclosed.

3. **GREEN** – A data privacy incident where mission critical systems or resources are not at risk, and no confidential information, PII or PHI has been accessed, acquired, used or disclosed.

D.DATA BREACH RESPONSE POLICY. In the event of a data breach involving PII and/or PHI, the Organization shall execute the following procedures, at a minimum:

1. **Containment** – The first priority after a data privacy incident is discovered is to contain the incident and notify supervisory personnel as quickly as possible. For any category of data privacy incident, the data must be secured, and the reasonable integrity, security and confidentiality of the data or data system must be restored.

2. **Classification** – The IRT shall immediately take steps to determine the exact nature of the incident in terms of its extent and potential risk to persons whose data has been compromised and to the organization. It is critical that external legal counsel be copied on all correspondence to maintain privilege.

3. **Internal Reporting of an Incident** – As soon as a privacy-related incident has been identified, the employee who discovered it must take immediate steps to report the breach to his or her supervisor. The supervisor must take immediate action to notify the IRT Leader, to determine the extent and cause of the incident, and to take such further action as is necessary to contain a data security incident or recover the missing PII and/or PHI. All incident reports and correspondence should be made to counsel’s attention and indicated directly on the reporting documents themselves (to preserve attorney-client privilege).

4. **Documentation** – The IRT, together with the supervisor reporting a data privacy-related incident (where applicable), must document the incident, noting the categories of information involved, the scope of the incident, steps taken to contain the incident, and the names or categories of persons whose PII/PHI was, or may have been, acquired by an unauthorized person. All members of the IRT must take care to document all actions taken, by whom, and the exact time and date. Record all forensic tools used in the investigation. Document all written notices made, web postings, communication plans and escalation records from the call center. This documentation is an ongoing obligation until the matter is concluded.

5. **Determination if Incident Constitutes a Breach** – The IRT, in conjunction with counsel, will determine, based on the facts and applicable law, if the data privacy incident rises to the level of a breach. This process includes conducting a risk assessment and evaluating the risk of harm thresholds (set forth above). If so, counsel will work with the IRT to determine the extent of reporting/notification obligations. If the Incident does not rise to the level of a breach, counsel, along with the IRT, will document their analysis accordingly.

6. **Notification to Affected Individuals** – Requirements, timing and forms of notification are all dependent upon **constantly changing** state and federal breach notification laws. The IRT should consult its external legal counsel for assistance in determining applicable statutes and notification requirements.

a. Time for Providing Notification. Once the IRT has determined that notification is required, the Organization shall notify affected individuals without unreasonable delay. However, notification may be delayed if law enforcement informs the Organization that disclosure of the breach would impede a criminal investigation or jeopardize national or homeland security. (Note: ***currently*** several states require that notification to affected individuals be sent within 30 or 45 days of discovery of the breach.)

b. Responsibility for Providing Notification. The responsibility for providing notification shall lie with the IRT Leader. The IRT Leader may delegate this responsibility, but should satisfy himself or herself that the proper notification has, in fact, occurred. (Note: some states ***currently*** require that copies of notifications and all records of the incident be maintained for at least five (5) years.)

c. Content of the Notification. Content of the notification is dependent upon ***current*** applicable statutes and regulations. ***Currently***, at a minimum, notification shall be clear and conspicuous, and it shall describe the incident in general terms along with the type of information involved (PII/PHI), the Organization’s actions to mitigate harm and investigate, steps individuals can take to protect themselves, information on fraud alerts and security freezes, contact information for nationwide credit reporting agencies, and contact information to receive further assistance from the Organization. Notices should also include a reminder to remain vigilant and promptly report incidents of suspected identity theft. Contact information for the FTC may also be included ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft); 1-877-IDTHEFT; Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580). Depending on state of residence of individual being notified, may need to include contact information for state Attorney General. Note, however, some states (i.e., Massachusetts) ***currently*** do not allow specific facts relative to the privacy incident to be included in the notification letters.

d. Method of Notification. Notification to affected persons must be provided as determined by the IRT and in compliance with applicable state or federal statutes, unless substitute notification is permitted.

e. Substitute Notification. Acceptable substitute notification will be determined by applicable state or federal statutes. Examples of ***current*** substitute notice include e-mail, conspicuous posting on website, and notice to statewide media.

7. **Notification Requirements to Regulators** – Many state and federal laws ***currently*** require notification to the state Attorneys’ General office, as well as other agencies. The time to notify may be as short as 14 days (i.e., Vermont). In addition, some states (i.e., Florida) require notice to the Attorney General after a risk assessment is completed and it is determined that the incident does not rise to the level of a breach.

**IV. PHASE 1: DISCOVERY**

A.OBJECTIVES.

1. Notify appropriate members of the IRT and Board of Trustees that there has been a possible incident.

2. If possible, assign a “Threat Level” to the privacy incident: (**RED, YELLOW** or **GREEN**).

3. Investigate and assess to confirm or rule out the existence of a data breach, and engage forensics experts as needed.

4. Contain the breach, if needed, and insofar as possible.

5. If credit cardholder data is involved, follow bankcard Organization requirements. (Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of compromise.)

6. Report findings to the designated IRT members and the Board of Trustees for approval to close the incident or move on to Phase 2: Investigation.

B. DISCOVERY REPORT. During this Phase 1, the IRT should answer the following questions with regard to the incident:

|  |  |  |
| --- | --- | --- |
| **Discovery Report** | | |
| Incident Number / ID: | | Threat Level: **RED** **YELLOW** **GREEN** |
| **Incident Facts** | Time incident reported: | |
| Time incident discovered: | |
| Time of incident: | |
| Place of incident: | |
| Persons involved in incident: | |
| What information was compromised and how much? ( administration, staff, faculty, employees, students, alumni, parents, donors and vendors data, financials, IP, health information) | |
| Accessibility/vulnerability of information (encryption, etc.): | |
| How was the information lost/compromised? (lost, misplaced, stolen, system failure, hacking, malicious attack on servers) | |
| Potential privacy breach (Yes/No): | |
| Who knows about the incident: | |
| **Initial Risk Assessment** | Number of individuals potentially affected: | |
| Risk to individuals (types and extents): | |
| Financial risk to organization: | |
| Legal/contractual risk to organization: | |
| Regulatory risk to organization: | |
| Public relations risk to organization: | |
| **Steps Taken** | Data loss containment: | |
| Legal counsel contacted: | |
| Law enforcement contacted: | |
| Agencies notified: | |
| Close or move to Investigation phase and why | |
| **Recommendations** | Any notification requirements yet? | |
| Priorities and considerations for further investigation | |
|  | |

C. CONCLUSIONS FOR PHASE 1. If the initial discovery efforts indicate that PII/PHI has been compromised or lost, or that there may be significant negative impact to the organization and/or the persons whose data has been compromised, the incident should move to the Investigation phase. It is not necessary to determine at this point what other specific actions are needed. The IRT need only establish that action is warranted and that further investigation and assessment are advisable. Reminder: All incident reports and correspondence should be made to counsel’s attention and indicated directly on the reporting documents themselves (to preserve attorney-client privilege).

**V. PHASE 2: INVESTIGATION**

A.OBJECTIVE. During this Investigation Phase, the IRT will conduct a thorough investigation and assessment to determine what further actions need to be taken and solidify the “Threat Level” of the incident.

B. FORENSICS. During this phase, the IRT needs to conduct an in-depth investigation to confirm that any breach has been fully contained and to determine the steps necessary to help prevent similar incidents in the future. This investigation will be conducted by a subset of the IRT and other vendors. This team will investigate to determine:

1. The exact circumstances and causes of the data breach or loss;

2. Whether the data breach or loss has been stopped to the full extent possible; and

3. What system, process or personnel changes are necessary or advisable to help prevent similar incidents in the future.

C. LEGAL. External legal counsel and certain members of the IRT are responsible for investigating the legal ramifications and risks of a privacy-related incident and formulating a plan to mitigate the risks. Legal counsel will need to determine:

1. Are there possible legal liabilities from this incident such that further evidence gathering or other action is advisable?

2. Are there regulatory or contractual obligations to notify any administration, staff, faculty, employees, students, alumni, parents, donors and vendors of this incident?

3. Are there any known contractual obligations to provide credit monitoring/identity theft protection in this case? (Although not legally required, it may still be provided.)

4. Are there other actions required by existing contractual obligations?

D. LAW ENFORCEMENT. With assistance from outside legal counsel and the internal legal department, IRT must determine whether law enforcement should be involved in the incident investigation and document as appropriate.

1. Should a written stay of notice be obtained pending law enforcement investigation of the incident?

D. INVESTIGATION REPORT. During this Phase 2, the IRT should answer the following questions with regard to the incident and prepare a report with its findings and recommendations:

|  |  |  |
| --- | --- | --- |
| **Investigation Report** | | |
| Incident Number / ID: | | Threat Level: **RED** **YELLOW** **GREEN** |
| **Incident Summary** | What, when, where, who was involved in incident: | |
| **Computer Forensic Findings** | Cause(s), contributing factors, etc.: | |
| **Risk Analysis** | Risks to organization (types and extents): | |
| Risks to individuals (types and extents): | |
| **Recommendations** | Notification: | |
| Credit Monitoring/Identity Theft Protection: | |
| Legal action: | |
| Communications: | |
| Personnel action: | |
| Prevention (system and process changes): | |

E. CONCLUSIONS FOR PHASE 2. At the end of the Investigation phase, the IRT should prepare a report with its findings and recommendations. The IRT can then decide what responses the organization will implement in Phase 3. Reminder: All incident reports and correspondence should be made to counsel’s attention and indicated directly on the reporting documents themselves (to preserve attorney-client privilege).

**VI. PHASE 3: RESPONSE**

A.OBJECTIVES. During this Response Phase, the IRT will execute those recommendations set forth in the Investigation Report and complete the following:

1. Execute approved recommendations from the investigation report, including notification and credit monitoring, public relations efforts, legal and law enforcement efforts, personnel actions, and system and process changes to help prevent similar incidents in future.

2. Resolve any issues that arise during implementation.

3. Track implementation and report status to the Board of Trustees.

4. Document responses and securely archive documentation.

5. Upon completion, report to the designated privacy/security officer and executive team and request approval to close the incident.

B.NOTIFICATION.

1. Investigation and assessment of notification needs are the responsibility of a subset of the IRT. This team will work in consultation with external legal counsel and the data breach notification vendor, the public relations vendor and any regulatory agency contacts.

2. Notification may be required under contractual commitments, applicable laws or regulations, or to avoid harm to the organization and/or the individuals whose data was compromised. The notification assessment needs to fully investigate the extent and risks of the data loss to determine:

a. Is there potential risk to individuals affected by the breach that can be mitigated through notification?

b. Is there a possible regulatory requirement to notify the individuals whose data was lost or compromised?

c. Is there a possible regulatory requirement to notify government or other agencies of a data breach?

d. Are the estimated business or public relations impacts such that notification may be advisable to prevent damage to our business or brand?

e. Would notification help to mitigate our legal liability for the data breach?

3. If the IRT, with advice from legal counsel, determines that notification is required or advisable, they will make recommendations outlining:

a. Groups of individuals who should be notified and deadlines for notification.

b. State and Federal Agencies to notify, agency contacts, required information and deadlines for notification.

c. State Attorneys General to be notified.

d. Timing of notification, to protect individuals and meet legal and regulatory requirements while not interfering with any law enforcement investigation.

e. The Various versions of the notification letters (given state nuances).

f. Any special notification needs (persons with disabilities, minors, military personnel on active duty, etc.) .

g. Recommended resources for assistance after notification (call center assistance, etc.).

4. The various versions of the notification required will vary by situation and state nuances, but standard best practices at this time include the following components:

a. Website to enroll victims in credit monitoring or other identity theft protection services, educate consumers about identity theft and provide contact information.

b. Call center to address questions or concerns consumers may have regarding the incident or protection of their PII.

c. Letter to notify breach victims about the incident, inform them about preventative and credit monitoring services and direct them to public resources for monitoring their credit. (It is critical to note that no single letter can comply with every state and federal regulation at this time. External legal counsel must assist in this matter.)

C.CREDIT MONITORING/IDENTITY THEFT PROTECTION SERVICES.

1. Investigation and assessment of credit monitoring/identity theft protection needs are the responsibility of a subset of the IRT. This team will work in consultation with external legal counsel and the data breach notification vendor and the public relations vendor.

2. Credit monitoring/identity theft protection may be required under contractual commitments or to avoid harm to the organization and/or the individuals whose data was compromised. The notification assessment needs to fully investigate the extent and risks of the data loss to determine:

a. Is it possible that persons or organizations whose information was compromised will be damaged by this data breach or loss?

b. Are the estimated possible damages to those individuals or organizations or to the Organization such that credit monitoring/identity theft protection services may be advisable?

c. Will credit monitoring/identity theft protection properly protect the affected individuals given the information compromised (i.e., credit monitoring may not help affected individuals’ if their PHI was compromised.)

d. Are there any known contractual obligations or legal or regulatory requirements to provide credit monitoring/identity theft protection in this case?

D. CONCLUSIONS FOR PHASE 3. The Notification phase will conclude, for the most part, when all notification letters have been sent to affected individuals and appropriate state and federal agencies, re-delivery has occurred relative to those individuals with invalid addresses on the first attempt, and once all response letters, calls and e-mails from affected individuals and state and federal agencies have been replied to.

**VII. PHASE 4: CLOSURE**

A.OBJECTIVE. After the IRT has the opportunity to review the incident, the actions taken, the effectiveness of the IRP and the reaction from affected individuals, it shall make all appropriate documentations and close out the incident.

B. CLOSURE REPORT. During the Closure Phase, the IRT will complete the following Closure Report:

|  |  |  |
| --- | --- | --- |
| **Closure Report** | | |
| Incident Number / ID: | | Threat Level: **RED** **YELLOW** **GREEN** |
| **Incident Summary** | Summary of incident, actions taken and completed: | |
| **Mitigation** | Partners and agencies notified: | |
| Contractual obligations fulfilled: | |
| Regulatory obligations fulfilled: | |
| Documentation archived: | |
| Other actions: | |
| **Notification** | Groups notified: | |
| Public/media notification: | |
| Summary of response: | |
| **Credit Monitoring/**  **Identity Theft**  **Protection**  **Offering** | Program(s) offered, % activation, etc.: | |
| Credit monitoring provided (number and type of incidents, actions taken, resolution to date): | |
| **Prevention** | System changes: | |
| Process changes: | |
| **Follow-up** | Actions remaining: | |
| Plan for monitoring and assessment (of process changes, etc.): | |
| **Recommendation to Close** | Criteria to consider the incident closed: | |

C. CONCLUSIONS FOR PHASE 4. The Closure phase will conclude, for the most part, after the Closure Report is completed, all responses to state and federal regulators have been made and the call center is closed.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.