ENTHEOS ACADEMY

EXCELLENCE • SERVICE • LEADERSHIP

6301 Data Breach

Purpose

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. Entheos Academy's operations rely on the proper use of Confidential Information and Personally Identifiable Information (PII) on a daily basis. Managing risk and responding in an organized way to Incidents and Breaches is key to operations and required by Utah state law.Entheos Academy must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize the district-wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure Entheos Academy can act responsibly, respond effectively, and protect its information assets to the extent possible.

Scope

This policy applies to all Entheos Academy staff.

Definitions

I. A "Data Security Incident" or "Incident' shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of Entheos Academy. Common examples of data security Incidents include, but are not limited to, any of the following:
   A. Successful attempts to gain unauthorized access to an Entheos Academy system or Student or Educator PII regardless of where such information is located
   B. Unwanted disruption or denial of service
   C. The unauthorized use of an Entheos Academy system for the processing or storage of Confidential Information or PII
   D. Changes to Entheos Academy's system hardware, firmware, or software characteristics without Entheos Academy's knowledge, instruction, or consent
   E. Loss or theft of equipment where Confidential Information or PII is stored

F. Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII
G. Human error involving the loss or mistaken transmission of Confidential Information or PII
H. Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

II. A "Data Security Breach" or "Breach" is any Incident where Entheos Academy cannot put in place controls or take action to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an Incident where data has been misused.

Policy

I. Adopting a standardized and consistent approach to Incident management shall ensure that:
   A. Incidents are reported in a timely manner and can be properly investigated
   B. Incidents are handled by appropriately authorized and skilled personnel
   C. Appropriate levels of management are involved in response management
   D. Incidents are recorded and documented
   E. Organizational impacts are understood and action is taken to prevent further damage
   F. Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
   G. External agencies, customers, and data users are informed as required
   H. Incidents are dealt with in a timely manner and normal operations are restored
   I. Incidents are reviewed to identify improvements in policies and procedures

II. Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

Data Classification

I. Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that Entheos Academy management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

II. All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following Entheos Academy data categories:

A. Public Data - Information intended for public and community use or information that can be made public without any negative impact on Entheos Academy or its customers. Student PII shall never be considered public data unless the data is Directory Information as defined by Entheos Academy policy.
B. Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of Entheos Academy. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within Entheos Academy. Employee and Educator PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification.
C. Highly Confidential Data- Information that, if breached, causes significant damage to Entheos Academy operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.

INCIDENT REPORTING

I. The following process shall be followed when responding to a suspected Incident:
   A. Confirmed or suspected Incidents shall be reported promptly to the Chief Privacy Office and the IT Security Manager. A formal report shall be filed that includes full and accurate details of the Incident including who is reporting the Incident and what classification of data is involved.
   B. Once an Incident is reported, the Chief Privacy Officer shall conduct an assessment to establish the severity of the Incident, next steps in response, and potential remedies and solutions. Based on this assessment, the Chief Privacy Officer shall determine if this Incident remains an Incident or if it needs to be categorized as a Breach.
   C. All Incidents and Breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.

CLASSIFICATION

I. Data Breaches or Incidents shall be classified as follows:
   A. **Critical/Major Breach or Incident –** Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale LEA-wide. All Incidents or Breaches involving Student PII will be classified as Critical or Major. They typically have the following attributes:
      1. Any Incident that has been determined to be a Breach

2. Significant Confidential Information or PII loss, potential for lack of business continuity, Entheos Academy exposure, or irreversible consequences are imminent
3. Negative media coverage is likely and exposure is high
4. Legal or contractual remedies may be required
5. Requires significant reporting beyond normal operating procedures
6. Any breach of contract that involves the misuse or unauthorized access to Student PII by a School Service Contract Provider

B. **Moderately Critical/Serious Incident** – Breaches or Incidents in this category typically deal with Confidential Information and are on a medium scale (e.g. <100 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:
   1. Risk to the Entheos Academy is moderate
   2. Third party service provider and subcontractors may be involved
   3. Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized Entheos Academy exposure
   4. Significant user inconvenience is likely
   5. Service outages are likely while the breach is addressed
   6. Negative media coverage is possible but exposure is limited
   7. Disclosure of Educator or Employee PII is contained and manageable

C. **Low Criticality/Minor Incident** – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale (e.g. <10 users on the internal network), personal or mobile device related). Incidents in this category typically have the following attributes:
   1. Risk to Entheos Academy is low
   2. User inconvenience is likely but not LEA damaging
   3. Internal data released but data is not student, employee, or confidential in nature
   4. Loss of data is totally contained on encrypted hardware
   5. Incident can be addressed through normal support channels

INCIDENT RESPONSE

Management response to any reported Incident shall involve the following activities:

I. *Assess, Contain and Recover Data* - All security incidents shall have immediate analysis of the Incident and an Incident report completed by the Chief Privacy Officer or their designee. This analysis shall include a determination of whether this Incident should be characterized as a Breach. This analysis shall be documented and shared with the Executive Director, the affected parties, and any other relevant stakeholders. At a minimum, the Chief Privacy Officer shall:

Step	Action	Notes
A	Containment and Recovery:	Contain the breach, limit further organizational damage, seek to recover/restore data.
1	Breach Determination	Determine if the Incident needs to be classified as a Breach.
2	Ascertain the severity of the Incident or Breach and determine the level of data involved.	See Incident Classification
3	Investigate the Breach or Incident and forward a copy of the Incident report to the Executive Director	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the IT Security Manager. In the event that the Incident or Breach is severe, Entheos Academy's executive management, general counsel and the Board Chair shall be contacted
4	Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterized as a Breach.	Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the Incident.
5	Determine depth and breadth of losses and limit exposure/damages	Can data be physically recovered if damaged through use of backups, restoration or other means?
6	Notify authorities as appropriate	For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve Student PII that involves a School Service Contract Provider, notify the Entheos Board members.

7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting.	Complete Incident Report and file with Executive Director

II. *Assess Risk and Incident Scope* – All Incidents or Breaches shall have a risk and scope analysis completed by the Chief Security Officer or their designee. This analysis shall be documented and shared with the Executive Director, the affected parties, and any other relevant stakeholders. At a minimum, the Chief Security Officer shall:

B	Risk Assessment	Identify and assess ongoing risks that may be associated with the Incident or Breach.
1	Determine the type and breadth of the Incident or Breach	Classify Incident or Breach type, data compromised, and extent of breach
2	Review data sensitivity	Determine the confidentiality, scope and extent of the Incident or Breach.
3	Understand the current status of the compromised data	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk.
4	Document risk limiting processes or technology components that contain and manage the Incident	Does encryption of data/device help to limit risk of exposure?
5	Determine what technologies or processes will mitigate the loss and restore service	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of Incident or Breach	How many individuals' personally identifiable information were affected?
7	Define individuals and roles whose data was compromised	Identify all students, staff, districts, customers or vendors involved in the Incident or Breach

8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential Information or PII could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.
9	Determine actual or potential harm that could come to any individuals	Identify risks to individuals: Physical Safety, Emotional Wellbeing, Personal or Business Reputation, Financial Implication, Identity Concerns
10	Are there wider consequences to consider?	Is there risk to another LEP, the state, or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact all local education providers, agencies, or companies impacted by the breached data, notify them about the Incident, and ask for assistance in limiting the scope of the Incident.

III. *Notification and Incident Communication*s - Each security Incident or Breach determined to be "moderately critical" or "critical" shall have communication plans documented by the LEA's senior leadership, and their designees to appropriately manage the Incident and communicate progress on its resolution to all effected stakeholders. At a minimum, the Chief Security Officer shall:

C	Notification and Communications	Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the Incident or Breach.

1	Are there legal, contractual or regulatory notification requirements associated with the Incident or Breach?	Review vendor contracts and compliance terms, assure state and federal reporting and notifications are understood. Contact legal services as necessary to begin contractual adherence. Should the Breach include Student PII, initiate the Entheos Board hearing process.
2	Notify impacted individuals of Incident or Breach remedies.	Provide individuals involved in the Incident or Breach with mitigation strategies to re-secure data (e.g. change user id and/or passwords etc.)

3	Determine Internal Communication Plans	Work with senior leadership and provide regular internal updates on status of Incident or Breach, remedies underway, and current exposure and containment strategies. This messaging should be provided to all internal state stakeholders and management. Messaging shall be coordinated through the main office.
4	Determine Public Messaging	Prepare and execute a communication and follow-up plan with the Executive Director and senior leadership. Communication strategies need to define audience(s), frequency, messaging, and content.
5	Execute Messaging Plan	Working through the Executive Director and appropriate leadership, execute the public and internal communication plans. Depending on the nature and scope of the Incident or Breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include: ● A description of the Incident or Breach (how and when it occurred) ● What data was involved and whose data was compromised ● Details of what has been done to respond to the Incident or Breach and any associated risks posed ● Next-steps for stakeholders ● LEA contacts for the Incident or Breach, any follow-, and other pertinent information ● When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what Entheos Academy and/or third party vendor will do to help minimize their exposure ● Provide a way in which they can contact Entheos Academy for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page)

IV. Post Mortem Evaluation and Response – Each Incident or Breach determined to be "moderately critical" or "critical" shall have a post mortem analysis completed by the

Chief Security Officer and their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future. At a minimum, the Chief Security Officer shall:

	Evaluation and Response	To evaluate the effectiveness of the school's response to the Incident or Breach.
	Establish where any present or future risks lie.	Assess and evaluate the root causes of the Incident or Breach and any ways to mitigate and/or prevent a similar occurrence.
	Consider the data and security measures employed.	Evaluate, analyze, and document the use cases and technical components of the Incident or Breach. Document areas for improvement in environment, technology, or approach that limit future security exposures. Make recommendations as appropriate.

	Evaluate and identify areas of weakness in existing security measures and procedures.	Document lapses in process, procedure, or policy that may have caused the Incident or Breach. Analyze and document solutions and remedies to reduce future risks.
	Evaluate and identify areas of weakness related to employee skills.	Assess employee readiness, education, and training. Document and plan for updates in education or procedural changes to eliminate potential for future Incidents.
	Report on findings and implement recommendations.	Prepare report and presentation to Entheos Academy for major Incidents or Breaches.

V. Each of these four elements shall be conducted as appropriate for all qualifying Incidents or Breaches. An activity log recording the timeline of Incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the Chief Security Officer.

VI. Audit Controls and Management

A. On-demand documented procedures and evidence of practice should be in place for this operational policy. Appropriate audit controls and management practice examples are as follows:

B. Archival completed Incident Reports demonstrating compliance with reporting, communication and follow-through.

C. Executed communication plans for Incident management.

D. Evidence of cross-departmental communication throughout the analysis, response and post-mortem processes.

VII. Enforcement

A. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

VIII. Distribution: This policy is to be distributed to all Entheos Academy staff.