1.7 - Data Breach Response Policy and Procedure

Overview

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. WVUP 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 West Virginia state law.

Purpose

WVUP must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize WVUP-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 WVUP can act responsibly, respond effectively, and protect its information assets to the extent possible.

Scope

This policy applies to all WVUP staff.

Policy

GENERAL INFORMATION

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 WVUP.

Common examples of data security Incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorized access to a WVUP system or Student or Educator PII regardless of where such information is located
- Unwanted disruption or denial of service
- The unauthorized use of a WVUP system for the processing or storage of Confidential Information or PII
- Changes to WVUP system hardware, firmware, or software characteristics without WVUP's knowledge, instruction, or consent

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

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

Adopting a standardized and consistent approach to Incident management shall ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorized and skilled personnel
- Appropriate levels of management are involved in response management
- Incidents are recorded and documented
- Organizational impacts are understood and action is taken to prevent further damage
- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
- External agencies, customers, and data users are informed as required
- Incidents are dealt with in a timely manner and normal operations are restored
- Incidents are reviewed to identify improvements in policies and procedures

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.

Any contract breach that results in the misuse or unauthorized access to Student PII by a School Service Contract Provider must be handled according to the Board Policies Regarding SSCP Breaches and as required by C.R.S. 22-16-107(2)(a).

DATA CLASSIFICATIONS

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 WVUP management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

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 WVUP data categories:

Public Data - Information intended for public and community use or information that can be made public without any negative impact on WVUP or its customers. Student PII shall never be considered public data unless the data is Directory Information as defined by WVUP policy.

Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of WVUP. 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 WVUP. Employee and Faculty PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification

Highly Confidential Data – Information that, if breached, causes significant damage to WVUP operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Faculty Financial Information, Social Security Numbers, and other critical information also falls into this classification.

Incident Reporting

The following process shall be followed when responding to a suspected incident:

- Confirmed or suspected incidents shall be reported promptly to the Chief Information Officer. 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.

- Once an incident is reported, the CIO shall conduct an assessment to establish the severity of the incident, next steps in response, and potential remedies or solutions. Based on this assessment, WVUP shall determine if this incident remains an incident or if it needs to be categorized as a breach.

- All incidents and breaches will be centrally logged and documented to ensure appropriate documentation, oversight and consistency in response, management, and reporting.

Classification

Data breaches or incidents shall be classified as follows:

Critical/Major Breach or Incident – Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale WVUP-wide. All incidents or Breaches involving Student PII will be classified as Critical or Major. They typically have the following attributes:

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

Moderately Critical/Serious Incident – Breaches or incidents in this category typically deal with Confidential Information and are on a medium scale. Incidents in this category typically have the following attributes:

- Risk to WVUP is moderate
- Third party service provider and subcontractors may be involved
- Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized WVUP exposure.
- Significant user inconvenience is likely
- Service outages are likely while the breach is addressed
- Negative media coverage is possible but exposure is limited

- Disclosure of Faculty or Employee PII is contained and manageable

Low Critically Minor Incident – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale. Incidents in this category have the following attributes

- Risk to WVUP is low
- User inconvenience is likely but not WVUP damaging
- Internal data released but data is not student, employee, or confidential in nature
- Loss of data is totally contained on encrypted hardware
- Incident can be addressed through normal support channels

Incident Response

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

Assess, Contain, and Recover Data – All security incidents shall have immediate analysis of the incident and an incident report completed by the CIO 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 WVUP Executive Team, the affected parties, and any other relevant stakeholders. At a minimum the CIO shall:

Step	Action	Notes
A	Containment & 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 WVUP EVP of Finance & Administration	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the Executive Team. In the event the Breach is severe, general counsel shall be consulted
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	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.

	possible. If this loss cannot be mitigated, any incident will be considered a breach	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 WVUP Board of Governors
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting	Complete Incident Report and file with EVP of Finance.

Asses Risk and Incident Scope – All incidents or Breaches shall have a risk and scope analysis completed by the CIO or their designee. This analysis shall be documented and shared with the EVP of Finance & Administration, President, the affected parties, and any other relevant stakeholders. At a minimum the CIO 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 the 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 possess 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 services	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	How many individuals PII were affected?
7	Define Individuals and Roles whose data was compromised	Identify all students, staff, 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 individual	Identify risks to individual's physical safety, emotional wellbeing, personal or business reputation, financial implications, or identity concerns
10	Are there wider consequences to consider?	Is there risk to the State or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact local colleges, agencies, or companies impacted by the breached data and request assistance.

Notification and Incident Communication – Each security incident or breach determined to be "moderately critical or critical" shall have communication plans documented by the CIO, executive team, President or their designee to appropriately manage the incident and communicate progress on its resolution to effected stakeholders

Post Mortem Evaluation and Responses – Each incident or Breach determined to be "moderately critical or critical" shall have a post mortem analysis completed by the CIO and their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future.

Each of the four elements shall be conducted as appropriate for all qualifying incidents or Breaches. An activity log recording the timeline of the incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the CIO.

Audit Control and Management

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:

- Archival completed incident reports demonstrating compliance with reporting, communication and follow-through
- Executed communication for incident management
- Evidence of cross-departmental communication throughout the analysis, response, and post-mortem processes.

Enforcement

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