West Virginia Higher Education Policy Commission
West Virginia Community and Technical College System

Privacy Management and Incident Response Plan

1. Purpose

The purpose of this plan is to provide effective and appropriate response procedures to events and situations that may expose personally identifiable information (PII), student education records collected and maintained by the West Virginia Higher Education Policy Commission (Commission) and the West Virginia Community and Technical College System (Council) to unauthorized individuals, both internally and externally.

The procedures in this plan are based on industry standards and adheres to state and federal privacy laws and regulations[1] and best practices recommended by the U.S. Department of Education's Student Privacy Policy Office (SPPO). This plan is reviewed annually or as circumstances dictate and revised as applicable.

2. Scope and Authority

This plan applies to all employees (paid and unpaid, full-time and part-time, technical and non-technical), vendors, contractors, researchers, and all other individuals acting as official agents of the Commission or Council. The plan encompasses all data and information collected and maintained, whether in electronic, paper, or other format and regardless of the collection and storage method.

The Executive Vice Chancellor for Administration for the Commission and Council has appointed a Privacy Officer and named them as the designated authority to establish and maintain a system of data privacy and information security and protection. The Privacy Officer has the authority needed to make crucial decisions, delegate tasks, serve as a liaison between leaders and stakeholder groups, and provides relevant direction to manage and maintain privacy and deal with real and potential threats.

3. Definitions

It is vital for the elements and concepts associated with privacy and privacy incidents be consistent, understood, and evident. The following definitions are provided to describe terms and concepts used throughout this plan.

Access means to view, print, download, copy, or otherwise retrieve data from a computer, computer system, or computer network.

[1] *State and Federal privacy laws and regulations include but are not limited to the following: W.V. Code §46A-2A et seq., Family Educational Rights and Privacy Act (FERPA), the Higher Education Act of 1965 as revised in 2008 (HEA), the Gramm-Leach-Bliley Act (GLB), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

Authorized Party refers to those individuals or organizations with consent to access information or with a legitimate interest in or need for access to PII and other records about individuals in order to perform appropriate tasks necessary for their jobs.

Consent in general, means permission from a parent/guardian, eligible student, or other responsible party to disclose information from official records to another party.

Data breach is any successful or confirmed incident in which personally identifiable information (PII), sensitive, confidential or protected data has been disclosed and/or accesses by an unauthorized individual or in an unauthorized fashion. Data breaches are a subcategory of privacy incidents.

Disclosure means to permit access to, release, transfer, or otherwise communicate personally identifiable information (PII) from a record to any party by any means, including electronic, written, or verbal.

> An authorized disclosure refers to any disclosure of information about an individual for which that individual has given consent or that is permitted or required pursuant to federal or state regulation for legitimate purposes. These types of disclosures are made to authorized parties.
>
> An unauthorized disclosure refers to any access to or disclosure of information about an individual that is not authorized or that is made to or by an unauthorized party. Unauthorized disclosures can be internal to the agency or institution, or to an external organization or party. They may be the result of personal negligence, system failures, or malicious acts.

Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

Personally Identifiable Information (PII) includes any information that by itself or in combination with other information, has the potential to directly determine or find the identity of an individual person and could be harmful to an individual if disclosed.[2]

- Social security number, state/federal issued personal identification number, or driver's license number.
- Banking or credit card numbers.
- Financial information including State and Federal tax information.
- Full name and personal address.
- Name of student's parent and other family members, or mother's maiden name.
- Citizenship or immigration status.
- Health and medical information.

[2] *See Family Educational Rights and Privacy Act (FERPA) regulations, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.*

- Student grades, GPA, ACT or SAT scores.
- FAFSA or financial aid information.

Sensitive data is defined as data that if disclosed could result in a moderate level of risk. This includes data that is made available through open record requests or other formal or legal processes.

- Employment and training program data.
- Most data elements in State personnel records.
- State/federal contracts data.
-

Indirect PII is information, when linked or linkable could be used to identify an individual

- Date or place of birth.
- Business phone.
- Race/ethnicity.
-

Public information is characterized as being open to the public. Information that alone or in combination with other data can cannot be used by a reasonable person to identify an individual; furthermore, if disclosed or shared, it would result in little or no risk to the individual or agency.

- Directory information which includes information that is not generally considered to be harmful to an individual, or an invasion of privacy.
- Enrollment in an institution.
- Official honors and awards received.
- Participation in officially recognized sports.
- Agency public websites.
- Commission and Council policies and procedures.
-

A Privacy Incident is an attempted or successful effort to access, acquire, disclose, or use PII or other information without authorization (i.e., any potential or actual unauthorized disclosure) regardless of the format. Such events may expose PII or other information to parties that are not authorized to access the information or may involve the misuse of PII or other information for purposes other than those that are explicitly permitted.

A security breach refers to any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy and data or information.

Unauthorized Party refers to individuals or organizations without consent and without a legitimate interest in having access to PII and other records about individuals.

4. Examples

Privacy incidents, including data breaches, may be the result of accidents or negligence on the part of authorized individuals, failures of systems designed to store and protect information, or malicious acts intended to cause harm. These incidents can take many forms including (but not limited to) the following examples:

- Lost, stolen, unsecured, or temporary misplaced equipment, tablets, laptops, physical records, or other devices such as smart phones;
- Lost or stolen storage media, including flash drives, CDs/DVDs, external hard drives, SD cards, or other external storage that contains PII or other sensitive data;
- Improper storage or disposal of records, whether electronic or physical;
- Posting or exposure of student information on public facing websites, public formal or informal reports and publications, social media, or other public venue;
- Intentional or accidental transmission of student information to unauthorized parties regardless of the method;
- Sharing data without full authorization or through non-secure methods such as email, texting, or other non-secure methods;
- Sharing, posting, or otherwise not securing your passwords that allow access to PII or other sensitive information;
- Compromised computers or servers, such as times where a machine or network has been hacked or accessed by an unauthorized party;
- Receipt of student information that an individual is not entitled to;
- Use of student or employee information for purposes other than official institution or agency related business;
- Malware, computer viruses, or other malicious attacks that could compromise the security of a computer or network; and
- Violations of official security policies and procedures.

The Commission and Council's privacy management and incident response process is designed to protect against and respond swiftly to all privacy incidents; special care is indicated in responding to those incidents that are malicious in nature and those that are data breaches.

5. Roles and Responsibilities

Privacy management and data security is the responsibility of all employees, vendors, contractors, researchers, and all other individuals acting as official agents of the Commission or Council. Specific divisions and employees have heightened responsibilities to ensure appropriate data governance and to manage and respond to privacy incidents.

The general responsibilities for key staff involved in privacy incident response for the Commission and Council are outlined below.

Commission and Council Privacy Officer

The Privacy Officer represents the Commission, the Council, West Virginia Network for Educational Telecomputing (WVNET), the public regional institutions, and the community and technical colleges on the state privacy management team. The Privacy Officer is responsible for all privacy management and incident response efforts undertaken by the Commission and Council. The Privacy Officer may appoint a designee to lead the efforts if the situation is warranted.

State Level Incidents
When a potential incident is discovered at the state level, the Privacy Officer is responsible for initiating the incident response plan, reporting the incident to the State Privacy Office if applicable, assigning an incident response team, and leading the efforts from the initial identification of the incident through the post-incident review of lessons learned.

The Privacy Officer will review the incident to determine potential criminal activity underlying the incident or whether there was systematic or willful noncompliance with state or federal policy concerning data security or student privacy. The Privacy Officer will review all evidence related to an incident, collect more as necessary, and determine whether additional action is necessary in addition to resolution of the incident (e.g., referral for further enforcement, or recommendations to pursue criminal prosecution, as in the case of malicious data breaches).

WVNET or Institutional Incidents
For incidents discovered at WVNET or the institutional level, the Commission and Council Privacy Officer will work with WVNET or the institution to help direct and oversee the response and investigation efforts. The Privacy Officer will coordinate with WVNET or the institution to ensure that an adequate response effort is underway.

The WVNET or institutional representative will provide the Privacy Officer with regular updates about the progress of all privacy incident response efforts, serve as a liaison between the Privacy Officer and WVNET or institutional leadership as necessary, and ensure that all necessary documentation relating to the incident is produced, disseminated to relevant stakeholders, the Privacy Officer , and archived as appropriate. The Privacy Officer will work with WVNET or the institution to ensure that proper handling and closing of the incident occur.

For WVNET or institutional incidents best handled by a state-level response, the Privacy Officer will be responsible for initiating the incident response plan, providing resources, and leading the efforts from the initial identification of the incident through the post-incident review of lessons learned.

Data Stewards and Technical Governance Group

Some members of the data steward and technical governance group serve as experts for data security, confidentiality, and privacy. When appropriate, certain members of this group may assist the Privacy Officer in leading and coordinating responses for certain incidents.

Incident Response Team

The incident response team supports the Privacy Officer by assisting with in assessing and classifying the incident, determining the appropriate immediate response, and managing all other aspects of response and mitigation, up to and including a post-incident review and recommendations for changes in policy or practice to prevent similar incidents in the future.

The size and composition of the team will vary based on the circumstances of the specific privacy incidents they will manage. The team will consist primarily of Commission and Council employees, and other identified staff, as appropriate.

When needed, the Privacy Officer may request external state agencies to participate on the response team to provide additional depth of knowledge or expertise and breadth of experience to the containment, investigation, and resolution process.

The Commission and Council's general counsel will be an ex officio member of all incident response teams formed at the state-level; the Privacy Officer will be an ex officio member of incident response teams formed at WVNET or the institutional level as applicable.

Senior IT Systems Administrator

When warranted, the Privacy Officer may request assistance from the Commission's Senior IT Systems Administrator in the incident response process to examine the risk and magnitude of harm to internal systems due to the privacy incident. The IT systems administrator also assists with systems and network reviews and forensics. If warranted the Privacy Officer will recommend the use of forensics services offered by the state privacy office as part of BRIM insurance.

Official Communications

Given the likelihood that some privacy incidents, particularly those that are data breaches, may require notification of the affected parties and/or the general public, the Executive Vice Chancellor for Administration and the Director of Communications will be involved in the privacy incident response process when warranted.

At a minimum, the Chancellor(s) and the Executive Vice Chancellor for Administration will be kept informed of the key facts of all major incidents and the progress of the response efforts so that he or she may accurately respond to or refer questions from news media.

When notification of students, or other individuals is required due to the nature or scope of a data breach, the Privacy Officer will relate the details to the Chancellor(s), the Executive Vice Chancellor for Administration, the Director of Communications and the Commission and Council legal staff so they can collaborate and provide support and assistance in creating appropriate letters and other messages explaining the incident and next steps families may need to take.

Data Governance Representatives

Staff and stakeholders who serve in various capacities within the Commission and Council data governance structure will be informed of all privacy incidents and data breaches as applicable. They may be asked to serve on incident response teams or to provide guidance for appropriate and effective mitigation of threats and potential systemic weaknesses.

Local Law Enforcement

Local law enforcement officials may need to be involved in investigations and prosecutions, depending on the circumstances of the individual incident. If computers, storage media, or other equipment are stolen, the individual from whom they were taken will need to file a police report. If the circumstances surrounding an incident or data breach warrant criminal prosecution, county prosecutors will need to bring appropriate charges in court.

State and Federal Offices

If warranted, other state and/or federal officials may need to be consulted or notified about data breaches involving electronic student records or systematic noncompliance with state or federal law. Depending on the nature and circumstances of the incident, offices to be consulted may include the WV Auditor's Office, the WV State Privacy Office, the U.S. Department of Education (USED), the Federal Bureau of Investigations (FBI), or the U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security.

The Commission and Council reserves the right to involve any other state or federal offices or officials it deems necessary to adequately investigate, litigate, or resolve any privacy incident. Other stakeholders may be involved in the response process depending on the specific circumstances of any given privacy incident and kept informed of progress toward full resolution via regular updates.

In the case of privacy incidents or data breaches involving the Statewide Longitudinal Educational Database, all partner agencies will be notified and kept informed of progress toward full resolution. The Privacy Officer will develop annual reports about the privacy-related activities of the Commission and Council, including privacy incidents handled during the year.

6. Incident Classification

All incidents are classified into levels depending upon the type of unauthorized disclosure and the nature of the information disclosed. Depending on the incident, it is possible that it may not fit into one of the classification levels. The Privacy Officer will determine the proper classification.

> **Level 1** – level 1 incidents include unauthorized internal disclosures of or access to data and information that does not include any sensitive PII about the individual(s) whose records were disclosed.
>
> These incidents may be referred to the appropriate division head by the Privacy Officer for management and response. If this is the case, the Privacy Officer will provide suggestions and resources to assist with training or education to prevent similar incidents in the future.
>
> > **Level 1-A** – level 1-A incidents include authorized disclosure of data and information that may or may not include sensitive PII about individual(s) but was transmitted in an unauthorized manner (Ex. Sending PII via email).

Level 2 – level 2 incidents include unauthorized internal disclosures of or access to data and information that does include sensitive PII about the individual(s) and unauthorized external disclosures of or access to PII that does not include any sensitive PII.

Level 3 – level 3 incidents involve unauthorized external disclosures of or access to data and information that does include sensitive PII about individual(s). Unauthorized disclosure of or access to any data and information containing sensitive PII is considered a data breach, regardless of whether the disclosure was internal or external.

All level 3 incidents will be immediately reported to the WV State Privacy Office the Chancellor(s), the Executive Vice Chancellor for Administration, and the data governance implementation team.

All incidents, regardless of classification level, must immediately be reported in accordance with the procedures described below in the incident reporting section.

7. Incident Reporting

Privacy incidents are discoverable through many mechanisms such as routine network monitoring, suspicious activity found during database activity monitoring, security audits, loss or theft of equipment, or failure to comply with policies and procedures. It is possible for anyone to find or suspect that an incident has occurred.

It is vital that all suspected incidents be investigated. It is the responsibility of all employees, contractors, vendors, researchers, authorized representatives, other agents, and/or stakeholders to report any suspected or confirmed privacy incidents to the Privacy Officer for immediate investigation and handling.

Incident reports should, to the extent possible, use established forms (see Appendix A) and shall include as much information as possible. At minimum, they must include the following.

- Location the incident occurred.
- Date the incident occurred (if known) and the date the incident was discovered.
- Description and list of the specific information disclosed, including database field names if appropriate.
- Number of individuals whose information was affected or disclosed.
- How the incident happened and indicate if the incident was intentional or the result of an accident/negligence.
- How the incident was discovered.
- Name of who reported the incident and if appropriate, the name and title or role of the individual who disclosed the information.
- Description or list of the person/people to whom the information was disclosed.
- What steps or actions, if any, have been taken to repair or correct the issue.
- Detailed description of the incident, and any other information that may be relevant.

All incidents—whether suspected or confirmed—must be reported to the Privacy Officer. When employees, contractors, vendors, researchers, authorized representatives, other agents or stakeholders discover an incident, the Commission and Council Privacy Officer should be notified as quickly as possible but **absolutely no later** than 24 hours following the discovery.

8. Response Procedures

The following response procedures may not always happen in a linear process as described and situations may require additional steps, multiple steps occurring simultaneously, or other deviations from the steps listed. This is to be expected based on the nature of the incidents.

All incidents will be fully investigated, and all evidence relating to the incident must be preserved and/or archived for future investigation in accordance with best practices. Technology staff will be consulted to ensure appropriate preservation of electronic evidence. When a privacy incident involves out-of-state individuals, additional investigation may be required, and that state's breach and notification policy reviewed.

9. Detect and Identify

Upon receiving an incident report, the Privacy Officer will determine if an incident has occurred or if it can be considered a non-incident. If an incident has been determined to have occurred, the Privacy Officer will implement the incident response process, review the initial report and information, ask follow-up questions, and make a preliminary assessment as to the severity and classification of the incident.

The Privacy Officer will inform the incident response team members and report the privacy incident to the WV State Privacy Office when applicable. The Privacy Officer may also inform appropriate agency leaders or other officials to alert them to the incident and the initiation of a formal response when applicable.

Evidence Collection and Documentation

A formal incident log will be established to document the incident, its causes, the response, and potential steps for future prevention and/or deterrence efforts. The log must be updated regularly throughout the response process (i.e., each time a meeting is held, or decision is made) and must be sufficiently detailed to allow for use in similar incidents.

The Privacy Officer may consult the Commission and Council general counsel if applicable, to determine appropriate strategies and procedures for collecting, handling, storing, and documenting the custody of any evidence that may need to be collected throughout the response and investigation, particularly if the evidence may become part of a criminal prosecution.

10. Contain and Recover

Following determination of a level 1-A, 2 or 3 incidents, the incident response team will assemble per the Privacy Officer's direction to begin reviewing available information and devising an appropriate strategy for containment and response.

The composition of teams will vary based on the nature and severity of the incident and may include, as needed, experts in other areas such as data governance, technology, communications, human resources, and legal issues.

As the team is assembling and beginning to review information, the Privacy Officer will supervise efforts to contain the incident and recover any exposed PII. If steps have already been taken to contain the incident and retrieve the information, all efforts should be documented.

If containment and PII retrieval efforts have not yet been started, the Privacy Officer will direct and document that work immediately. This includes determining and assessing the most appropriate course of action to contain the incident and mitigate risks. The course of action shall be designed to (1) contain the incident, particularly those of an ongoing nature; (2) stop or limit further data loss or exposure; and (3) mitigate potential adverse effects for all those affected.

As part of assessing the appropriate course of action, the potential benefits and risks associated with the proposed actions, including whether any action may introduce additional vulnerabilities or pose political risks should also be assessed.

Documentation will include evidence or statements of belief about whether the exposed PII will be misused or further disseminated. All individuals who will be responsible for implementing any part of the plan will be provided with the full plan to ensure a comprehensive understanding of how their responsibilities are related to or associated with other steps or components of the process.

11. Investigate

During the contain and recover process, the incident response team will review all available information about the incident, including its potential causes and impacts. The team will determine the immediate cause and explore potential related vulnerabilities or threats. Assistance from subject matter experts should be sought as needed.

As necessary, the incident response team may gather additional information in order to document the incident more completely. Such efforts may include additional requests for documentation or evidence; interviews with subject matter experts, key personnel, or others with knowledge of the incident, and other reasonable and necessary steps. It is vital that the gathering of additional information should not prevent or delay action.

Given the available information about the cause of the incident and the nature and extent of the exposed information, the incident response team will analyze possible risks to affected individuals,

data systems, equipment, institutions, and other external agencies. The team will then reassess the severity and scope of incident given all available information and the assessment of risk.

The incident response team, working with other staff members with knowledge of the incident, will prepare a complete inventory of the data exposed during the incident or data breach. To the extent possible, a complete list of the individuals whose information was disclosed should be created. This list should include as much contact information as possible.

Identify Related Threats or Vulnerabilities

Throughout the investigation, the team should work to identify any other potential threats or vulnerabilities to the system, the data, or any processes used to enter, store, manage, or extract information.

The incident response team should remain mindful that threats or vulnerabilities could include inadequate awareness or training among staff, insufficient security procedures, insufficient capacity for comprehensive security, limited resources, and other factors.

Initial Briefing Report

The incident response team will prepare and submit an initial briefing to the Privacy Officer regarding the nature and scope of the incident and the preliminary identified risks.

Update and Advise

Situational status updates will be provided to the Privacy Officer who will keep key personnel at the appropriate levels abreast of the status. The frequency with which updates are provided may vary based on the level of the incident as well as its scope and potential for negative publicity and/or political ramifications.

The Privacy Officer will engage division heads, including legal representatives, in discussions about necessary processes if criminal activity is suspected and law enforcement involvement may be warranted.

The Privacy Officer will advise all other staff aware of the incident to keep all details in confidence until notified otherwise.

Preserve Evidence and Update Documentation

The Privacy Officer will ensure that the incident log/record is fully updated throughout the response process. Other relevant documents (e.g., emails, reports) will be collected and preserved appropriately and in accordance with established protocol.

In cases involving breaches of electronic systems, the Privacy Officer will consult directly with agency technology experts to determine appropriate ways to capture and preserve information about the systems at the time the compromise was discovered.

12. Communicate

The Privacy Officer will ensure that all relevant employees, stakeholders, and leaders have been fully informed about incident and briefed on the ongoing investigation and response efforts.

For level 1-A, 2, and 3 incidents, the Privacy Officer will report the incident to the state privacy office and ensure that the Executive Vice Chancellor for Administration and the Director of Communications are fully aware of all pertinent facts and able to answer questions from members of the media, should the need arise.

As needed, the Director of Communications should review the communications plan with the Privacy Officer and Executive Vice Chancellor for Administration to prepare for managing public notification and media inquiries.

Determine Notification Needs

For Level 1-A and 2 incidents, the Privacy Officer will determine whether notification of affected individuals is required. For Level 3 incidents, which involve the external disclosure of sensitive PII, notification of affected individuals is often required. Final notification determination is dependent on many factors including state or county residence.

The Privacy Officer will collaborate with the State privacy office, the Executive Vice Chancellor for Administration and the Director of Communications to determine appropriate notification methods and message content based on the incident type, scope, and severity and the stakeholder group affected.

It is possible that some affected individuals may not be directly reachable, therefore plans must include reasonable methods for providing information for these individuals.

It will be determined whether a toll-free number and/or incident-specific email address is needed to assist with communication and notification efforts. The possibility of hosting an incident-specific informational website, if the scope and severity of the incident warrant such a resource will also be considered. Incident type specific templates may be developed and made available for phone calls, email messages, letters, presentations (e.g., PowerPoint), and informational websites.

Based on information gathered during the initial stages of the response, the team will develop a contact list for individuals directly affected by the incident (i.e., individuals whose information was exposed). At this step, the team will work to confirm the accuracy of the available contact information.

Notify Affected Stakeholders

When notification is required, affected individuals must be notified about the incident as soon as possible and as is required by state breach laws. Normally this will be no longer than 10 calendar days after the incident is discovered and the identities of affected individuals are determined.

The Privacy Officer will consult State or federal resources to determine notification requirements. In general, notifications must provide as much information about the incident as is reasonable, including what happened, the likely cause, what staff are doing to resolve the issue, and how the incident may affect the individual being notified. Notifications should also describe any steps or actions affected individuals may need to take to proactively protect or monitor their identity and personal records.

Press releases, press conferences, media advisories, and any other mass communication efforts should, to the extent possible, be timed to coincide with or follow notification of individuals. Circumstances may dictate different priorities and shorter timelines; guidance from the State privacy office should be followed in planning all mass communications. The Executive Vice Chancellor for Administration and the Director of Communications should serve as the key representative for all comments to the public or the media.

Report to Key Leaders and Other Officials

All notifications that are required to be provided to the governor, other governmental officials, or other external stakeholders should be concise while providing sufficiently descriptive information about the incident, including the cause(s), the scope and severity, number of individuals affected, and the work being done to respond to the incident and mitigate potential harms.

The Privacy Officer will provide regular updates or reports for key internal leaders and stakeholders (e.g., administrators, technology personnel, staff who may have been the victims of equipment theft or hacking) to keep them fully informed of the incident and progress toward resolution.

As needed, and in consultation with the Privacy Officer, the State privacy office, Commission and Council leadership, and general counsel, the team will determine whether federal officials need to be notified of the incident. Federal officials may include the Family Policy Compliance Office (FPCO) at the U.S. Department of Education; the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security; the Federal Bureau of Investigations (FBI), or other federal offices or officials.

If warranted, law enforcement officials (to include police and local prosecuting attorneys) will be contacted to assist with the response to any incidents involving hacking or malicious attacks and all incidents involving the loss or theft of equipment.

Police reports are needed for all cases involving the theft of equipment or other resources and materials containing PII.

Communicate with the Public

If the incident is widespread, has potential high visibility, may have political ramifications, or involves particularly sensitive data, the Privacy Officer will present available information to the Chancellor(s), Executive Vice Chancellor for Administration, and the Director of Communications to determine whether public notification or reporting is needed.

As needed, the Commission and Council will communicate broadly with the public about the incident. The communication team should enact a pre-established crisis communication plan to avoid confusion, distribution of misinformation, or other preventable mistakes in the midst of the response.

The Chancellor(s), the Executive Vice Chancellor for Administration, and the Director of Communications should lead all efforts in communicating with the public. Other representatives or spokespeople for the Commission and Council should follow all guidance from the Executive Vice Chancellor for Administration relating to communicating with external audiences.

Preserve Evidence and Update Documentation

The Privacy Officer will ensure that the incident log/record is fully updated throughout the reporting process. Other relevant documents (e.g., emails, reports, notifications) will be collected and preserved appropriately and in accordance with established protocol.

All notifications (including copies of letters, emails, or phone scripts; websites created for the incident; etc.) will be archived for future reference. The Privacy Officer will ensure that all evidence is collected and preserved appropriately and in accordance with established protocol.

13. Review and Repair

The Privacy Officer and the incident response team will conduct a full review of the investigation and of the incident. The Privacy Officer and the incident response team will determine whether an internal review (conducted by internal staff) is appropriate or whether and external/third-party review is warranted. Different types of incidents may require different types of reviews based on causes, scope or severity, and potential political or public relations implications.

The incident response team should examine and document any lapses between the actual occurrence and the discovery of the incident as well as the time from incident discovery to reporting to the Privacy Officer. Throughout the investigation, the team should continue documenting and preserving evidence according to established protocol and/or instructions from the Privacy Officer or general counsel.

The team should review and assess the effectiveness of initial response efforts. Any preliminary strengths and weaknesses in the response should be fully explored and documented.

The incident response team should review and assess the potential threats or vulnerabilities to the system, the data, or any processes used to enter, store, manage, or extract information that was found through the investigation and document these.

To the extent possible, the team should classify threats or vulnerabilities as high- or low-priority based on their severity and the likelihood that they may result in future privacy incidents.

Develop and Implement Plan for Repairs

In addition to the immediate response processes that were undertaken, the incident response team should develop a plan (or set of plans) to make comprehensive repairs or corrections to the systems or processes that contributed to the incident. The team should also plan for corrections to any related vulnerabilities identified through the investigation.

The team may collaborate with subject matter experts to develop appropriate, comprehensive, and responsive plans. Plans for repairs (or components of those plans) should be prioritized based on the severity of the threats and the likelihood that future incidents may arise as a result of the vulnerabilities.
The team should develop short-term and long-term timelines to make updates or corrections for factors that may not be immediate threats but that could present risks in the future.

The Privacy Officer will collaborate with administrators or other leaders to ensure that immediate action is taken to repair system vulnerabilities or security lapses identified as high-priority or likely to result in future incidents.

Repair plans should be implemented by appropriately qualified staff or contractors. The Privacy Officer will be provided with updates about the progress of repairs on an ongoing basis until all repairs are successfully completed.

Determine Appropriate Sanctions

If appropriate (and in accordance with state, federal, and other relevant policies and procedures), the Privacy Officer will collaborate with general counsel to determine what appropriate sanctions or penalties might be for individuals, agencies, or other agents (e.g., contractors, vendors) who caused or substantially contributed to the cause of the incident.

In consultation with general counsel, the Privacy Officer, and Commission and Council leadership should discuss and determine whether any civil action against individuals, agencies, or other agents may be appropriate or warranted.

The incident response team, administrators, and staff who were directly involved with an incident should cooperate and collaborate with law enforcement and local prosecutors as warranted in any criminal investigations (e.g., for theft of equipment, electronic hacking or other malicious attacks). Criminal prosecution may be warranted in cases of malicious attacks or theft of property. Such determinations will be the exclusive purview of local prosecuting attorneys.

The incident response team, in consultation with the Privacy Officer, general counsel, and appropriate Commission and Council leadership, should discuss and determine whether a formal complaint should be filed with the FPCO for any violations of FERPA by individuals, agencies, or other agents.

All repair plans should be distributed to appropriate internal staff for documentation and prioritization of work efforts. The Privacy Officer will ensure that the incident log/record is fully

updated throughout the repair process. Other relevant documents (e.g., emails, reports, plans, work orders) will be collected and preserved appropriately and in accordance with established protocol.

14. Recover

Verify Success of Repair Efforts

The Privacy Officer will work to confirm and document that all repair efforts have been successful. Confirmation may include checks of electronic systems to ensure they are fully functional and verification that new procedures or processes work as intended. Staff should reestablish all operations after making necessary repairs to systems and processes.

The Privacy Officer will verify that individuals have received appropriate training and/or reminders of their responsibilities concerning PII and personal records. As necessary and warranted, the Privacy Officer may ask staff to provide formal assurances of compliance or improved conduct in the future.

The Privacy Officer will provide all affected and involved stakeholders with an update to report that the incident has been successfully resolved. As necessary, a summary of actions to date may be included as part of that notification.

If warranted, the Privacy Officer or other designated staff member should follow up with individuals whose information was inappropriately disclosed to determine whether they have any lasting needs or concerns resulting from the incident. The team should collaborate with those stakeholders to develop an appropriate plan to address those needs or concerns.

Follow Through with Sanctions

At this time, appropriate personnel should levy any sanctions or penalties deemed appropriate. The person responsible for this task will vary depending on the nature or the sanction and the individual or entity against whom it will be levied. The team should determine who that person should be.

Any other actions determined to be appropriate (e.g., filing complaints with the FPCO, pursuing criminal or civil action through the courts) should be implemented. A staff member should be designated to follow up on these actions and provide ongoing reports to the team and relevant administrators until a final resolution is reached.

The Privacy Officer will ensure that the incident log/record is fully updated throughout the recovery process. Other relevant documents (e.g., emails, reports) will be collected and preserved appropriately and in accordance with established protocol.

15. Access and Learn

It is vital that all lessons learned are appropriately shared and documented. This will help in the prevention of future privacy incidents and with future incident response plan trainings. These lessons will also help to update preparedness activities.

Debrief Incident (Causes, Identification, and Response)

The Privacy Officer will convene the full incident response team to review the incident and all actions taken in response. The team will assess the effectiveness of the response effort. Strengths and weaknesses will be fully documented.

The team will detail and document the lessons learned from both the incident itself and from the response effort. These lessons learned will be included with the incident documentation and be used in the next incident response training if applicable. The team will develop recommendations to assist with future incident prevention and response efforts.

Review and Revise Policies, Procedures, and Practices

The Privacy Officer and the incident response team will review existing policies, procedures, plans, and practices in light of lessons learned. The team will recommend any necessary changes and/or new policies, procedures, plans, and practices to improve security or better ensure privacy.

Proposed changes in Commission or Council policy and procedures will be developed, reviewed, and approved through the standard policy revision process. Based on lessons learned, there may also be recommendations to change, add, or otherwise modify the current incident response processes to improve response to future incidents.

Share Lessons Learned with Stakeholders

The Privacy Officer will lead the incident response team in sharing lessons learned from the incident and the response process with other stakeholders. Such stakeholders may include personnel within the Commission and Council, other state agencies, and public higher education institutions.

If new tools or resources are developed as a result of the incident response, those tools or resources should be shared broadly with all Commission and Council divisions.

Provide Training and Support

As warranted, the Privacy Officer will coordinate with other staff to ensure that training materials and resources for the processes or systems affected by repairs are updated appropriately.

Training materials and resources pertaining to any policies, procedures, or practices related to the cause of the incident will also be reviewed and updated as needed in light of lessons learned.

The Privacy Officer will provide training and support for all divisions and employees as well as other official agents as changes are implemented and made following incident response. The Privacy Officer will communicate on an on-going basis with stakeholders regarding new or revised policies, plans, procedures, and processes.

As needed, the Privacy Officer will provide reminders about existing policies, plans, procedures, and processes that may be related to the incident (e.g., policies that were not followed correctly) or that are identified as potential risks or vulnerabilities.

Update and Archive Documentation

The Privacy Officer will ensure that all incident documentation is complete, up-to-date, and inclusive of all necessary components, including:

- Causes of the incident.
- How the incident was discovered.
- Findings of the full investigation.
- Actions taken to repair the incident (including dates/times and names of actors).
- Current system status if applicable (post-repair and recovery)..
- Other relevant information (including whether legal action was pursued)
- Names of the incident response team members.

The incident response team will create a concise summary of the incident from identification through resolution and lessons learned, and a formal summary of lessons learned and recommendations for the future. These documents will be given to the Privacy Officer for appropriate distribution.

All documentation and records must be archived according to established protocol.

16. Enforcement

Commission and Council employees found to have violated these guidelines or any other privacy-related procedures or regulations may be subject to disciplinary or corrective actions, including, but not limited to, revocation of privileges up to and including termination of employment. Certain violations, misuse, or disclosures of confidential information may include civil and/or criminal penalties.

Contractors, vendors, researchers, and other agents working for or on behalf of the Commission and Council who are found to have violated these guidelines or any other privacy-related procedures or regulations will be subject to reprimands and action commensurate with the violation, including termination of contracts or pursuit of other legal action.

Appendix A

Commission and Council Incident Report

Please complete the following form with as much detail as possible. **DO NOT** include actual personally identifiable information (PII) in this form.

Return completed form to Melanie Baker at Melanie.Baker@wvhepc.edu or Dr. Zornitsa Georgieva at Zornitsa.Georgivea@wvhepc.edu

Name: (Name of Person Completing Form)		Date: (Date form completed)	
Location of incident:		Date incident occurred:	
Please briefly describe the incident:			
Please list the specific **type** of information disclosed below. Include database field if appropriate. ***(DO NOT list actual data that was disclosed here)***			
Number of individuals whose information was disclosed:		Number of individuals who received disclosed information *(if known)*:	
Describe how the incident occurred below. Include if the incident was intentional or the result of an accident/negligence:			
How was the incident discovered?			
Name of individual who disclosed the information *(if known)*:			
Division of individual who disclosed the information *(if known)*:			
List individual(s) to whom the information was disclosed:			
Please list the steps (if any) that have been taken to repair or correct the issue below.			
Please give a detailed description of the incident and include any other information that may be relevant to the investigation below.			