Data Breach Response

UNIVERSITY POLICY #81

Authority: BOG Policy 60: Information Technology Governance
Approval Date: 10/06/21
Effective Date: 10/06/21
Revision History:
President's Signature: On File

SECTION 1: Purpose and Scope

1.1 The purpose of this Policy is to provide a process to report suspected thefts involving University Data ("Data"), and Data breaches or exposures (including Unauthorized Access, Use, or disclosure), ("Breach Incident") to appropriate individuals; and to outline the response to a confirmed Breach Incident based on the type of Data involved.

1.2 This Policy applies to all computer systems, network devices, and any additional systems and outputs containing or transmitting Data.

SECTION 2: Policy

2.1 **Reporting Suspected Breach Incident.** Any individual who suspects that a Breach Incident has occurred **must** immediately provide a description of what occurred via email to privacyofficer@westliberty.edu or by calling 304-336-8495. This email address and phone number are monitored by WLU's Privacy Officer who will investigate all reported Breach Incidents to confirm if a Breach Incident has occurred. If a Breach Incident has occurred, the Privacy Officer will follow the appropriate procedure depending on the class of Data involved.

2.1.1 If the Breach Incident is a suspected theft, WLU's Campus Police shall be notified by the Privacy Officer. They will determine whether a local law enforcement agency should be contacted based on the location and details of the incident. If a local law enforcement agency is contacted, the name of the agency and the report number should be provided to WLU via the methods of contact outlined above.

2.1.2 Failure to report a suspected Breach Incident is a violation of this Policy.

2.2 **Confirmed Breach Incident.** As soon as a Breach Incident containing Data is identified, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of WLU, that site will be contacted to have the information removed as soon as possible.

2.2.1 The Chief Information Officer will be notified of the Breach Incident and will inform the Director of Media Relations as soon as possible. The WLU IT Department (IT) will analyze the Breach Incident to determine the root cause, work with the appropriate parties to remediate the root cause and examine any involved systems to ensure the integrity of all Data within those systems.

2.2.2 Failure to report an actual Breach Incident is a violation of this Policy.

SECTION 3: Response Team

3.1 **Breach Incident Response Team**. The Privacy Officer will chair a Response Team to handle the Breach Incident. The Response Team will include members from: IT, the Director of Media Relations, the Office of the General Counsel, the affected unit or department that uses the involved system or output or whose Data may have been breached or exposed, and additional departments based on the Data type involved and as deemed necessary by the Privacy Officer.

3.1.1 This team will provide information regarding how the Breach Incident occurred, the types of Data involved, the WLU Data Classification, any protective measures around the involved Data (such as encryption), and the number of internal/external individuals and/or organizations impacted. The Director of Media Relations will handle all communications about the Breach Incident. IT will work with the appropriate parties to remediate the root cause of the breach or exposure.

3.2 For any Breach Incident involving information listed below, a representative from the listed areas will be included on the Response Team:

Financial information, including but not limited to credit card numbers, bank account numbers, investment information, grant information, and budget information	**VP of Finance, Controller,** **Director of Financial Aid**
Information about individual employees, including but not limited to social security numbers	**Human Resources**
Student financial information	**VP of Finance, Controller, VP Student Affairs**
Student information protected by FERPA	**VP Student Affairs, Registrar, Provost**
Student health information	**VP Student Affairs, Director of Student Health**
Student information not listed above	**VP Student Affairs, Marketing Communication Services**

Research data	**Provost**
PII concerning faculty	**Provost, CHRO**
PII concerning donors or unreleased information about gifts received	**Director of Advancement**
Payroll information	**VP of Finance, Controller**

3.3 The Response Team should consider the following when responding to a Breach Incident.

3.3.1 The following materials may need to be developed to handle the Breach Incident including: Web pages, Notification letters, Press releases, Q&A for media, Q&A for other potential responders (Law Enforcement for example).

3.3.2 Alert university leadership teams (President, Cabinet, Information Technology, Deans) so they understand what is being done to address the Breach Incident and are apprised of status. The order and frequency of updates to these groups will be determined by the Privacy Officer.

3.3.3 All available information about the Breach Incident, including both information that has been confirmed and information that is suspected, will be provided to the Response Team. As new information is discovered, it will be provided to the Response Team as quickly as possible.

3.3.4 Daily conference calls to checkpoint progress and obstacles are tremendously helpful in keeping things moving and sharing information.

3.3.5 Size and severity (likelihood of fraud) of the incident may warrant different actions, i.e., whether credit monitoring is affordable and/or appropriate.

3.3.6 Track the amount of time that has passed between the Breach Incident, discovery of the Breach Incident, and notification of affected individuals. While none of these steps are necessarily long, each one of them adds to the number of days to notification.

3.3.7 If contracts need to be negotiated to provide services to the affected individuals, those negotiations should begin immediately. Check to see if previously negotiated contracts can be applied to the situation (especially for credit monitoring).

3.3.8 Depending on the number of individuals impacted, it can take some time to assemble mailing address information for large groups. Begin pulling this data immediately. A percentage of the initial mailings will be returned as undeliverable so the number of deliveries to attempt and methods to pull additional delivery information should be identified.

SECTION 4: Policy Adherence:

4.1 Any employee who violates this Policy will be subject to appropriate disciplinary action.

4.2 Any student who violates this Policy will be subject to appropriate disciplinary action in accordance with the Student Code of Conduct.

4.3 Any individual affiliated with the University who violates this Policy will be subject to appropriate corrective action, including, but not limited to, termination of the individual's relationship with the University.

4.4 The University's Chief Information Officer and/or the Privacy Officer will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

4.5 Responsibility for interpretation of this Policy rests with the President and Chief Information Officer and/or the Privacy Officer.

SECTION 5: Definitions

5.1 **"Data Breach"** means the unauthorized access and acquisition of unencrypted and unredacted computerized data or physical records that compromise the security or confidentiality of personal information maintained by the West Liberty University.

5.2 **"Unauthorized Access"** means a person gains logical or physical access without permission to a University network, system, application, data, or other resource.

5.3 "**Unauthorized Use**" means when Data is used by someone who does not have permission to use the Data and/or in a way that interferes with an individual's privacy either under the relevant privacy law or in breach of the WLU Acceptable Use Policy.

5.4 **"University Data"** means data created, received, maintained, or transmitted by or on behalf of the University through the course of its academic, administrative, research, or outreach activities. **Examples of University Data include, but are not limited to:**

5.4.1 **Personally Identifiable Information (PII)**. Data that specifically identifies an individual, including, but not limited to: Social Security number, driver's license number, credit card numbers, bank account information, employee performance or salary information, student grades, disciplinary information, account passwords, or Protected Health Information (PHI).

5.4.1.1 **Protected Health Information (PHI):** Data as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). PHI under the US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a third-party associate) that can be linked to a specific individual.

5.4.2 **Education Records:** Data as defined by the Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA governs access to educational information and records by potential employers, publicly funded educational institutions, and foreign governments.

5.4.3 **Customer Information:** Data as defined by the Gramm-Leach-Bliley Act (GLB Act, GLBA or the Financial Modernization Act of 1999), requiring financial institutions to explain how they share and protect their customers' private information.

5.4.4 **Card Holder Data:** Data as defined by the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an information security standard that tells organization's how to handle branded credit cards from the major card schemes.

5.4.5 **University Sensitive Data**. Sensitive Data based on departmental/internal standard operating procedures including, but not limited to, budgetary, departmental, or University planning information, intellectual property, system credentials, personnel records, unpublished grant proposals/research data, and non-public financial, procurement, health/safety, audit, insurance and claims information.

5.5 "**WLU Data Classification"** means the classification of Data based on its level of sensitivity and the impact to the University should that Data be disclosed, altered, or destroyed without authorization. To define how much protection different types of Data require, WLU has adopted a three-tier classification system:

Level 1: Confidential information governed by state or federal privacy regulations and data protected by confidentiality agreements, including but not limited to, FERPA, HIPAA, GLBA, PCI, confidentiality agreements, non-disclosure agreements, and Attorney Privileged Data.

Level 2: University Sensitive Data that must be protected for ethical or privacy reasons.

Level 3: General information that may be sensitive in nature, such as a person's title, email address, or other published information that exists in the public domain.

Questions about this Policy: If you have questions about this policy, please contact the Privacy Officer at privacyofficer@westliberty.edu.