UNITECH TRAINING ACADEMY

Data Breach Incident Response Plan

Purpose

This document outlines the incident response plan for addressing a data breach at Unitech Training Academy. The purpose is to minimize the impact of the breach on students, faculty, staff, and the school's reputation while ensuring compliance with relevant laws and regulations.

Responsibility

The Director of IT is responsible for the administration of this plan.

The IT Department will support the operation and execution of the Data Breach Incident Response plan at the direction of the Director of IT, the CEO, and COO.

Third party assistance may be requested for data recovery, forensic analysis, legal counsel, and public relations for items above and beyond the scope of ability or resources.

Procedure

1. **Incident Identification and Reporting**
   - Any individual who suspects or identifies a data breach must immediately report it to the Director of IT and/or the Incident Response Team. This includes the IT Department and COO.

     Director of IT – David Morvant – dmorvant@unitechta.edu – (337) 303-5205

     IT Specialist – Dillon Morvant – djmorvant@unitechta.edu – (337) 368-9268

     IT Specialist – Daniel Motes – dmotes@unitechta.edu – (337) 280-7432

     IT Systems Specialist – Royal Robins – rrobins@unitechta.edu – (504) 460-9212

     COO – Chris Bordes – cbordes@unitechta.edu - (337) 349-6722

2. **Initial Response**
   - Upon receiving a report of a data breach, the IRT will convene immediately to assess the situation.
   - The primary objectives of the initial response are to contain the breach, preserve evidence, and mitigate further damage.
   - The IT Department will isolate affected systems and networks to prevent unauthorized access.

3. **Investigation and Assessment**
   - The IRT will conduct a thorough investigation to determine the scope and nature of the breach.
   - The IT Department will analyze system logs, conduct forensic analysis, and identify compromised data.
   - The COO will contact legal counsel to assess legal and regulatory implications and provide guidance on compliance requirements.
   - The Director of IT will give an assessment report to the COO to be discussed with the CEO.
   - Messaging will be prepared for internal and external personnel.

4. **Notification**
   - Depending on the nature and extent of the breach, affected individuals, regulatory authorities, and other relevant parties will be notified in accordance with applicable laws and regulations.
   - If the data breach is determined to be significant, the breach will be reported to the following agencies:
     - Cybersecurity and Infrastructure Security Agency – report@cisa.gov – 888-282-0870
     - Federal Student Aid – cpssaig@ed.gov - Cybersecurity Breach Intake Form
     - Federal Bureau of Investigation – neworleans.fbi.gov – 504-816-3000
   - Notification methods may include email, letters, phone calls, or public announcements.

5. **Response Coordination**
   - The Director of IT will coordinate with relevant stakeholders, including the COO, CEO, legal, communications, human resources, and external vendors or consultants.
   - External resources may be engaged to assist with data recovery, forensic analysis, legal counsel, and public relations.

6. **Remediation and Recovery**
   - The IT Department will implement remediation measures to address vulnerabilities and prevent future breaches.
   - Efforts will be made to restore affected systems and data from backups.
   - Additional security measures, such as enhanced monitoring or encryption, may be implemented to safeguard sensitive information.

7. **Communications and Public Relations**
   - The COO will manage external and internal communications throughout the incident response process.
   - Regular updates will be provided to affected individuals, staff, students, parents, regulatory authorities, and the media as appropriate.
   - Transparency and accountability will be emphasized to maintain trust and credibility.

8. **Post-Incident Review**
   - Following resolution of the breach, the Director of IT will conduct a comprehensive review to evaluate the effectiveness of the response and identify areas for improvement.
   - Lessons learned will be documented, and recommendations will be implemented to enhance incident response capabilities.

9. **Training Awareness**
   - Ongoing training and awareness programs will be conducted to educate staff, faculty, and students about data security best practices and the importance of incident reporting.
   - Regular drills and simulations will be conducted to test the effectiveness of the incident response plan and ensure readiness for future incidents.

10. **Documentation and Compliance**
    - All actions taken during the incident response process will be thoroughly documented for regulatory compliance and legal purposes.
    - Compliance with relevant laws, regulations, and contractual obligations will be a top priority throughout the incident response process.

11. **Revision and Updates**
    - This Data Breach Incident Response Plan will be reviewed and updated regularly to reflect changes in technology, regulations, and organizational structure.
    - Feedback from post-incident reviews and exercises will be incorporated to continuously improve the effectiveness of the plan.