Data Incident Response Plan

The Importance of Securing Electronic Data

Much of the data stored or transmitted via Knox's computing equipment and network is confidential. Unauthorized access to this data may constitute a violation of federal statutes such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and other laws and College policies designed to protect privacy. A breach in data security that compromises personal information can lead to identity theft, putting members of the Knox community at risk, and exposing the College to litigation. Unauthorized access to other confidential data, though not usable for identity theft, may nonetheless have serious legal, financial, or public relations implications for the College.

Preventing Data Breaches

The duty to secure protected or confidential data (PCD) is shared by all members of the Knox community. PCD should not be accessed, copied, stored, downloaded, transmitted, or used unless it is essential for College business. When PCD is no longer required it should be securely disposed of. Every effort should be made within and between offices and departments to minimize the volume and numbers of copies of PCD.

PCD should not be stored on laptops or other mobile devices for longer than necessary and should be encrypted at all times. Devices and physical storage devices that contain PCD, whether mobile or not, should be secured by authentication, encryption, and/or well as by physical means (security cables, locked cabinets, etc.). PCD should be under the physical control of the custodian at all times. If it is required that PCD be left unattended, it should be securely stored in a locked container such as a hotel room safe, trunk or glove compartment of an automobile.

Care should be taken to ensure PCD is not left unattended or unsecured on desks, work surfaces and computer screens. When leaving an area, lock the computer, remove PCD from work surface and store in locked container, or close and lock the door of the office.

The Chain of Responsibility

Under certain circumstances, confidential electronic data — such as student names, email addresses, or other information — may need to be conveyed to individuals or groups who are not employees of the College. These may be vendors, contractors, professional organizations, (internal) student organizations, or others. In these circumstances, the College must require the recipient of the data to abide by the same (or stricter) guidelines to protect the data from unauthorized access or abuse. This chain of responsibility must extend to any third parties (or beyond) to whom the confidential data might be further conveyed.

Individuals and offices who are stewards or custodians of PCD shall have sufficient knowledge of the volume, access methods, location, and nature of the data in their care to assist in determining the scope of a breach. For example, the volume and type of PCD exposed, storage location and access methods to the PCD, and details on method of storage (encrypted or clear text).

Responding to Digital Data Security Breaches

Despite explicit guidelines for securing confidential electronic data, breaches may still occur. At such times, it is important that the College respond as quickly and professionally as possible. Computer thefts, should be reported immediately to the Director of Campus Safety (x7979 or 309-341-7979). Campus Safety will assess the nature of the breach and will secure and attempt recovery of any physical assets.

Campus Safety will notify the Vice President for Information Technology Services, Vice President for Finance and Administrative Services, and the Vice President for Communications of any suspected data breach. These individuals will determine the appropriate response and may utilize the Breach Response Guidelines and Procedure outlined in this document.

Breach Response Guidelines and Procedure

1. Documentation (Campus Safety)

- identification of the person reporting the breach (name, contact info, etc.)
- basis for belief that a breach has occurred
- location, timeframe, equipment, and/or other details of breach
- preliminary identification of confidential data that may be at risk
- identification and recovery of physical assets

2. Communication

- Vice President for Communications
- Vice President for Information Technology Services
- Vice President for Finance and Administrative Services
- Director of Campus Safety (physical access to facilities and/or physical assets)
- President and other senior officers (depending on sensitivity, scope of nature of data exposed)
- Legal counsel (depending on sensitivity and scope of data exposed)
- Law enforcement (depending on the nature/scope of theft)
- Beazley (Data Breach insurer and access to services retained by Knox to assist with breach notification and forensics)
- If credit card data has been breached, notify bankcard holder within 24 hours of confirmed breach discovery

3. Investigation

- Identify if there is an ongoing vulnerability and take immediate steps to redress
- Conduct preliminary forensic analysis. Retain outside assistance as required.
- Prepare inventory of data at risk
- Determine if exposed data were encrypted
- Identify security measures that were defeated and by what means

4. Assessment

- Identify affected individuals at risk of identity theft or other harm
- Assess financial, legal, regulatory, operational, reputational, and other potential institutional risks

5. Remediation

- Implement password changes and other security measures to prevent further data exposure
- Determine if corrupted data can be restored from backups; take appropriate steps recover data and restore business functions.
- Determine if risk associated with exposed data can be neutralized by changing account access, ID information, or other measures

6. Notification

Based on regulatory requirements and other factors, Senior Officers, in consultation with legal counsel, if needed, determine whether notifications are required (or advisable) for:

- Government agencies
- Affected individuals
- Knox community
- Business partners
- Public

If Senior Officers determine that notifications are needed:

- The Vice President for Information Technology Services will notify Beazley who will coordinate notifications to affected individuals. Unless directed otherwise by law enforcement, such notifications will be made without delay.
- The Vice President for Finance and Administrative Services will notify government agencies and business partners.
- The Vice President for Communications will coordinate notifications to the Knox community, the public, and others as necessary.

Communications will address the following points:

- Nature and scope of breach
- General circumstances of the breach (e.g., stolen laptop, hacked account or database etc.)
- Approximate timeline (e.g., date of breach discovery)
- Steps the college has taken to investigate and assess the breach
- Any involvement of law enforcement or other third parties
- Appraisal of any misuse of the missing data
- College-provided *credit-watch* service for affected individuals (1-2 years)
- Beazley steps taken on behalf of affected individuals
- Steps that the College is taking to prevent future breaches of this nature

Post-Incident Follow-Up

In the wake of a data security breach, Knox will:

- Ensure that missing data cannot be used to access further information or cause harm in other ways to Knox's electronic or other resources
- Pursue with law enforcement all reasonable means to recover lost data and equipment
- Review and modify as needed all procedures and policies governing security policy and procedure, systems and software management procedures, access to information, etc., to prevent future data breaches of a similar nature
- Take appropriate corrective or punitive actions if staff negligence or behavior contributed to the incident