Collin College Technology Services (CC-TS)
Electronic Data Security - Incident Response Plan (IRP):

The Importance of Securing Electronic Data

Much of the data maintained, stored, or transmitted via Collin College's technology resources and computing equipment is confidential. Unauthorized access to this data may violate federal statutes such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and other laws designed to protect privacy. A breach in data security that compromises personal information can lead to identity theft, putting members of the Collin College (CC) community at risk and exposing the College to liability or litigation. Though not used for identity theft, unauthorized access to other confidential or protected data may have profound legal, financial, or public relations implications for the College.

Preventing Electronic Data Breaches

The task of protecting confidential electronic data is shared by all members of the Collin College community who have authorized access to such data. Confidential data should not be accessed, copied, stored, downloaded, transmitted, or used unless it is essential to conduct College business or as otherwise authorized.

Confidential data should not be stored on laptops or mobile devices for longer than necessary and should be encrypted when not in use. Devices that contain confidential data, whether mobile or not, should be secured by strong authentication (e.g., multiple levels of passwords) and physical means (security cables, locked cabinets, etc.). CC-issued technology resources and mobile devices should never be put into checked luggage when traveling.

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 authorized to receive such information. In these circumstances, the College must require the data recipient 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 confidential data might be further conveyed.

Responding to Data Security Breaches

Despite explicit guidelines for securing confidential electronic data, breaches can still occur. At such times, the College must respond as quickly and professionally as possible. Computer thefts should be reported **immediately, and no later than within 24 hours,** to the Collin College Technology Cybersecurity Department (ext. 5769 or (972) 881-5769). The steps that the Cybersecurity Office will take in the event of a data security breach are as follows:

1. **Determination of the nature and scope of a breach or potential breach**

    - Identify the person reporting the breach (name, contact info, etc.)
    - Record of the location, timeframe, and apparent source of the breach
    - Preliminary identification of confidential data that may be at risk
    - Identify the steps that were taken to mitigate the breach

2. **Communication**

    - Chief Information Officer (CIO) or Chief Information Security Officer (CISO)
    - Director of Emergency Management (Depending on the nature/scope of the attack)
    - District President and Cabinet members (depending on sensitivity and scope of data exposed)
    - CC Chief of Police or other Law Enforcement (depending on the nature/scope of the attack)
    - Campus Vice President and Provosts (VPP) (depending on the nature/scope of the attack)
    - General Counsel or External Legal Counsel (depending on sensitivity and scope of data exposed)
    - Cybersecurity Insurance Provider (or company retained by CC to assist with breach notification)
    - Senior Vice President (SVP) of External Relations (depending on sensitivity and scope of data exposed)
    - If credit card data is involved, notify the bank card holder within 24 hours of confirmed breach discovery
    - Department of Information Resources (DIR) if the breach meets required reporting laws.

3. **Investigation**

    - Identify ongoing vulnerability of data to exposure from breach source (take immediate steps to address)
    - Conduct preliminary forensic analysis (retain outside assistance as needed)
    - Prepare an inventory of data at risk
    - Determine if exposed data were encrypted
    - Identify security measures that were defeated (and by what means)
    - Identify security measures that mitigated the breach, if any

4. **Assessment of breach**

    - Identify affected individuals at risk of identity theft or other harm
    - Identify categories of exposed data, including disclosure of isolated or multiple data points
    - Assess financial, legal, regulatory, operational, reputational, and other potential institutional risks

5. **Remediation**

    - Implement immediate security measures to safeguard other CC data
    - Implement password changes and additional security mitigating actions to prevent further data exposure
    - Determine if exposed or corrupted data can be restored from backups; take appropriate steps
    - Determine if the value of exposed data can be neutralized by changing account access, ID information, or other measures

6. **Notification**

Based on regulatory requirements and other factors, the District President, CIO, Cabinet Members, and SVP of External Relations (in consultation with General Counsel or Legal Counsel as appropriate) determine whether notifications are indicated for:

- Government Agencies
- Law Enforcement Agencies
- Affected Individuals
- Collin College community
- Business Partners
- Public
- Other

If the District President, Cabinet members, CIO, and SVP of External Relations determine that notifications are needed:

- The CIO or Chief Financial Officer (CFO) will notify the cybersecurity insurance company, which will coordinate notifications to affected individuals. Unless directed otherwise by law enforcement, such notifications will be made without delay
- Either the CISO, CIO, or CFO will notify government agencies and business partners depending on the nature of the breach
- The SVP of External Relations will coordinate notifications to the Collin College community, the public, and others as necessary

Communications will address the following points as needed:

- Nature and scope of the breach
- General circumstances of the breach (e.g., stolen laptop, hacked database, etc.)
- Approximate timeline (e.g., date of breach discovery)
- Steps the College has taken to investigate, assess, or mitigate the breach
- Any involvement of law enforcement or other third parties
- Appraisal of any misuse of the missing data
- Cybersecurity Insurance steps on behalf of affected individuals
- Actions that the College is taking to prevent future breaches of this nature

Post-Incident Follow-Up

In the wake of a data security breach, Collin College will:

- Take steps to prevent any additional access to further information or cause harm in other ways to Collin College'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 governing systems administration, software management, database protections, access to hardware, etc., to prevent future data breaches of a similar nature
- Take appropriate actions if employee or student misconduct or negligence or other's behavior contributed to the incident
- Modify procedures, software, equipment, etc., as needed to prevent future data breaches of a similar nature
- Implement additional training or mandatory security measures for personnel or affected departments.

Related Policies, References, and Attachments:

An index of approved CC-Technology Services Information Security Procedures (CC-TS ISPs) can be found on the CC Information Technology Services ISP website at https://www.collin.edu/security/.

Implementation Information

Review Frequency:	Annually
Responsible Person:	SVP – Campus Operations
Approved By:	Abe Johnson, Ed. D.
Approval Date:	02/09/2022

Revision History

Version:	Date:	Description:
1.0	02/09/2022	Initial document
1.1	10/28/2022	Annual Review – No Changes Required.
1.2	11/09/2023	Annual Review – No Changes Required.