UNIVERSITY of DENVER	**UNIVERSITY OF DENVER** **POLICY MANUAL** **DATA BREACH PROTOCOL**

Responsible Department: Information Technology **Recommended By:** SVC Business and Financial Affairs, Registrar **Approved By:** Chancellor	**Policy Number** IT 2.30.065	**Effective Date** 6/8/2023

I. INTRODUCTION

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures, including unauthorized access, use, or disclosure, to appropriate individuals and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved. Examples of breaches might include loss or theft of hard copy notes, USB drives, computers or mobile devices, unauthorized persons gaining access to a laptop, email account or computer network, or sending an email with person data to the wrong recipient.

The University of Denver collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (accidental or deliberate) to avoid a data protection breach that could compromise security. Compromise of information may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial costs.

II. POLICY OVERVIEW

The University is obliged to have a framework in place designed to ensure the security of all personal data during its lifecycle. This policy sets out the procedures to ensure a consistent and effective approach is in place for managing data breaches and information security incidents across the University. This policy relates to all personal and special categories (sensitive) data held by the University or held by third parties working on behalf of the University regardless of format. This policy applies to all faculty, staff, students, and volunteers at the University. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the University. The objective of this policy is to contain any breaches, minimize risks associated with breaches and consider what action is necessary to secure personal data and prevent further breaches.

III. PROCESS OVERVIEW

A. Determination of Breach

1. Determine exactly what information was compromised, including but not limited to: name, addresses, SSNs, ID numbers, credit card data, grades;
2. Determine how the incident occurred, including but not limited to: school official having control and responsibility for the information compromised;
   a. Reference the Information Technology Division's Incident Response policy for guidance on information gathering techniques.
3. Determine appropriate response team (i.e. Registrar, Risk, Counsel, IT, Safety, Data owner);
4. Determine if FSA (ED) should be notified
   a. https://ifap.ed.gov/fsa-cybersecurity-compliance
5. Determine if EU GDPR Articles 33 and 34 breach notifications apply (e.g. notification of EU supervisory authority);
6. Determine if the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 or Section 13407 of the HITECH Act apply;
7. Determine if state(s) privacy laws are invoked
   a. Colorado (https://coag.gov/resources/data-protection-laws)
8. Determine if institutional policies and procedures were breached, including but not limited to: organizational requirements governing access (user names, passwords, PINS, etc.); storage, transmission, destruction of information from education records.

B. Communication of Breach

1. Report the incident to law enforcement authorities as needed; (Counsel and CIO)
2. Determine appropriate communications:
   a. To Marketing and Communications
      i. To affected data owner (i.e. student, staff, faculty or other)
      ii. To University executives

C. Cause of Breach and Notification/Actions

1. Identify all affected records and data owners;
2. Retrieve data and take steps to prevent further disclosures;
3. Determine cause of breach (e.g. lack of monitoring and/or oversight);
4. Conduct a risk assessment and identify appropriate physical, technological and administrative measures to prevent similar incidents;
5. Determine if Red Flag (identity theft) procedures are required;

https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business#how

6. Determine if disciplinary actions are warranted;
7. Notify students of the Office of Inspector General's website that describes steps to take if suspicious of being a victim of identity theft:
   a. http://www.ed.gov/about/offices/list/oig/misused/idtheft.html
   b. http://www.ed.gov/about/offices/list/oig/misused/victim.html

IV. DEFINITIONS/REFERENCES

References:

FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure - 34 CFR 99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. Direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Colorado Notification Requirements:
https://coag.gov/resources/data-protection-laws/

PTAC Checklist:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

General Data Protection Regulation:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Breach Notification Rule, 45 CFR §§ 164.400-414

The Health Information Technology for Economic and Clinical Health (HITECH) Act

Revision Effective Date	**Purpose**
6/28/2021	*Minor revisions*
6/8/2023	*Minor revision to add HIPAA and HITECH Act references*