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

ation could result in harm to individuals, reputational damage, detrimental effect on service provision, and legislative non-compliance.

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 state(s) privacy laws are invoked
   a. Colorado (https://coag.gov/resources/data-protection-laws)
7. 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.

6. Determine if disciplinary actions are warranted;
7. 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 Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and

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

Revision Effective Date	**Purpose**
6/28/2021	*Minor revisions*