CAMERON UNIVERSITY
Sensitive Data Protection Policy

Policy Statement

This policy describes the procedures to be followed to ensure safeguards are followed for handling sensitive data by Cameron University faculty, students and employees. The University handles vast amounts of personal data on students and employees in day-to-day operations. Some of this data is not sensitive and is publicly available. The University has legal and ethical obligations to ensure the data is managed in a manner to minimize risks of unauthorized access. This policy outlines the guidelines for safely handling sensitive data and actions taken for violations of mishandling sensitive data or unauthorized disclosure of sensitive data.

Contents

Who Should Know This Policy

President
Vice Presidents
Deans
Department Chairs
Directors
Faculty
Other Accounting/Finance Personnel
Students
Other Groups
All Employees

Responsibilities

Responsible for Policy
University Officer Responsible — Vice President for Academic Affairs

Procedure

STATEMENT OF PURPOSE: In support of the above policy statement, the following procedures and information are provided:

1.0 Definitions

1.1 **Sensitive Data**–any information that is protected by Federal law, State of Oklahoma law and University policy. Some examples include:

- Family Educational Rights and Privacy Act (e.g., student and transcript information)
- Health Insurance Portability and Accountability Act (e.g., health, medical or psychological information
- Social Security Number (SSN)
- Credit card number or banking information
- Tax information
- Information that can be used to facilitate identity theft, (e.g., birth date, mother's maiden name, place of birth, first school attended)
- Passwords
- Personal Identification Number (PIN)
- Human subjects research data
- University restricted data
- ID pictures
- Donor information
- Mailing lists
- Financial aid information

1.2 **Non-Sensitive Data**–any information that is lawfully made available to the public from records of another federal or local agency. e.g., telephone directory information.

1.3 **Information Security Incident**–an information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of incidents include activities such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Unauthorized changes to system hardware, software, data, or networks

2.0 General Guidelines

2.1 Do not collect or store SSN unless it is required by university policy, federal or state agency and there is no other option to be used for unique identification purposes. If you must store and report SSN for any reason, you must provide details and receive clearance from the University's Information Security Officer at (580) 581-6735 before proceeding.

2.2 Always use University assigned ID numbers unless a SSN is required by university policy, federal or state agency. If you must use the SSN for any reason, you must provide details and receive clearance from the University's Information Security Officer at (580) 581-6735 before proceeding.

2.3 Sensitive data should be stored in as few places as possible and should always be stored on central University servers. There should be very few exceptions. You must know if you have sensitive data stored outside servers maintained by the University and notify the Information Security Officer at (580) 581-6735.

2.4 Do not store data on departmental computers that duplicate data on central University servers.

2.5 Do not collect and store sensitive data unnecessarily or for convenience purposes.

2.6 Do not store sensitive data on mobile devices, such as CD, DVD, laptops, notebooks, USB devices, cell phones, etc., that are easily stolen or compromised.

2.7 Do not send sensitive data via email as it is not secure.

2.8 Practice a clean desk policy by securing all sensitive data, documents, CD-ROM, DVD- ROM, USB drives, etc., under lock and key when you leave your desk.

2.9 Lock your computer (CTRL+ALT+DELETE) anytime you leave your desk.

2.10 NEVER share your password or give it to anyone claiming to be from ITS.

2.11 Should you have any reason to believe sensitive data may have been compromised or released, immediately contact the University's Information Security officer at (580) 581-6735.

2.12 Sensitive data must be encrypted anytime it has to be uploaded to another site. The website MUST use HTTPS or SSL encryption. If you are required to use FTP or Telnet, you must use the encrypted versions of these protocols, e.g., SSH and SFTP. There are no exceptions. If you need assistance, contact the Help Desk at 580-581-2454.

2.13 All hard copy sensitive data must be shredded. If the department does not have a shredder, they should contact the Business Office to reserve a time for shredding sensitive documents.

3.0 Notification

A member of the University community who becomes aware of an information security incident involving an Academic or Administrative Computing System should immediately contact the University's Information Security Officer at (580) 581-6735.

Contacts

Policy Questions: Information Security Officer, (580) 581-6735

Forms

In support of this policy, the following forms are included:

Policy History

Policy

Issue Date: April 25, 2012
Reviewed, no revision: February 2016
Reviewed, no revision: June 6, 2023