CAMERON UNIVERSITY

Information Security Program Policy

Policy Statement

At Cameron University, we are committed to we are committed to ensuring the confidentiality, integrity, and availability of our information assets. Information is a vital and a key enabler for achieving our strategic and educational goals. Protecting this this information from unauthorized access, disclosure, alteration, destruction, and disruption is paramount to our success and reputation.

Contents

- Who should know this Policy?
- Responsibilities
- Procedure
- Contacts
- Forms
- Policy History

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 (VPAA)

Procedure

STATEMENT OF PURPOSE:

The Information Security Program of Cameron University is designed to safeguard the confidentiality, integrity, and availability of information assets within the university's environment. This program establishes guidelines, roles, and responsibilities to ensure the protection of sensitive data, compliance with relevant regulations, and the proactive management of information security risks. The Information Security Program at Cameron University is intended to protect the university's information assets while enabling the efficient and effective use of technology to support the institution's core mission. By fostering a culture of security awareness and implementing robust controls, we aim to minimize risks and ensure the ongoing confidentiality, integrity, and availability of information.

1.0 Definitions

1.1 **Confidentiality:** We will protect sensitive information from unauthorized access, ensuring that it is disclosed only to authorized individuals for legitimate purposes.

1.2 **Integrity:** We will maintain the accuracy, consistency, and reliability of our information assets. Any unauthorized modification or alteration will not be tolerated.

1.3 **Availability:** We will ensure that information and information systems are available to authorized users when needed. We will implement measures to prevent and minimize disruptions.

1.4 **Compliance:** We will comply with all applicable laws, regulations, and contractual obligations related to information security. Non-compliance is unacceptable and may result in disciplinary actions.

1.5 **Responsibility:** All employees, contractors, and third-party partners are responsible for adhering to this program. Training and awareness programs will be provided to ensure everyone understands their roles and responsibilities.

1.6 **Continuous Improvement:** We will regularly review and update our information security measures to adapt to evolving threats and technologies. Feedback and lessons learned will be used to enhance our security posture.

2.0 Information Security Organization

2.1 Information Security Officer (ISO)

2.1.1 The ISO is responsible for the overall management and implementation of the Information Security Program.

2.1.2 The ISO will collaborate with stakeholders to develop, maintain, and update security policies, standards, and procedures.

2.1.3 The ISO will oversee security awareness and training initiatives.

2.1.4 The ISO will serve as the primary point of contact for information security incidents.

2.2 Information Security Team

2.2.1 The Information Security Team will assist the ISO in implementing and maintaining the Information Security Program.

2.2.2 The team will conduct regular risk assessments and vulnerability scans to identify potential threats.

2.2.3 The team will collaborate with other departments to address security gaps and implement necessary controls.

2.2.4 The team will provide training and awareness programs to educate faculty, staff, and students about information security best practices.

3.0 Risk Management

3.1 IT Services will conduct periodic risk assessments to identify and prioritize potential threats and vulnerabilities.

3.2 Risk assessments will be reviewed periodically and updated as necessary to reflect changes in the environment.

3.3 Mitigation strategies will be developed and implemented to reduce the impact and likelihood of identified risks.

3.4 Regular monitoring and review of security controls will be performed to ensure their effectiveness.

3.5 An Incident Response Plan will be established to minimize the impact of security incidents and ensure timely recovery.

3.6 Controls will be implemented to address vulnerabilities and protect information assets from unauthorized access or disclosure.

4.0 Data Protection and Access Controls

4.1 Access controls will be implemented to ensure that only authorized individuals can access sensitive information.

4.2 User access privileges will be granted based on the principle of least privilege.

4.3 Strong authentication mechanisms, such as multi-factor authentication, will be used to protect user accounts.

4.4 Encryption will be employed to protect sensitive data both in transit and at rest.

4.5 Cameron University will conduct a periodic inventory of collected data, 4.5.1 All stored data at Cameron University is stored on-premises.

4.5.2 Data inventory will include, but not be limited to; location, record type, metadata.

5.0 Information Security Monitoring and Incident Response

5.1 IT Services will implement appropriate monitoring tools and techniques to detect and respond to security incidents.

5.2 Logs of incidents will be sent to a security incident and event management (SIEM) tool for review and monitoring by the Incident Security Team

6.0 Incident Response and Management

6.1 The Incident Response Plan will outline the steps to be taken in the event of a security incident.

6.2 Incident response roles, responsibilities, and escalation procedures will be defined.

6.3 Security incidents will be investigated and mitigated to minimize their impact.

6.4 Lessons learned from security incidents will be used to improve incident response procedures and preventive measures.

7.0 Security Awareness and Training

7.1 Ongoing security awareness and training programs will be conducted for students, faculty, and staff.

7.2 Training will cover topics such as data protection, phishing awareness, social engineering, and password security.

7.3 Regular communication channels will be used to provide updates on emerging threats and best practices.

7.4 Training programs will be tailored to the specific needs and roles of different user groups.

8.0 Compliance with Laws, Regulations, and Policies

8.1 The Information Security Program will comply with all applicable laws, regulations and University policies

8.2 Regular reviews and updates will be conducted to ensure compliance with evolving requirements.

8.3 Audits and assessments will be performed to validate compliance and identify areas for improvement.

9.0 Physical Security

9.1 Physical access controls will be implemented to protect information systems and infrastructure.

9.2 Sensitive areas such as server rooms and data centers, will be secured with appropriate measures.

9.3 Equipment and devices containing sensitive information will be properly secured to prevent theft or unauthorized access.

10.0 User Responsibilities

10.1 All users are responsible to maintaining the confidentiality, integrity, and availability of information assets.

10.2 Users must comply with applicable laws, regulations and University Policies.

10.3 Users should report any suspected program violations to the appropriate channels for further investigation.

11.0 Vendor Management

11.1 Vendors providing on-premises and cloud-based data services will be carefully evaluated for their security controls and compliance.

11.2 Contracts and agreements with vendors will include provisions for data protection and security.

11.3 Regular assessments and audits of vendors' security practices will be conducted to ensure ongoing compliance.

12.0 Continuity and Disaster Recovery

12.1 Business continuity and disaster recovery plans will be established to minimize disruptions and ensure the timely recovery of information systems.

12.2 Data backups will be performed regularly and tested to ensure their integrity and availability.

13.0 Update

13.1 This program will be periodically reviewed and updated to reflect changes in risks to faculty, staff, students and affiliates at Cameron University with respect to Red Flags and identify theft. Any incidents in the current year will be reported to the Vice President for Academic Affairs on or before December 31st of the current year. Reports will include:

13.1.1 The number of detected issues

13.1.2 The response to and outcome of such issues; and

13.1.3 The areas that have been identified as requiring updates or modifications to this program.

14.0 Oversight

14.1 Oversight for this program will be provided by the Vice President for Academic Affairs. He/she shall ensure that the program is implemented and updated. He/she will also provide the relevant affected units with training concerning these rules.

Contacts

Policy Questions: Director of Information Technology Services, (580) 581- 2255

Policy History

Policy

Issue Date:	11/29/23
Revised:	4/18/25