TITLE: INFORMATION TECHNOLOGY SECURITY

POLICY STATEMENT:

Red Deer College (RDC) manages information technology resources to ensure that information assets and information systems are identified, secured, protected, and accessible throughout their life cycle.

RDC protects the security of information assets and information systems by establishing standards and procedures for authorized access and asset protection.

RDC conducts regular evaluations to ensure that current security safeguards, policies, standards and procedures are effective in protecting information assets and information systems.

RDC establishes standards and procedures for the acquisition, security, implementation and use of information assets and information systems.

PURPOSE:

The purpose of this policy is to:

- Ensure information systems are designed, implemented, and maintained to support the mission of RDC.
- Protect information assets and information systems from unauthorized access and disclosure, from inappropriate modification and from loss and inappropriate or accidental destruction.
- Ensure information is accessible and available to individuals with proper authorization, where authorization is established and based on business need.
- Ensure compliance with the Freedom of Information and Protection of Privacy Act of Alberta and other applicable laws and legislation.

SCOPE:

This policy applies to all learners, employees, volunteers, contractors, and any other individuals who create, access, or use information assets and information systems owned by, in the custody of, or under the control of RDC.

PRINCIPLES:

1. Decisions involving information assets and information systems are conducted in consultation with the Information Technology Department.
2. All individuals share responsibility for the security and protection of RDC information assets and information systems including any networks, computers, software, and data over which the individual has use or control.

DEFINITIONS:

Business Unit: a logical element or segment of the College representing a specific business function. Also known as a department, service, division, School, program, or functional area.

Information Assets: data in any form or media that is placed into a meaningful context for users. These assets contribute to the College's knowledge base and help to achieve strategic goals. They may be collected in relation to business, research or scholarly activity. Examples may include paper and electronic documents; spreadsheets; email; web content; databases such as student, human resources and financial information systems; other databases; content in learning management systems such as Blackboard; images; and video and other content in physical and digital form.

Information Systems: the infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support the college. Also referred to as information services or information technology.

GUIDELINES:

1. **Electronic Access Control:** Individuals require proper authorization to access information assets and information systems. The owner and/or designate of the information asset or the information system is responsible for determining permissions for access In addition, the user of an information asset or information system may request access of permission from the owner based on business need. The Information Technology Department is responsible for maintaining a roster of permissions.
2. **Physical Access Control:** Physical access controls are employed to protect areas containing information storage/processing facilities, information assets, and information systems.
3. **Physical Asset Protection:** Information assets stored in electronic form in information systems owned by, in the custody of, or under the control of the College, are protected against storage media deterioration and software/hardware obsolescence that may leave information inaccessible over time.
4. **Compliance:** Individuals are held accountable for knowing and complying with RDC information technology policies, guidelines, standards, and procedures. Non-compliance with this policy constitutes misconduct. Individuals may be denied access to College information assets or information systems and may be subject to penalties under College regulations, collective agreements, and provincial and federal law.

PROCEDURE:

1. The Information Technology Department publishes and maintains the *Information Technology Standards Manual* on the RDC portal, with required information technology procedures.

OFFICER RESPONSIBLE: Vice President of College Services

RECOMMENDING AUTHORITY: Service Council, upon recommendation from Deans' Council

CONSULTATION FOR REVIEW: Chief Information Officer, Deans' Council, Service Council

POLICY REVIEW DATE: June 2020

EFFECTIVE DATE: July 15, 2016

REVISION HISTORY: June 1, 2015
July 15, 2016

RELATED POLICIES:

- Communication and Information Systems Acceptable Use
- Freedom of Information and Protection of Privacy
- Information and Technology Management
- Intellectual Property
- Risk Management

CONNECTION TO BOARD POLICIES:

All RDC policies support relevant Board of Governors policies.