Privacy, information security, and identity management policy

Policy statement

The policy of Bow Valley College (the College) is to ensure that its information privacy, security, and identity management strategy:

1. Incorporates information privacy, security and identity management concepts into the design and implementation of new information technology initiatives and in its daily operations.
2. Manages information as an asset and its management
   2.1. Protects information throughout its lifecycle.
   2.2. Ensures information confidentiality, integrity and availability.
   2.3. Maintains trust between the College and its information users.
3. Identifies roles and responsibilities related to managing information privacy, security and identity management.
4. Is in compliance with legal, regulatory, and ethical obligations in respect to how it protects and controls access to the College's business information and its related technology.
5. Is routinely evaluated and, when needed, adapted to assure continued compliance to legal, regulatory, and ethical obligations related to privacy and security of information and related technology.
6. Incorporates alignment with industry standard information privacy and security frameworks in its daily operations and audit practices.

Purpose

The purpose of this policy is to outline at a high level the College's approach to ensuring the privacy and security of information under its custodianship. As well, this policy will show how identity management is utilized to protect information and related technology from unauthorized access.

This policy applies to College related business information that is created, stored, processed, or transmitted on Information Technology Resources (ITR) supported by the College. This policy applies to College related business information that is created, stored, processed, or transmitted on non-College resources.

Scope

This policy applies to College community members including the Bow Valley College Board of Governors, Executive Management, employees, third party vendors, contractors, and learners.

Principal objectives

The principal objectives of the Privacy, Information Security, and Identity Management Policy are to:

1. Ensure that privacy, information security and identity management concepts are incorporated into the design and implementation of information technology initiatives and in daily operations, by:
   1.1. Providing channels for communicating privacy obligations to stakeholders.
   1.2. Supporting information governance to provide an enterprise approach to information and its related technology.
   1.3. Ensuring privacy, information security and identity management concepts are included in risk, change and project management processes.
   1.4. Ensuring information security and privacy risks are assessed and correlated against industry standard information security and privacy frameworks.

2. Ensure that information is managed as an asset and its management: protects information privacy throughout its lifecycle; ensures information confidentiality, accuracy, availability and integrity; and, maintains trust between the College and its information users through:
   2.1. Open, transparent and understandable decision-making related to information and access management processes.
   2.2. Identifying information users and determining how information users are given an identity to access the College's information and related ITR.
3. Identify roles and responsibilities related to managing information privacy and security and identity management:
   3.1. The Bow Valley College Board of Governors, Executive Management, Information Technology Services and IT Security are responsible for creating a governance structure that provides direction and processes for managing business information appropriately.
   3.2. Information Technology Services and IT Security are responsible for managing identity assurance and information and its related technology in alignment with the direction of the governing bodies.
   3.3. Management roles are responsible for handling identity assurance, and information and ITR under their jurisdiction in compliance with legal, regulatory, and ethical obligations.
   3.4. Employees are responsible for managing information and related technology under their control in compliance with legal, regulatory, and ethical obligations.
   3.5. Individuals are responsible for information generated on College systems for their personal use.
4. Ensure the policy is in compliance with legal, regulatory, and ethical obligations in respect to how it protects information and controls access to the College's technology by:
   4.1. Maintaining and managing roles and access for information users.
   4.2. Enabling procedures and processes that incorporate best practices and compliance with regard to identity assurance and information classification.
   4.3. Identifying procedures for reporting and managing a security breach of College business information and its related technology.
   4.4. Ensure that the College routinely evaluates and, when needed, adapts processes to assure continued compliance to legal, regulatory, and ethical obligations.

Severability clause
If any one of the statements in this document proves to be invalid or unenforceable it will not undo the validity of the remaining statements. The College reserves the right to correct a disputed statement in such a way that it does not modify the overall original intent of the document.

Compliance

Employees, contractors, and learners are responsible for knowing, understanding, and complying with Bow Valley College policies, procedures, and any other attached documentation that relate to their position, employment, or enrolment at the College.

Definitions

Business information:
Information that is solicited or created as a part of a business activity taken on behalf of the College.

Identity management:
A method of protecting information from unauthorized access through processes that ensure that individuals are who they say they are.

Information security:
The protection of information from a wide variety of threats in order to ensure business continuity, minimize risk and maximize return on investments and opportunities.

Privacy:
The right of an individual to be secure from unauthorized collection, use, and disclosure of information about oneself.

Data sheet

Accountable officer
VP Strategy and CIO

Responsible officer
Lead, IT Security
Director, Information Technology Services

Approval
President and CEO

Contact area
Information Technology Services

Relevant dates

Approved	Board of Governors: BOG200618-04
Effective	July 2021
Next review	June 2022
Modification history	• Rebranded 2021
Verified by	Office of the President, March 2022*

Associated policies
Code of Conduct (200-1-1 & 500-1-1)
Electronic Communications Policy (300-2-13)
Enterprise Architecture Policy (300-2-8)
Enterprise Risk Management Policy (600-1-4)
Information and Technology Management Governance Policy (300-2-6)
Information Management Policy (300-2-9)
Print and Imaging Management Policy (300-2-12)
Records Management Policy (200-1-8)
Technology Management Policy (300-2-7)

Directly related procedures
Privacy and Information Security Breach Procedure

Directly related guidelines
Control Objectives for Information and related Technology (CoBIT)
Bow Valley College Records Retention and Disposal Guideline
Provincial PSS Information & Technology Management (ITM) Control Framework