

Policy Information	
Policy No:	AD-IT-6.04
Approved by:	Executive Committee
Approval Date:	June 22, 2022
Executive Responsible:	Vice President, Finance and Corporate Services
Administrator Responsible:	Chief Information Officer
Date of Next Review:	June 2027

IDENTITY AND ACCESS MANAGEMENT

Policy Statement

This policy describes how access to applications and systems required to engage in CNC related duties and activities is initiated, evaluated, granted, reviewed, and removed.

Purpose / Rationale

This policy reinforces CNC's commitment to protecting individuals' personal information while ensuring users have access to the applications and systems needed to perform their roles at CNC. This access is managed throughout the onboarding, position change, and offboarding stages of employee, student, and contractor lifecycles. Managing access ensures institutional data and personal information is accessible only to those who require it to perform their duties and allows the College to maintain an up-to-date and auditable access tracking system.

Scope / Limits

This policy applies to person-based access for all user accounts, licenses, and logins that are provided to students, faculty, employees, contractors, vendors, and volunteers in their engagement with the College. These individuals are referred to as "users" in this policy.

This policy does not apply to permissions used to customize person-based views, functionality, and content within applications and systems.

Principles / Guidelines

1. The College uses Role-Based Access Control (RBAC) rules to assign access to all users.
2. The College will follow the principle of least privilege to ensure users are granted access only to what is required for their specific role.
3. The Information Technology Services (ITS) department administers the RBAC rules and workflows that automate the access management request, review, and approval process.

4. Each user will be assigned a unique username which may not be reused for another individual.
5. Shared and generic accounts for CNC applications and systems are discouraged. Where shared and generic accounts cannot be avoided, their use must be documented and approved by the application or system Approver and ITS.
6. The Office of the Registrar manages and is responsible for student data and lifecycle changes including onboarding and offboarding.
7. Human Resources manages and is responsible for employee data and lifecycle changes including onboarding, offboarding, and position changes.
8. Access requests, approvals, and removals for contractors, vendors, and others external to CNC are the responsibility of the department requesting the external access.
9. The ITS Department is responsible for administering and supporting the technical aspects and infrastructure related to access management.

Legislative and Collective Agreement References

[BC Freedom of Information and Protection of Privacy Act](#)

Links to Other Related Policies, Documents and Websites

Identity and Access Management Procedures

Freedom of Information and Protection of Privacy Policy AD-CO-4.14

Policy Amendment Log

Amendment Number:	Date:
0	June 2022
1	
2	