College of New Caledonia
CNC

Procedure Information	
Related to 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 PROCEDURES

Definitions

Access Management

Governance and processes around how access is granted, managed, and revoked over the lifecycle of a user.

Accounts

Any password protected login for CNC systems and applications, accessed either on campus or remotely.

Approver

A unit or individual who is responsible for approving access requests for systems or applications.

Least Privilege

The principle that requires each user to be granted the minimum set of privileges, or access permissions, needed for the performance of authorized tasks.

Product Owner

A unit or individual who is responsible for managing permissions for systems or applications.

Users

Faculty, employees, students, contractors, volunteers, and any other individuals who use CNC facilities, accounts, email, internet, systems, and services.

Procedures

User Account Provisioning and Management

1. Human Resources (HR) creates employee user profiles in Colleague (CNC’s Enterprise Resource Planning system) and assigns role types to these users.
2. The Office of the Registrar (OREG) creates student user profiles in Colleague and assigns role types to these users.
3. The HR and OREG departments manage employee and student user details throughout the user lifecycle. These details may include department, program, and start and end dates.

4. The user’s role type and user details together determine which systems and applications the user can access and may also determine the permissions available to the user within the systems and applications.
5. The HR and OREG departments will annually review role types and user details to ensure permissions are up to date.

Role Based Access and Workflows

6. Information Technology Services (ITS) manages the Role-Based Access Control (RBAC) rules which define the access permissions granted to each role type in Colleague.
7. ITS manages the automated process that is triggered when user profiles are created or updated. This process grants, changes, and revokes access to users as appropriate.
8. User profiles for external service providers (such as contractors, volunteers, and vendors) are not entered in Colleague and do not follow the automated workflow.
   - 8.1. ITS grants permissions for contractors, vendors, or service providers.
   - 8.2. The department overseeing the work of those external to CNC may request access for these individuals by submitting a request through the ITS Helpdesk Portal.
9. ITS and Product Owners review the RBAC rules annually to ensure access and permissions granted to each role type continue to align with operational needs.

Shared and Generic CNC Accounts

10. Shared and generic CNC accounts are discouraged and must not be used unless required for a specific purpose.
    - 10.1. Where shared and generic CNC accounts are required, the Product Owner, with support from the Approver, may submit the request through the ITS Support Portal.
    - 10.2. These requests are reviewed and approved by IT Services.
    - 10.3. A department’s use of shared and generic CNC accounts must be tracked by the Product Owner and reviewed annually.

Usernames and Passwords

11. A unique username is generated when a user profile is created in Colleague. This username is used for authentication and user access to systems and applications.
12. Users will be prompted to create strong passwords when they first access CNC’s systems and applications using their new username.

Department Managed Application and System Permissions

13. All systems and applications used at CNC will have a designated departmental Product Owner responsible for managing access.

14. Each system or application will have a designated departmental Approver responsible for reviewing and approving access requests.
15. The Product Owner and Approver may be the same individual.
16. Access permissions to systems and applications managed by departments will be reviewed annually by the Product Owner and Approver to ensure access and permissions are up to date.
17. Any required access or permission changes can be submitted to the ITS Department through the ITS Support Portal.

Links to Other Related Policies, Forms, Documents and Websites

Identity and Access Management Policy
Freedom of Information and Protection of Privacy Policy AD-CO-4.14
ITS Support Portal

Procedure Amendment Log

Amendment Number:	Date:
0	June 2022
1	
2	