Information Security: User Access Provisioning, Deprovisioning and Transfer

Resource reference: **VPS-33-D01**
Status: **APPROVED**
Last revision: **2023-11-01**

Introduction

User accounts control access to Concordia's information systems. This directive's objective is to establish standardized management of both centralized and decentralized identity and access management in compliance with the Information Security Policy (VPS-33) at Concordia. The provisioning, changing, deprovisioning, and auditing of user accounts are within scope of this directive with the goal of ensuring these processes are documented, communicated, authorized, implemented, and monitored in an effective and consistent manner.

This directive is developed and maintained as part of Concordia IT's risk management approach to help Concordia's community efficiently and safely perform their tasks by avoiding and mitigating risks such as:

a. Insufficient or inappropriate access
b. Decreased quality of services
c. Unmet compliance requirements
e. Operational inefficiencies
f. Loss of sensitive data
h. Inefficient utilization of resources
i. Cybersecurity threats

Concordia's Chief Information Security Officer has issued this directive under the authority of Policy Number: VPS-33 - Information Security Policy.

Questions about this directive may be referred to: ciso@concordia.ca.

Definitions

User Accounts – Identifiers such as the Concordia Netname or User Principal Name (UPN) that are uniquely associated with a specific person and allow that person to access eligible services offered by the University.

Centralized identity and access management – A framework of Concordia processes, policies, and technologies such as the IITS-managed Concordia Account Management System (CAMS) that are used to automatically manage user accounts with access privileges granted according to a person's role for identification, authentication, authorization, and audit.

Decentralized identify and access management – Management of user accounts and/or access privileges not managed by Concordia's centralized identify and access management framework.

Identities – Containers that collect and hold all the users' privileges across the enterprise. An identity may contain many user accounts, but there is only one, single identity record per user. Identities are provisioned automatically through source data for each staff, faculty, or student member.

Privileges – Identities and accounts are given rights to IT environments or applications. The level of access is determined by the person's role and the privileges assigned to them.

Principle of least privilege (PoLP) - The principle means giving any users account or processes only those privileges which are essentially vital to perform its intended functions. For example, a user account for the sole purpose of creating backups does not need to install software: hence, it has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked.

Segregation of duties (SoD) principle – The primary objective of this principle is the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users. This principle is demonstrated in the traditional example of segregation of duty found in the requirement of two signatures on a cheque.

Scope

IITS manages the Concordia identity and access management systems for both students and employee identities by assigning privileges based on a person's role, that are used to manage authentication, authorization, and audits for all systems and applications utilizing centralized identity and access management. Faculties, departments, and units must leverage centralized identity access and management wherever possible when managing IT environments and applications.

In cases where the centralized Concordia identity and access management systems cannot be used and accounts or access are created or managed outside the centralized identity and access management systems, the unit's IT application owners and administrators creating or modifying this access must define, document, and follow procedures for access approval, creation, maintenance, and removal based on IITS' standardized templates and procedures.

Roles and Responsibilities

IITS

- Manage all accounts, privileges, and access requests through the centralized Concordia identity and access management systems.
- Maintain a catalog and inventory of IT environments and applications using both centralized and decentralized identity and access management.
- Maintain and provide consultation and support on standardized templates and procedures for access approval, creation, maintenance, and removal.
- Inform the application owners and administrators using decentralized identity and access management when certain changes occur.

- Collect bi-annual audit reports/reviews for each service using decentralized identity and access management and work with IT environment or application owners and administrators to address any discrepancies.
- Regularly review this directive and apply corrective measures.
- Continuously monitor, analyze, and propose improvements for related processes and guidelines.

IT application owners and administrators:

- Define, document, and follow procedures for access approval, creation, maintenance, and removal based on IITS' standardized templates and procedures.
- Manage and track all user accounts and privileges where the central Concordia identity access and management systems is not used.
- Record the provisioning, changing and deprovisioning of access.
- Ensure that privileges are assigned using the principle of least privilege ensuring access is only granted to eligible users requiring it.
- Perform, document, and share user access reviews for audit on a bi-annual basis.
- Ensure that all IT environments and applications are included in the inventory managed by IITS.
- Collaborate with IITS to improve and enforce this directive.

General Policies

1. Wherever possible, Concordia's centralized identity and access management systems must be used when managing access to IT environments or applications.
2. All IT environments and applications must be configured according to Concordia's identity and access management parameters listed below.
3. IITS maintains an inventory of IT environments and applications. Owners of IT environments and applications are responsible for maintaining the accuracy of the records of environments and applications they manage and/or administer.
    a. Queries and modifications to this inventory are requested by emailing ITAM@concordia.ca.
4. All access changes including provisioning, deprovisioning, and transfers must be logged for troubleshooting, monitoring, investigation, and auditing purposes, and kept for at least one year.
5. IITS maintains detailed processes and templates to standardize the user account management for IT environments University-wide.
    a. Process documents, consultation, and support is requested by emailing ITAM@concordia.ca.

Metrics and Controls

A bi-annual access audit review of IT environments and applications using decentralized identity and access management must be conducted for each IT environment or application by its application owner and administrator.

IITS maintains detailed processes to standardize the bi-annual reviews and allows for units to submit their reviews by emailing ITAM@concordia.ca. These reports will be used by the IITS cybersecurity operations team or internal audit to validate the processes and effectiveness.

Identity and Access Management Parameters

- Multi-factor authentication (MFA) should be enabled on all information systems and must be enabled on all information systems accessible by the internet.
- Account locking for failed or suspicious login attempts must be enabled wherever possible.
- Role-based privileges must be enabled wherever possible.
- The principle of least privilege (PoLP) must always be applied.
- All approvals should be done in alignment with the segregation of duties (SoD) principle.
- All temporary access must be granted for the required period only.
- Passphrase or password complexity must meet or exceed the complexity documented in Concordia's passwords and passphrases directive (VPS-33-D03).

Exceptions

Exceptions to this directive must be documented and reported to the office of the Chief Information Security Officer (CISO) by email to: ciso@concordia.ca. Each exceptional instance will be assigned a consultant to perform a risk assessment and assist in the definition of appropriate mitigation measures if required.

Accessibility

Community members with accessibility questions or needs related to this directive are asked to contact the appropriate IITS resource person by emailing iits-accessibility@concordia.ca.

Implementation, audit, and review

Concordia's Chief Information Security Officer (CISO) is responsible for the implementation, review, and approval of this directive. Concordia's CISO initiates a review on an annual or as-needed basis to ensure alignment with both internal and external requirements and regulations.