POLICY ON THE MANAGEMENT OF DIGITAL ASSETS

Effective Date: May 9, 2023

Approval Authority: Vice-President, Services and Sustainability

Supersedes/Amends: June 1, 2013

Policy Number: VPS-32

PREAMBLE

Concordia University's (the "University") Information Technology (as defined below) ecosystem is aimed to provide support to Employees and Students (as such terms are defined below) in the fulfillment of their respective roles. University Digital Assets (as defined below) are critical for the ongoing effective and secure fulfillment of the University's mission. This Policy describes how the University manages and supports all University Digital Assets in alignment with the government's measures regarding cyber-security.

SCOPE

This Policy and the related guidelines, processes and procedures, which are available in the IT Service Catalogue, (the "Catalogue") apply to all Employees and Students of the University, including all departments and units that utilize University Digital Assets. All Employees, Students, departments and units must comply with the defined Digital Asset Management (as defined below) and the applicable guidelines, processes and procedures provided for in the Catalogue. Digital Asset Types (as defined below) are defined in the Catalogue and governed by this Policy.

This Policy does not apply to Personal Digital Assets (as defined below). Nothing in this Policy and the Catalogue shall replace or supersede any provisions set out in other University policies but it shall supersede any faculty, departmental or unit's guidelines, processes or procedures with respect to the management of University Digital Assets.

PURPOSE

The purpose of this Policy is to support Employees and Students in ensuring the effective, and efficient management of University Digital Assets throughout the asset lifecycle and to preserve the security and integrity of the University's proprietary Information Technology ecosystem. In addition to ensuring compliance with the Catalogue, the Policy aims to support the implementation of best practices for Digital Asset Management, including:

- contributing to improved Employee and Student experiences related to the provisioning for, access to, use and maintenance of University Digital Assets;
- maintaining a single, up-to-date central repository for all University Digital Asset data, accessible to authorized technical and management teams, and individuals as required;
- identifying, managing and mitigating information security risks;
- reducing the total cost of ownership of University Digital Assets across the University through volume acquisition and standardization of assets and baselines;
- promoting the planned and coordinated renewal of University Digital Assets through an inventory process and a needs prioritization;
- ensuring that all University Digital Asset management and acquisition are consistent with the sustainability goals and procedures provided for in the relevant University policies, including the *Sustainability Policy* (BD-7)
- facilitating ongoing asset management process improvements;
- ensuring license compliance; and
- integrating and aligning with the University's Enterprise Asset Management Program in accordance with the *Enterprise Risk Management Policy* (BD-14) and the *Capital, Asset Management, Funding and Financing Policy* (CFO-4).

DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

Employee(s)" means a full-time, part-time or temporary employee of the University, including staff, faculty, postdoctoral fellows, researchers, members of the administration, stagiaires and interns; any individual engaged by the University on a consulting basis or in virtue of any other contractual agreement; and appointees (including volunteers) of the University.

"Information Technology" or "IT" means anything related to information technology computing, such as networking, cloud services, hardware, software, data, or other services that support or use these technologies.

"Digital Asset Management" means the set of practices that join financial, contractual and inventory functions to support the lifecycle management and strategic decision making for the IT environment.

“Digital Asset Types” means the classified sets of University Digital Assets possessing similar characteristics.

“IT Management Agent(s)” means software that provides functionality, including but not limited to, patch management, software distribution, operating system deployment and hardware and software inventory.

“IT Support” means staff that performs technical support functions within a University department or unit.

“Personal Digital Asset(s)” means all assets not purchased, acquired, owned or contracted for by the University, including, but not limited to, personal smartphones, personal digital assistants, tablets and/or computers.

“Student(s)” means any person registered in a course or program on a full or part-time basis, for credit or not, and includes undergraduate and graduate students, independent students as well as visiting students, exchange students and interns.

“University Digital Assets” mean discrete or aggregated software, data or hardware components within an IT environment, both on and off University premises and include cloud-based services, including but not limited to computers, servers, mobile devices, tablets, networking equipment, audio-visual equipment, software licenses, applications and data solutions purchased, acquired, owned or contracted for by the University. The Concordia University telecommunications network is considered an aggregated University Digital Asset.

POLICY

1. The University will implement necessary processes and controls to ensure appropriate asset lifecycle management, including processes related to procurement, securing, deployment, maintenance, renewal, reallocation and decommissioning of all University Digital Assets.

2. All Employees and Students will comply with this Policy and the Catalogue when utilizing any University Digital Asset.

3. Regular audits by Digital Asset Type will be conducted by Instructional and Information Technology Services (IITS), Office of the Treasurer and Internal Audit.

4. The acquisition of University Digital Assets requires long-term planning. It is the responsibility of each unit manager or department chair to assess the need for University Digital Assets in the units reporting to them, in accordance with the IT governance framework which is provided for in the Catalogue.

5. The acquisition of all University Digital Assets shall be approved by IITS and shall be done in accordance with this Policy, the Catalogue, the *Procurement Policy* (CFO-20) and other applicable University policies.

6. All University Digital Assets will be tracked in a central repository for Digital Asset data, including contract information.

7. All University Digital Assets must conform to IITS standards, security baselines and periodic testing requirements for such assets and be included in the central repository for Digital Assets. Any Digital Asset that does not conform to these standards and requirements will be, as appropriate, removed from the user or decommissioned.

8. Personal Digital Assets can be used in conjunction with University Digital Assets, such as software and data. In such cases, the University Digital Asset must be used and managed in compliance with the present Policy.

9. All integration of University Digital Assets onto the University’s network acquired or contracted for outside of IITS, by Employees or Students, will be done in compliance with this Policy and the Catalogue.

10. A University licensed and/or recommended software list will be published as part of the Catalogue. All software not in the Catalogue must be assessed and approved by IITS. Unapproved software may be subject to it being removed or secured, as required.

11. All University Digital Assets must be configured and secured in accordance with the Catalogue. This configuration must be maintained at all times. The University endpoint protection software and IT Management Agents are listed in the Catalogue.

12. It is the responsibility of IT Support, Employees and Students to ensure that equipment and their components are decommissioned in compliance with the Catalogue. Where an Employee is ending their employment relationship with the University, or a Student is no longer undertaking any University activities or have completed their academic activities, it is their responsibility to return all University Digital Assets to the University.

13. Any exceptions to this Policy shall be approved by the Chief Information Officer or their delegate and shall be subject to the process provided for in the Catalogue.

14. The overall responsibility for implementing and recommending amendments to this Policy shall rest with the Vice-President, Services and Sustainability.