KPU | KWANTLEN POLYTECHNIC UNIVERSITY

Policy History
Policy No. IM9
Approving Jurisdiction: President
Administrative Responsibility: Vice President Administration
Effective Date: December 7, 2020

Information Security Policy

A. CONTEXT AND PURPOSE

Kwantlen Polytechnic University possesses information that is sensitive and valuable, such as personal information, financial data, building plans, research data, and other information considered confidential. Some information is protected by Federal or Provincial laws or contractual obligations that prohibit its unauthorized use or disclosure.

The disclosure of certain University information to unauthorized parties could cause irreparable harm to the University or members of the University community, and could also subject the University to fines or other government sanctions. Additionally, if University information was tampered with or made unavailable, it could impair the University's ability to do business.

This Policy and related Procedure establish guidelines to protect University information as appropriate to its Information Sensitivity Level.

This Information Security Policy and related Procedure shall be interpreted in harmony with up-to-date versions of related legislation, agreements, and policies, as they may be amended from time to time.

B. SCOPE AND LIMITS

This policy and its related procedure apply to:

1. All University employees.
2. Contractors, students and individuals associated with the University and/or working on behalf of the University who have access to University information.

C. STATEMENT OF POLICY PRINCIPLES

1. The University is committed to taking the appropriate measures to preserve the confidentiality, integrity and availability of University information and information technology systems. Reasonable security arrangements for information resources are necessary to achieve the University's commitment to the protection of privacy and compliance with the Freedom of Information and Protection of Privacy Act (BC), University policies, other relevant

legislation/regulations and contractual obligations.

2. All employees and individuals (including students, contractors and those who are associated with the University and/or working on behalf of the University) who have access to University information are expected to adhere to this policy. Responsibilities include:

    a. Protect the confidentiality, integrity and availability of the University's information wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.

    b. Handle University information in accordance with the University's requirements for protecting privacy and confidentiality as set out in the Confidentiality Policy (IM4) and the Freedom of Information and Protection of Privacy Policy (IM2).

    c. Report any activities that may compromise University information to the employee's supervisor, Information Guardian or to the IT Service Desk.

    d. All KPU employees must complete the mandatory Information Security Awareness Training.

    e. While many federal or provincial laws create exceptions allowing for the disclosure of information in order to comply with subpoenas, court orders and other compulsory information access requests, anyone who receives such compulsory requests for information should contact the University's Office of the General Counsel before taking any action.

    f. Breaches of this Policy and its related Procedure may be subject to the full range of disciplinary actions available to the University including relevant University policies (e.g. IM3 Information and Educational Technology Usage Policy, IM4 Confidentiality, collective agreements and relevant legislation such as the Criminal Code of Canada, the B.C. Civil Rights Protection Act, the B.C. Freedom of Information and Protection of Privacy Act and the B.C. Human Rights Code).

    g. In the event of a discrepancy between this policy and KPU's Collective Agreement with either the KFA or the BCGEU, the Collective Agreement shall prevail.

3. Department/unit managers and supervisors are responsible to:

    a. Ensure departmental procedures support the objectives of confidentiality, integrity and availability defined by the appropriate Information Guardian, and that those procedures are followed.

    b. Ensure that any restrictions on disclosure of University information are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.

    c. Ensure that each staff member understands their information security-related responsibilities.

4. Technology managers who manage computing and network environments that capture, store, process and/or transmit University information, are responsible for ensuring that the requirements for confidentiality, integrity and availability as defined by the appropriate Information Guardian are being satisfied within their environments. These include the requirement to:

    a. Understand the Information Sensitivity Level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.

b. Develop, implement, operate and maintain a secure technology environment that includes:

   i. A cohesive architectural plan.

   ii. Product implementation and configuration standards.

   iii. Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Guardians.

   iv. Ensure the assignment and revocation of access rights follow a formal and documented process.

   v. Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are up to date.

   vi. Ensure security controls are maintained when computer equipment, information or software is used outside KPU facilities.

c. Develop an effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.

d. Ensure that staff members and any third parties understand the Information Sensitivity Level of the information being handled and the related security requirements.

e. Ensure that Privacy Impact Assessments are completed as required pursuant to the Freedom of Information and Protection of Privacy Act and that the appropriate Information Guardians are apprised of risk factors associated with information stored off premise under the responsibility of a third party in multiple jurisdictions.

5. Operations Security

   a. This section establishes a framework for identifying requirements to control, monitor, and manage information security and any changes to the delivery of KPU computing services.

   b. KPU Information Technology must:

      i. Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems.

      ii. Monitor and maintain information systems software throughout the software lifecycle.

      iii. Define, document, assess, and test backup and recovery processes regularly.

      iv. Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems.

      v. Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis.

      vi. Establish controls to protect log files from unauthorized modification, access or disposal.

      vii. Establish processes to identify, assess, and respond to vulnerabilities. Including annual vulnerability assessment scans on all business critical IT infrastructures.

viii. Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting.

ix. Establish and maintain regular security patching on all enterprise server and workstation operating systems including network devices.

x. Establish and maintain regular security patching on all business critical software applications.

xi. Establish and maintain regular access control audits on all business critical file stores and systems.

D. DEFINITIONS

Refer to Section A in the related Procedure document for definitions which will enhance the reader's interpretation of this Policy.

E. RELATED POLICIES & LEGISLATION

AR3 *Confidentiality of Student Records/Files* Policy
BP5 *Use of University Property* Policy
IM2 *Freedom of Information and Protection of Privacy* Policy
IM3 *Information and Educational Technology* Policy
IM4 *Confidentiality* Policy
Freedom of Information and Protection of Privacy Act (BC)

F. RELATED PROCEDURES

IM9 *Information Security* Procedure