KPU | KWANTLEN POLYTECHNIC UNIVERSITY

| Policy History |
|---|
| **Policy No.**<br>IM9 |
| **Approving Jurisdiction:**<br>President |
| **Administrative Responsibility:**<br>Vice President Administration |
| **Effective Date:**<br>December 7, 2020 |

# Information Security Procedure

## A. DEFINITIONS

1. **Availability:** Refers to the protection of information and information systems from unauthorized disruption. Ensuring availability is ensuring timely and reliable access to and use of information and information systems.

2. **Confidentiality:** Confidentiality is the security principle that controls access to information. Access must be restricted to those whose roles require it.

3. **Contact Information:** Contact information is information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

4. **FIPPA:** The Freedom of Information and Protection of Privacy Act (British Columbia).

5. **Information Guardian:** The guardian of an Information Collection is typically the head of the administrative department or Dean from the faculty areas on whose behalf the information is collected or that is most closely associated with such information.

6. **Integrity:** Refers to the protection of information from unauthorized modification or destruction. Ensuring integrity is ensuring that information and information systems are accurate, complete and uncorrupted.

7. **Personal Information:** Personal Information is recorded information about an identifiable individual other than business contact information. Examples include name, address, telephone number, personal email address (including, for students, KPU email address), race, origin, color, political or religious beliefs, age, sex, sexual orientation, marital or family status, and any identifying number or symbol assigned to

| | | |
|---|---|---|
| | | an individual. It includes an individual's personal history regarding finances, education, health, criminal records, employment, anyone else's opinion about the individual, as well as the individual's personal views or opinions, unless they are about someone else. These examples of personal information are not exhaustive. There may be other types of information that, alone or in combination, would reveal the identity of a particular individual.<br><br>All Personal Information in the custody or control of the University is considered confidential, and may only be disclosed by the appropriate Information Guardian and/or in accordance with FIPPA. |
| **8.** | **Privacy** | A type of confidentiality specifically related to Personal Information. |
| **9.** | **Privacy Impact Assessment (PIA):** | An assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the privacy requirements of Part 3 of FIPPA. |
| **10.** | **University:** | Kwantlen Polytechnic University (KPU). |
| **11.** | **University information:** | For the purpose of this Policy, "University information" includes but is not limited to information, publications, documents or records, in any format, belonging to and/or maintained, stored, controlled, or possessed by the University and/or Personal Information entrusted to the University by a third party, and/or pertaining to the business or affairs of the University that are not in the public domain. |

# B. PROCEDURES

**1. Information Confidentiality, Integrity and Availability**

**a. The Confidentiality Level for an Information Collection will be expressed in the following terms:**

i. Measures undertaken to ensure Confidentiality are designed to ensure that unauthorized parties cannot gain access to Confidential and/or Restricted information while ensuring authorized parties can access it.

ii. Protecting confidentiality may also include special training for those who share sensitive data, including familiarizing authorized users with security risk factors and teaching them how to guard vulnerable data assets.

iii. In addition to training, strong passwords and password-related best practices must be used as well as information about social engineering attacks to prevent employees from unwittingly avoiding proper data-handling rules and potentially causing disastrous results.

**b. The integrity/availability requirement for an Information Collection will be expressed as follows:**

i. **Integrity** involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file encryption, permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem.

ii. **Availability** ensures that information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching and network optimization. Processes such as redundancy, failover, RAID and high-availability clusters are used to mitigate serious consequences when hardware issues do occur. Dedicated hardware devices can be used to guard against downtime and unreachable data due to malicious actions such as distributed denial-of-service (DDoS) attacks.

iii. Information is "**Non-critical**" if its unauthorized modification, loss or destruction would cause temporary inconvenience to the user community and support staff, and incur limited recovery costs.

iv. Information is "**Critical**" if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the University to:

1) Suffer significant financial loss or damage to its reputation,

2) be non-compliant with legal/regulatory or contractual requirements,

3) Adversely impact its students and staff.

**c. Employee and Contractor responsibilities**

i. Departmental supervisors must ensure:

1) During employment, employees are informed about the information security policies and procedures, Information Security roles and responsibilities.

2) Ensure the mandatory employee Information Security Awareness training is successfully completed. All KPU employees that have been provisioned a KPU computing account must complete the mandatory information security awareness training. This includes contract, volunteers and employees working outside of Canada.

3) Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary; and

4) Contractor responsibilities for information security are set out in FIPPA and may be identified in contractual agreements.

**d. Personal Information**

i. All Personal Information in the possession of KPU is considered Restricted or Confidential (as determined by the applicable Information Guardian) unless:

1) The information is designated as "Contact Information" by the appropriate Information Guardian (in which case it is not Personal Information); or

2) The Information Guardian has otherwise authorized its disclosure.

ii. The University requires that the following pieces of Personal Information may not be collected, stored or used except in situations where the Information Guardian determines that there is legitimate business need and **no reasonable alternative**:

1) Social Insurance Number
2) Date of birth
3) Place of birth
4) Mother's maiden name
5) Credit card numbers
6) Bank account numbers
7) Income tax records
8) Driver's license numbers
9) Personal Heath Number (PHN)

iii. Managers must ensure that their employees understand the need to safeguard Personal Information, and that adequate procedures are in place to minimize the risk of unauthorized collection, use, disclosure, access, storage, or retention. The security requirements for Restricted and Confidential information must be applied to all Personal Information. Access and/or disclosure to such information may only be granted to authorized individuals on a need to know basis and must be authorized by the appropriate Information Guardian.

iv. Notwithstanding anything contained in this Policy, any collection, use, disclosure, access, storage, or retention of Personal Information must be done in accordance with and pursuant to FIPPA.

**e. Contact Information**

i. All Personal Information in the custody or control of KPU is considered Confidential unless it is deemed "Contact Information" by the appropriate Information Guardian in accordance with FIPPA. Contact Information may be disclosed by the University without the consent of the individual about whom the Contact Information relates.

ii. Please see IM2 Freedom of Information and Protection of Privacy Policy for the information outlining unauthorized collection, access, use or disclosure of Personal Information.

iii. For information about providing references for students or employees, please see HR17 Provision of References Policy.

## 2. MANAGING/HANDLING INFORMATION

### a. Security Requirements for Restricted and/or Confidential information

i. No one may access information that has been classified as Restricted or Confidential without authorization by the appropriate Information Guardian. For information classified as Confidential, such authorization may be granted to individuals by name, by policy or to all individuals serving in a specific job function. For information classified as Restricted, access must be authorized for each individual by name.

ii. In addition to any particular security requirements imposed by the appropriate

Information Guardian for information classified as Restricted or Confidential, the following procedural and system-level controls must be in place:

1) Access to a Restricted or Confidential Information Collection may only be granted after receiving permission by the appropriate Information Guardian/designee authorizing such access. The authorization by the appropriate Information Guardian/designee must be documented.

2) Departmental procedures must be in place to ensure that all individuals who have access to Restricted or Confidential information are aware of the Information Sensitivity Level to which they have access, understand their responsibilities to protect that information appropriately, and acknowledge their understanding and intent to comply with this policy.

3) Tangible records (paper documents, microfilm, etc.) containing Restricted or Confidential information must be:

    a) Stored in a locked cabinet or drawer when not in use with access limited to authorized individuals, and

    b) Physically shredded/destroyed before discarded.

**b. Requirements for KPU provisioned computers used to conduct University business**

Reasonable measures should be used to protect all University information regardless of the Information Sensitivity Level, including storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.

i. In order to adequately protect the Confidentiality, Integrity and Availability of University information systems, KPU provisioned computers used to conduct University business must be configured using security industry-sanctioned best practices that include but are not limited to the following:

1) Maintain an inventory of KPU information systems and devices.

2) Validate the measures taken to protect information systems and devices.

3) Configure and use computers in a manner that is compliant with industry standard security configurations.

4) Mobile device users must lock and/or secure unattended mobile devices to prevent unauthorized use or theft.

5) Define accounts intended for day-to-day computer use as "general user accounts". Accounts that have administrative privileges must only be used for system setup and maintenance.

6) Computers should be configured to "time out" after no more than 20 minutes of inactivity.

7) Ensure that system and application security updates are applied as soon after being released by the vendor as possible.

8) Limit the services running on University computers to those needed by the computer user to perform his or her assigned tasks.

9) In the event of employee termination,

    a) All computers and mobile devices provisioned to the employee must be

inventoried and returned to Information Technology shortly after the termination date.

b) Terminated employee must not leave the University premises with University computers or mobile devices.

c) University computers and or mobile devices must not be reallocated until IT has secured the local data and re-imaged or wiped the device.

10) Computers/systems that accept, capture, store, transmit or process information classified as **Restricted or Confidential** must comply with the following requirements:

a) Any piece of Restricted or Confidential information that is transmitted across the network must be encrypted using an encryption product and methodology approved by IT.

b) Personal computers should not be used to accept, capture, store, transmit or process restricted or confidential information.

c) Computer servers storing the information must be secured by an IT approved and managed Firewall that only permits connections with authorized systems using approved protocols.

d) Laptops and other mobile and external devices must only be usable by a limited number of specific users and system administrators explicitly authorized by the department that owns the laptop.

**c. Responsibility of employees and individuals who have access to University information**

i. Do not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the Information Guardian within the scope of his/her professional activities.

ii. Use only University provided email account for conducting University business. Automatic forwarding of university email account to external/personal email accounts is prohibited.

iii. Safeguard any physical/encryption key, ID card or computer/network account that allows access to University information. Create strong computer passwords.

iv. Lock or log off their computers before leaving them unattended.

v. Destroy or render unusable any Restricted or Confidential information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.

1) **Restricted (including any Personal Information) or Confidential information** should be removed from laptops or any mobile devices and stored in an approved secured manner before traveling outside Canada.

a) Border guards at some countries, including USA and Canada, have practices to compel travelers to provide passwords to laptops and may retain the laptop if the password is not provided.

2) Be aware of the potential security risks when connecting laptops and other mobile devices to unsecured Wi-Fi hotspots e.g. free public Wi-Fi hotspots at cafes, hotels and airports. Understand that information transmitted over the unsecured Wi-Fi network are susceptible to interception by hackers, and devices connecting to these networks and information contained in the devices are vulnerable to hacking.

**d. Freedom of Information and Protection of Privacy**

i. Notwithstanding anything contained in this Policy, this Policy and related Procedures must be interpreted and applied in a manner consistent with FIPPA.

## 3. RELATED POLICY

AR3 *Confidentiality of Student Records/Files* Policy
BP5 *Use of University Property* Policy
HR17 *Provision of References* Policy
IM2 *Freedom of Information and Protection of Privacy* Policy
IM3 *Information and Educational Technology* Policy
IM4 *Confidentiality* Policy
IM9 *Information Security* Policy