

Security Breach Policy: Information & IT Systems

Institution: Futures Canadian College of Business, Health & Technology

Effective Date: October 11, 2025

Policy Owner: Karan Bagga

Approved By: Tzarina Saldana

1. Purpose

The purpose of this policy is to establish procedures and responsibilities for identifying, responding to, and mitigating **security breaches** involving **student information** and **IT-related systems** at [College Name]. This policy aims to protect the **confidentiality, integrity, and availability** of student data and institutional IT assets.

2. Scope

This policy applies to:

- All students, staff, faculty, contractors, and third-party vendors who access college systems.
- All information systems, databases, devices, networks, and platforms are used for academic or administrative purposes.
- All types of data breaches, including unauthorized access, loss, theft, or compromise of personal, academic, financial, or health information.

3. Definitions

- **Security Breach:** Any event that results in unauthorized access to, use, disclosure, modification, or destruction of data or IT systems.
- **Personal Information:** Any information that can identify an individual, such as name, student ID, address, academic records, or SIN.
- **IT Systems:** All digital infrastructure owned or managed by the college, including email systems, student portals, LMS, databases, and network services.

4. Responsibilities

Role	Responsibilities
IT Department	Monitor systems, respond to incidents, maintain cybersecurity protocols
Privacy Officer	Ensure compliance with privacy laws, report data breaches to authorities if required
All Employees & Students	Report suspected breaches immediately; follow IT policies

5. Breach Response Procedure

Step 1: Identify & Contain the Breach

- Immediately report suspected breaches to the IT Department.
- Isolate affected systems to prevent further access.
- Disable compromised accounts if necessary.

Step 2: Assess the Breach

- Determine the scope, type, and sensitivity of compromised data.
- Identify affected individuals and systems.
- Evaluate risks to student privacy and institutional operations.

Step 3: Notify Relevant Parties

- Notify the Privacy Officer and senior management.
- If required by law (e.g., under **PHIPA** or **PIPEDA**), notify:
 - Affected students
 - Regulatory authorities (e.g., Information and Privacy Commissioner of Ontario)
- Notification should include:
 - What happened
 - What information was involved
 - What the college is doing in response
 - What individuals can do to protect themselves

Step 4: Mitigation and Remediation

- Reset passwords, patch systems, restore backups, or take other recovery measures.
- Offer support to affected students (e.g., credit monitoring, counselling if relevant).
- Document all steps taken.

Step 5: Post-Incident Review

- Conduct an internal investigation.
- Identify root causes and apply long-term fixes.
- Update security policies and procedures accordingly.
- Train staff and students on new measures.

6. Prevention Measures

- Use strong encryption and access controls.
- Conduct regular security audits and penetration testing.
- Require cybersecurity training for all staff and faculty.
- Maintain up-to-date anti-malware, firewall, and intrusion detection systems.
- Enforce strong password and MFA policies.

7. Legal & Regulatory Compliance

This policy complies with all applicable laws and regulations, including:

- **Personal Information Protection and Electronic Documents Act (PIPEDA)**
- **Ontario's Personal Health Information Protection Act (PHIPA)**
- **Freedom of Information and Protection of Privacy Act (FIPPA)**, where applicable

8. Policy Review

This policy will be reviewed annually or as needed based on changes in legislation or institutional practices.

9. Contact Information

For questions or to report a breach, contact:

IT Support: support@theshareplus.com

Privacy Officer: kbagga@theshareplus.com || Phone no: +16478464456

Emergency Line (after-hours): +16478464882



Dr. Sarwan Singh
Vice-President
Futures Canadian College