BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Policy

Emergency Management and Business Continuity

Policy No:	7110
Version:	7
Category:	Safety, Security and Emergency Management
Approval Body:	Board of Governors
Executive Sponsor:	VP Human Resources and People Development
Department Responsible:	Safety, Security and Emergency Management
Directory of Records Class:	0650-10
Approval Date:	2023 May 30

Policy Statement

BCIT is committed to building, maintaining, and improving its ability to mitigate, prevent, prepare for, respond to, and recover from natural or human-caused emergencies or disasters. The activities necessary for doing so are coordinated and integrated by the Emergency Management Program and its component Business Continuity Program.

Purpose of This Policy

The purpose of this policy is to establish the guiding principles by which BCIT manages emergencies and disasters, and to provide the foundations of BCIT's Emergency Management Program and Business Continuity Program, including the roles and responsibilities within them for mitigating, preventing, preparing for, responding to, and recovering from an emergency or disaster.

This policy ensures the Institute:

- Uses the British Columbia Emergency Management System (BCEMS) as its response management system for emergencies and disasters.
- Develops and implements response, recovery, and business continuity plans as required.
- Prepares, trains, and exercises response team members to ensure they respond effectively to emergencies or disasters.
- Acquires and maintains equipment necessary to ensure an appropriate response to any emergency or disaster.
- Provides a framework for protecting BCIT's operations in an emergency or disaster.
- Mitigates the long-term effects of an emergency or disaster on BCIT's operations and mission.

Application of This Policy

This policy applies to all BCIT employees, students, Board members, and contractors, and every other person who visits Institute grounds, buildings, or other facilities.

Related Documents and Legislation

Provincial Legislation

Emergency Program Act, RSBC 1996, c 111
Emergency Program Management Regulation, BC Reg 477/94
Workers Compensation Act, RSBC 2019, c 1
Occupational Health and Safety Regulation, BC Reg 296/97, ss 4.13-4.18 (General Conditions: Emergency Preparedness and Response)

Provincial Guides

British Columbia Emergency Management System [2016]

CSA Standards

Z1600-2017 – Emergency and Continuity Management Program
CSA Z731 – Emergency Preparedness and Response
NFPA 1600-2019 – Standard on Continuity, Emergency, and Crisis Management
ISO 22301:2019 – Security and resilience — Business continuity management systems
DRII Professional Practices for Business Continuity Practitioners, 2017
BCI Good Practice Guidelines, 2018

BCIT Plans

Emergency Support Plans

BCIT Policies

Policy 1300, Enterprise Risk Management
Policy 3502, Information Security
Policy 7100, Safety and Security
Procedure 7100-PR3, Fire Prevention and Preparedness
Procedure 7100-PR4, Response to Bomb Threat
Policy 7150, Occupational Health & Safety

Definitions

British Columbia Emergency Management System or "**BCEMS**"**:** means the guide published by the Government of British Columbia that is the standard system recognized for emergency and disaster response and is currently mandated for use within the Government of BC and recommended to local authorities.

business continuity management: means a management process that identifies risks, threats, and vulnerabilities that could impact BCIT's continued operations, and that provides a framework for building organizational resilience and capacity to respond effectively to them.

business continuity planning: means the process of developing and maintaining prevention and recovery systems, processes, and procedures before an incident occurs to ensure the continuity of primary business operations during such events and an orderly return to regular business operations after.

Business Continuity Plan: means a plan created by a school or department through business continuity planning to guide it in maintaining and restoring business operations during and after an incident.

Business Continuity Program: means the Institute-wide program that integrates business continuity management and business continuity planning with Business Continuity Plans to build organizational resilience in BCIT that ensures critical business functions can continue with planned levels of interruption or essential change during and after an incident.

Business Continuity and Disaster Recovery Steering Committee: means a committee comprised of key stakeholders and technology experts that is responsible for making strategic business continuity policy and planning decisions for BCIT, and assigning resources to achieve the goals of the Business Continuity Program.

Disaster Management Committee: means a committee responsible for setting policy direction for planning, mitigation, preparedness, emergency and disaster response, recovery, and business continuity. The Committee has the authority to expend monies and take actions required to achieve an effective response to incidents at a BCIT campus.

disaster recovery: means a subset of business continuity planning that aims to minimize business downtime during an incident, and that focuses on ensuring technical operations return to normal as soon as possible after.

emergency management: means the process for mitigating, preventing, preparing, responding to, and recovering from an incident.

Emergency Management Program: means the Institute-wide program that integrates emergency management with the BCEMS to enable BCIT to mitigate, prevent, prepare for, respond to, and recover from natural or human-caused emergencies and disasters. The program includes Emergency Response Plans as its cornerstone, which provides for a concise line of command.

Emergency Operations Centre or "**EOC**"**:** means a designated facility established by BCIT to coordinate the overall Institute emergency response and support to site during an incident.

Emergency Response Plan: means a plan created by a school or department that provides logistical, technical, operational, and administrative procedures to be followed in the event of an accident or incident, including relevant guidelines, strategies, information, and data.

Emergency Response Teams: means teams composed of individuals from all campuses who volunteer to conduct the frontline operations of an incident response under the direction of the Incident Commander.

Emergency Support Plan: means a plan that is a component of the Emergency Response Plan of a school or department that addresses emergency management and business continuity of particular operations or functions.

Hazard, Risk and Vulnerability Assessment or "**HRVA**"**:** means an assessment that assists BCIT to make risk-based choices to address vulnerabilities and mitigate hazards, and prepare for, respond to, and recover from a range of hazard events.

incident: includes an emergency event and a disaster event.

Incident Commander: means the official with overall responsibility for site level management of the response to an incident, as described in the BCEMS.

Information Technology Disaster Recovery Plan: means a plan developed by the Business Continuity and Disaster Recovery Steering Committee to manage risks associated with the use of information technology as part of disaster recovery.

mitigation: means actions and activities taken to eliminate or reduce hazards and their impacts.

Policy Group: means the group with members appointed by the President that is accountable to the President for the responsibilities assigned to it in this policy.

preparedness: means measures undertaken in advance to ensure that individuals and BCIT will be ready to react to incidents, including developing emergency plans, mutual aid agreements, resource inventories, and emergency communications systems, and conducting training and exercises.

prevention: means activities to prevent an incident from occurring or stop an incident in progress from progressing further.

response: includes activities that:

- begin when an incident is imminent or is occurring;
- address the direct effects of an incident; and
- are designed to limit loss of life, personal injury, and property damage.

recovery: means actions and activities designed to return BCIT and the BCIT community as close to the pre-incident state as possible.

SSEM: means BCIT's Department of Safety, Security and Emergency Management.

Guiding Principles

This policy is governed by the following guiding principles, which inform any questions about how the policy is to be interpreted or applied.

1. BCIT is committed to providing a safe and secure environment. As part of an overall protection strategy, BCIT will create and maintain a risk-based Emergency Management Program and Business Continuity Program, allocate the necessary resources, and develop and maintain processes and procedures to ensure the Institute responds effectively to any emergency or disaster so that students, employees, and visitors can learn, work, and visit in a safe environment.
2. BCIT recognizes the requirements for an effective response both internally and externally to incidents that may impede its ability to provide normal levels of service. BCIT will ensure the best possible service will be provided during a business disruption, emergency, or disaster by supporting the development, evaluation, and maintenance of the Emergency Management Program and the Business Continuity Program, a high level of readiness, and a coordinated response.
3. BCIT will comply with all applicable laws relating to emergency and disaster preparedness, prevention, mitigation, response, and recovery.

4. BCIT will provide for the continuation of business and a return to normal operations as soon as possible after an emergency or disaster, through the Emergency Management Program and the Business Continuity Program.
5. BCIT works to meet the following goals in the event of an emergency or disaster, through the Emergency Management Program and the Emergency Response Plans of each school and department:
    a. Provide for the safety and health of all responders
    b. Save lives
    c. Reduce suffering
    d. Protect public health
    e. Protect the Institute's infrastructure
    f. Protect the Institute's property
    g. Restore the Institute's operations
    h. Protect the environment
    i. Reduce economic and social losses
6. BCIT will ensure that a Business Continuity Program is in place as a component of the Emergency Management Program. The Business Continuity Program will integrate business continuity planning and management with the Business Continuity Plans of each school and department to build organizational resilience that ensures critical business functions can continue with planned levels of interruption or essential change during an emergency or disaster.
7. Schools and departments will protect their business by developing and maintaining Emergency Management Plans and Business Continuity Plans, reviewing them annually and updating as necessary.

Emergency Call-out Procedure

1. If a BCIT employee or contractor is the first person to receive a call involving an incident, they should immediately report all pertinent information to the BCIT Security Communications Centre at 604-451-6856.
2. Upon learning of an incident, the BCIT Security Communications Centre must advise the Senior Director of SSEM, the Associate Director of Campus Security, or the Security Manager.
3. The Senior Director of SSEM must assess a situation on the basis of available information and determine the extent that emergency personnel are to be mobilized, i.e., partial call-out or total call-out as appropriate to the incident. If practicable in the circumstances, the Senior Director must consult either BCIT’s President or Chief Financial Officer on the assessment and determination, but otherwise may proceed unilaterally.
4. The Senior Director of SSEM must instruct SSEM personnel who are called out, based on the available information.

5. If the Senior Director is not available to make the assessment and determination, or to instruct SSEM personnel, then the President will do so, after consulting with the Chief Financial Officer if practicable. If neither the Senior Director nor the President are available then the Chief Financial Officer will make the assessment and determination, and instruct SSEM personnel.

Duties and Responsibilities

Employees, Students, Contractors, Governors and Other Persons who Visit BCIT Premises

Any person who is aware of an emergency, disaster, or other incident that could affect BCIT and suspects that SSEM is not aware of it, should immediately report all pertinent information to the BCIT Security Communications Centre at 604-451-6856.

<u>If an emergency, disaster, or other incident occurs, every person must obey the instructions and directions of the Incident Commander without delay.</u>

Schools and Departments

Each school and department is responsible for:

- Developing and maintaining an Emergency Response Plan and a Business Continuity Plan.
- System owners must negotiate appropriate recovery time with Information Technology Services or other service providers. Where business requirements exceed the ability to recover information technology assets, establish mitigating controls.
- Cooperating with the Manager of Emergency Management to identify opportunities for improving standardization and effectiveness of its Emergency Response Plan and Business Continuity Plan.
- Reviewing its Emergency Response Plan and Business Continuity Plan annually and updating as necessary to improve standardization and effectiveness.

Senior Director of Safety, Security and Emergency Management

The Senior Director of SSEM is responsible for the overall management of response to an incident, including acting as Incident Commander or delegating the role of Incident Commander.

The Senior Director is also responsible for:

- Coordinating the members of the Disaster Management Committee and chairing the Committee.
- Coordinating the members of the Business Continuity and Disaster Recovery Steering Committee and chairing the Committee.
- Providing ongoing oversight of the Emergency Management Program and the Business Continuity Program.
- Ensuring a Hazard, Risk and Vulnerability Assessment is completed every five years, or sooner if necessary.
- Giving instructions and directions that implement Emergency Response Plans and Business Continuity Plans during and after an incident.

- Completing a formal investigation of an incident in a timely manner and making recommendations to the Disaster Management Committee and the Policy Group.
- Ensuring that designated personnel receive appropriate formal training in emergency management.

Manager of Emergency Management

The Manager of Emergency Management is responsible for managing the Emergency Management Program and the Business Continuity Program.

The Manager is also responsible for:

- Developing and maintaining standardization for Emergency Support Plans, Emergency Response Plans, and Business Continuity Plans.
- Developing policy and standards for the Business Continuity Program that align with BCIT objectives and industry best practice.
- Monitoring Emergency Response Plans and Business Continuity Plans, and providing guidance on improving their standardization and effectiveness.
- Managing Emergency Response Team volunteers, including recruiting, and providing training and appropriate equipment.
- Managing the BCIT Fire Warden program, including recruiting, providing training and appropriate equipment, and exercising designated employees to guide building occupants in taking safety measures in the event of an incident.
- Determining the type, amount, and frequency of training and exercises, and maintaining a record of training and exercise activities to ensure that the Emergency Management Program and the Business Continuity Program remain current, complete, and effective.
- Establishing effective emergency communications systems.
- Initiating and coordinating an annual emergency response exercise, with the assistance of the Disaster Management Committee.
- Initiating and coordinating business continuity exercises or simulations.

President

The President is responsible for:

- Declaring Emergency Response Plans to be in effect, and ceasing to be in effect.
- Appointing members of the Policy Group, which may act on the President’s behalf during an incident if the President is unavailable.

Disaster Management Committee

The Disaster Management Committee is responsible for:

- Developing, implementing, and maintaining a risk-based Emergency Management Program that includes comprehensive policies, plans, procedures, education, and training.

- Assisting the Manager of Emergency Management with initiating and coordinating an annual emergency exercise or simulation.
- Issuing directives and protocols for preparedness and incident response.
- Assigning resources and personnel responsible for incident response.
- Expending funds and taking actions to respond effectively to an incident at a BCIT campus.
- Following up on recommendations made by the Senior Director of SSEM.

Business Continuity and Disaster Recovery Steering Committee

The Business Continuity and Disaster Recovery Steering Committee is responsible for providing oversight of business continuity and disaster recovery initiatives, which include:

- Developing, implementing, and maintaining a risk management and recovery strategy for business continuity including comprehensive policies, plans, procedures, education and training, and exercising/testing.
- Assigning resources to accomplish BCIT's Emergency Management Program and Business Continuity Program goals.
- Developing an Information Technology Disaster Recovery Plan and procedures associated with the process of managing risks affiliated with the use of information technology.
- Participating in the development and execution of disaster recovery exercises to validate restoration and recovery of critical business data and applications.
- Overseeing the development and updating of Emergency Response Plans and Business Continuity Plans to ensure the plans are operationally reliable.
- Notifying Enterprise Risk Management of any significant risks to the operational reliability of Emergency Response Plans and Business Continuity Plans.
- Post-incident, following up on fundamental tasks for debriefing and assessing response that include recommending revisions to Emergency Support Plans.
- Following up on recommendations made by the Senior Director of SSEM.

Policy Group

The Policy Group is responsible for:

- Providing leadership in incident management.
- Establishing strategic direction for the Emergency Management Program and the Business Continuity Program.
- Allocating resources for the Emergency Management Program and the Business Continuity Program.
- Ensuring Emergency Response Plans and Business Continuity Plans can be operationalized.
- Mitigating long-term effects of an incident on the Institute's operations and mission.

- Restoring services and facilities as quickly as possible following termination of a response to an incident.
- Coordinating all efforts through the Emergency Operations Centre's formal liaison with provincial and federal officials.
- Acting on behalf of the President during an incident if the President is unavailable.

Emergency Response Teams

Emergency Response Teams are responsible for:

- Taking action during and after an incident under the direction of the Emergency Operations Centre or Incident Commander.

Procedures and Guidelines Associated with This Policy

Emergency Preparedness and Response – Employee Guide

Forms Associated with This Policy

None

Amendment History

		Approval Date	Status
Created:	Policy 7110 version 1	2003 Oct 28	Replaced
Revised:	Policy 7110 version 2	2005 Sep 26	Replaced
Revised:	Policy 7110 version 3	2008 July 15	Replaced
Revised:	Policy 7110 version 4	2008 Oct 21	Replaced
Revised:	Policy 7110 version 5	2012 Mar 30	Replaced
Revised:	Policy 7110 version 6	2017 Jan 30	Replaced
Revised:	Policy 7110 version 7	2023 May 30	In Force

Scheduled Review Date

2028 May 30 (sooner if there are changes to the applicable regulatory framework or relevant operational circumstances).