COMMISSIONER'S DIRECTIVE 564-6	In Effect: 2015-05-19 Due for Review: 2017-05-19
Business Continuity Program	
PROGRAM ALIGNMENT	Internal Services
OFFICE(S) OF PRIMARY INTEREST	Correctional Operations and Programs Sector
ONLINE @	• http://infonet/cds/cds/564-6-cd-eng.pdf • http://infonet/cds/cds/564-6-cd-fra.pdf • http://www.csc-scc.gc.ca/text/plcy/cdhtm/564-6-cd-eng.shtml • http://www/csc-scc.gc.ca/text/plcy/cdhtm/564-6-cd-fra.shtml
AUTHORITIES	• *Emergency Management Act* • Treasury Board Policy on Government Security
PURPOSE	• To provide direction and outline the responsibilities for the Business Continuity Program
APPLICATION	Applies to all CSC employees assigned responsibility for Business Continuity Plans (BCPs)

CONTENTS

RESPONSIBILITIES

1. The Executive Committee members will:

   a. approve the National Business Continuity Program policy and governance

   b. review and approve identified critical services and associated assets

c. approve Business Continuity Plans and activities

d. ensure regular training, review, testing and audit

e. ensure Business Continuity Program activities are supported by Information Management/Information Technology and other continuity plans and arrangements, as required.

2. The Assistant Commissioner, Correctional Operations and Programs, will:

a. oversee the Business Continuity Program as champion of emergency management through ensuring regular maintenance, training, testing and internal and external audits

b. appoint a National Business Continuity Program Coordinator

c. approve methodologies and guidelines for implementing the Business Continuity Program policy

d. ensure that National and Regional Headquarters establish a Crisis Centre/Emergency Operations Centre in order to ensure that accurate, up-to-date information is disseminated

e. ensure that information released to the public through the media is accurate, coordinated and consistent at all levels, and that it takes into consideration those factors which may be beyond the resolution of the emergency itself. No statement regarding the situation may be released unless it has been so coordinated

f. coordinate the obtaining of funding and required resources.

3. The Assistant Deputy Commissioner, Integrated Services/sector head will:

a. ensure the timely completion of their sector or branch Business Continuity Plans

b. approve, review and update plans annually or whenever there are significant changes to the organization, functions or service levels in order to maintain program readiness

c. approve Business Continuity Plans, training and exercises

d. participate in training and exercises to ensure the plans remain current and effective

e. direct the development, implementation and testing of regional and local contingency plans including emergency and Business Continuity Plans

f. report results to the National Business Continuity Program Coordinator

g. provide strategic advice and guidance during a crisis.

4. The Director General, Security Branch, will:

   a. manage the National Headquarters Crisis Centre/Emergency Operations Centre

   b. provide strategic advice and guidance during a crisis to ensure that accurate, up-to-date information is available to the Assistant Commissioner, Correctional Operations and Programs

   c. ensure that all Business Continuity Plans (e.g. contingency plans, disaster recovery plans, emergency plans) are reviewed, updated and approved, that they are inserted into the Crisis Response and Security Information Management System (CRSIMS), and that a signed paper copy is located in the National Headquarters Crisis Centre/Emergency Operations Centre by March 31st of every year

   d. ensure Business Continuity Plans in each sector are exercised at least every 12 months and report the results via email to GEN-NHQ Business Continuity Program.

5. The Departmental Security Officer will:

   a. direct the national Business Continuity Program by developing and publishing policies, requirements and guidelines on Business Continuity Plans

   b. implement a National Business Continuity Program which falls under the authority of the Treasury Board Policy on Government Security

   c. provide strategic direction and advice and ensure that accurate, up-to-date information is available to the Director General, Security Branch

   d. provide annual progress report with regard to the Business Continuity Program to the Executive Committee.

6. The National Business Continuity Program Coordinator will:

   a. develop National Business Continuity Program policies, requirements, guidelines and governance

   b. provide advice and assistance to various sectors and regions in developing and implementing their Business Continuity Plan

   c. communicate business continuity program activities to employees and stakeholders

   d. establish committees, working groups and teams with defined roles and responsibilities to meet program requirements and effectively respond to emergencies and service disruptions

e. ensure the completion of the business impact analysis and maintaining an inventory of CSC's critical business functions

f. ensure that Information Management/Information Technology and other continuity plans and arrangements are fully integrated into the Business Continuity Program

g. provide for regular training for employees having responsibilities in dealing with emergency situations, review, testing and audit of Business Continuity Plans for branches and sectors

h. liaise with other departments and agencies as necessary to coordinate Business Continuity Plans

i. direct the business continuity exercise program.

7. The Chief Information Officer and the Manager, Information Technology Security, will ensure that the Information Management Services Branch carries out the Business Continuity Program requirements pursuant to CD 225 – Information Technology Security.

8. CSC's Information Technology Continuity team, in partnership with business function managers, is responsible for ensuring that a comprehensive Information Technology Continuity Plan is developed, implemented and tested for all critical business functions. Responsibilities include:

   a. developing Disaster Recovery Plan standards, guidelines, models, processes and tools

   b. supporting the Business Continuity Program

   c. providing training to support the Disaster Recovery Plan

   d. maintaining a database of completed Disaster Recovery Plans

   e. executing information systems infrastructure recovery.

9. The Institutional Head/District Director will:

   a. manage the Crisis Centre/Emergency Operations Centre

   b. provide strategic advice and guidance during a crisis to ensure that accurate, up-to-date information is available to the Assistant Deputy Commissioner, Integrated Services

   c. ensure that all Business Continuity Plans (e.g. contingency plans, disaster recovery plans, emergency plans) are reviewed, updated and approved, that they are inserted into the CRSIMS, and that a signed paper copy is sent to National Headquarters, Business Continuity Program, by March 31st of every year

   d. ensure regional Business Continuity Plans are exercised at least every 12 months and report the results via email to GEN-NHQ Business Continuity Program

e. participate in training and exercises to ensure the plans remain current and effective.

10. The designated Regional Business Continuity Program Coordinator will:

a. collaborate with the National Business Continuity Program Coordinator

b. provide awareness/training sessions as well as advice and guidance

c. review the format and content of all Business Continuity Plans for regional sites

d. provide annually and as required, an electronic copy of regional Business Continuity Plans (e.g. contingency plans, disaster recovery plans, emergency plans) in CRSIMS, and a hard copy to the National Business Continuity Program Coordinator at National Headquarters.

ENQUIRIES

11. Strategic Policy Division
National Headquarters
Email: Gen-NHQPolicy-Politi@csc-scc.gc.ca

Commissioner,

Original Signed by:
Don Head

ANNEX A

CROSS-REFERENCES AND DEFINITIONS

CROSS-REFERENCES

CD 225 – Information Technology Security
GL 318-3 – Environmental Emergency Plan
CD 345 – Fire Safety
CD 600 – Management of Emergencies
CD 800 – Health Services

Tabletop Exercise Guide for the Correctional Service of Canada

Canada Labour Code

Treasury Board Directive on Departmental Security Management
Treasury Board Fire Protection Standard
Treasury Board Operational Security Standard – Business Continuity Planning (BCP) Program
Treasury Board Policy on Government Security
Treasury Board Standard for Fire Safety Planning and Fire Emergency Organization – Chapter 3-1
Public Safety Canada Federal Emergency Response Plan
Public Safety Canada Emergency Management Planning Guide
Public Safety Canada All Hazards Risk Assessment Methodology Guidelines
Public Works and Government Services Canada Emergency Management Vocabulary

DEFINITIONS

Assets: tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.

Business Continuity Plan (BCP): a plan developed to provide procedures and information for the continuity and/or recovery of critical service delivery and business operations in the event of a disruption.

Business Continuity Program: an integrated management process involving the development and implementation of activities that provides for the continuity and/or recovery of critical service delivery and business operations in the event of a disruption.

Business Impact Analysis: the process of determining the impact on an organization should a potential loss identified by the risk analysis actually occur. The business impact analysis should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial, loss of life or other standpoint.

Contingency Plan: a plan developed for a specific event or incident.

Crisis: a situation that threatens public safety and security, the public's sense of tradition and values or the integrity of the government.
*Note: The terms "**crisis**" and "emergency" are not interchangeable. However, a **crisis** may become an emergency. For example, civil unrest over an unpopular government policy may spark widespread riots.*

Critical Services: services whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the effective functioning of the Government of Canada.

Emergency: a present or imminent event that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment.
*Note: The terms "crisis" and "**emergency**" are not interchangeable. However, a crisis may become an **emergency**. For example, civil unrest over an unpopular government policy may spark widespread riots.*

Exercise: a simulated scenario or live situation in which an organization practises its response activities to test its contingency plan and Business Continuity Plan (BCP). The annual exercises will be carried out in order to randomly test, in a non-repetitive manner, each contingency plan and Business Continuity Plan. The outcome of an exercise is to allow an organization to reveal planning weaknesses or gaps in resources, improve organizational coordination and communications, clarify roles and responsibilities, improve individual performance and satisfy regulatory requirements.

***For additional definitions**, refer to the Public Works and Government Services Canada Emergency Management Vocabulary which lists over 200 terms and definitions for concepts used in emergency management.