



Government
of Canada

Gouvernement
du Canada

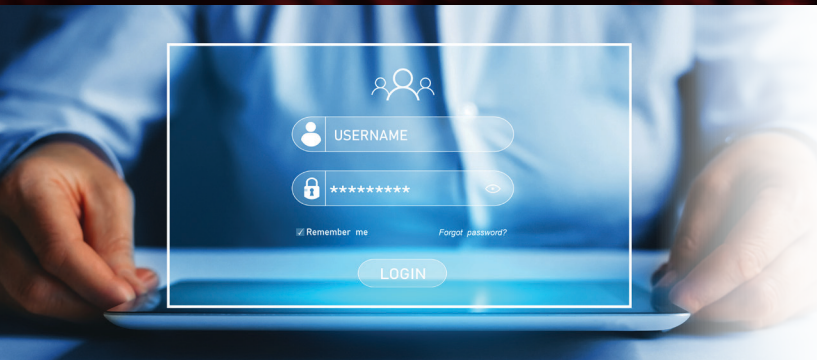
BIOSECURITY ADDENDUM

to the Canadian Biosafety Standard, Third Edition


For Containment Level 4 Facilities



**RESTRICTED
AREA**
**AUTHORIZED
PERSONNEL ONLY**



 USERNAME

 ***** 

Remember me [Forgot password?](#)

LOGIN

Canada 

TO PROMOTE AND PROTECT THE HEALTH OF CANADIANS THROUGH LEADERSHIP,
PARTNERSHIP, INNOVATION AND ACTION IN PUBLIC HEALTH.

—Public Health Agency of Canada

Également disponible en français sous le titre :

Addenda de biosûreté apporté à la Norme canadienne sur la biosécurité, troisième édition

Information contained in this publication or product may be reproduced, in whole or in part, and by any means, for personal or public non-commercial purposes without charge or further permission, unless otherwise specified. Commercial reproduction and distribution are prohibited except with written permission from the Public Health Agency of Canada. To obtain permission to reproduce any content owned by the Government of Canada available for commercial purposes, please contact pubsadmin@hc-sc.gc.ca.

To obtain additional information, please contact:

Public Health Agency of Canada
130 Colonnade Rd
A.L 6501H
Ottawa, ON K1A 0K9
Toll free: 1-844-280-5020
Fax: 613-941-5366
TTY: 1-800-465-7735
E-mail: publications-publications@hc-sc.gc.ca

© His Majesty the King in Right of Canada, as represented by the Minister of Health, 2024

Publication date: December 2024

Cat.: Not applicable
ISBN: Not applicable
Pub.: 240690

CONTENTS

ABBREVIATIONS AND ACRONYMS	iv
GLOSSARY	vi
CHAPTER 1 – INTRODUCTION	2
1.1 Scope.....	2
1.2 Biosecurity Concepts	3
1.2.1 Protection, Detection, Response, Recovery (PDRR)	3
1.2.2 Sensitive Information	4
1.2.3 Biosecurity Barriers	4
1.3 Risk-Based Exemptions to Biosecurity Requirements	6
1.4 How to Use the <i>Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition</i>	6
CHAPTER 2 – BIOSECURITY REQUIREMENTS	10
Matrix A.1 – Biosecurity Documentation.....	10
Matrix A.2 – Perimeter Security.....	12
Matrix A.3 – Biosecurity Barriers	14
Matrix A.4 – Access Controls	17
Matrix A.5 – Security Systems and Devices.....	19
Matrix A.6 – Transfer Security.....	23
Matrix A.7 – Personnel Security and Identification	26
Matrix A.8 – Security Procedures and Responsibilities	29
Matrix A.9 – Training and Exercises.....	31
Matrix A.10 – Information Management and Security	35
Matrix A.11 – Accountability Measures and Inventory Control.....	37
REFERENCES	40
Legislation	40
Guidance Documents.....	40
General Resources	40
Technical Standards and Codes.....	41

Abbreviations and Acronyms



ABBREVIATIONS AND ACRONYMS

2FA	Two-factor authentication
Ag	Agriculture (i.e., CL2-Ag, CL3-Ag)
CBS	<i>Canadian Biosafety Standard, Third Edition</i>
CCVE	Closed circuit video equipment
CFIA	Canadian Food Inspection Agency
CL	Containment level (i.e., CL1, CL2, CL3, CL4)
HAA	<i>Health of Animals Act</i>
HAR	<i>Health of Animals Regulations</i>
HPTA	<i>Human Pathogens and Toxins Act</i>
HPTR	<i>Human Pathogens and Toxins Regulations</i>
HVAC	Heating, ventilation, and air conditioning
ID	Identification
IDS	Intrusion detection system
IT	Information technology
PDRR	Protection, detection, response, recovery
PHAC	Public Health Agency of Canada
RG	Risk group (i.e., RG1, RG2, RG3, RG4)
SSBA	Security sensitive biological agent

Glossary



GLOSSARY

While some of the definitions provided in the glossary are universally accepted, many are specific to the *Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition* (the *Biosecurity Addendum*); therefore, some definitions may not be applicable to facilities that fall outside the scope of the *Biosecurity Addendum*. Definitions taken from the *Canadian Biosafety Standard, Third Edition* (CBS) are provided for convenience and are indicated by an asterisk (*).

<p>Access control system*</p>	<p>A physical or electronic system designed to restrict access to authorized personnel only (e.g., key locks, electronic access cards).</p>
<p>Authorized personnel*</p>	<p>Individuals who have been granted unescorted access past biosecurity barriers, or to the containment zone, by an internal authority (e.g., the containment zone director, biological safety officer, another individual to whom this responsibility has been assigned). Access to these areas and related assets (e.g., sensitive information, equipment, critical support systems) is dependent on personnel completing training requirements and demonstrating proficiency in the standard operating procedures, as determined by the training needs assessment. Additional criteria for granting access include possessing the appropriate security clearance (e.g., <i>Human Pathogens and Toxins Act</i> Security Clearance) or baseline security check and having a need-to-know, as determined by the biosecurity risk assessment for the areas and related assets.</p>
<p>Baseline security check</p>	<p>An assessment conducted by the organization in accordance with their risk tolerance for granting or refusing access, based on a documented confirmation of the need for site access, a confirmation of identity, and a criminal record check.</p>
<p>Biosecurity*</p>	<p>Security measures designed to prevent the loss, theft, misuse, diversion, or intentional release of regulated materials, and other related assets (e.g., personnel, equipment, non-infectious material, animals, sensitive information).</p>
<p>Biosecurity barrier</p>	<p>Obstructions preventing unauthorized access to the containment zone and related assets (e.g., sensitive information, equipment, critical support systems). Biosecurity barriers are designed and implemented as determined by a biosecurity risk assessment. Biosecurity barriers can be physical or logical in nature. Physical biosecurity barriers can be active (e.g., doors, gates) or passive (e.g., fences, walls). Logical biosecurity barriers are measures within digital systems for credential authentication, authorization, and accountability.</p>

Biosecurity incident	In the context of the <i>Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition</i> , an act, occurrence, or omission (e.g., failure to take reasonable care) leading to the loss, theft, misuse, diversion, sabotage, or unauthorized intentional release of regulated materials or related assets (e.g., sensitive information, equipment, critical support systems), or a biosecurity barrier breach.
Biosecurity risk assessment*	A risk assessment in which the regulated materials, and other related assets (e.g., equipment, animals, sensitive information, personnel, non-infectious material) are defined and prioritized, the likelihood of threats, vulnerabilities, and associated consequences are assessed, and appropriate mitigation strategies are recommended to protect these assets against potential biosecurity events.
Closed circuit video equipment (CCVE)	A wired security camera system providing live monitoring, recording, and video management to a central security monitoring station.
Community*	Encompasses both human (i.e., the public) and animal populations.
Containment*	The combination of physical design parameters and operational practices that protect personnel, the immediate work environment, and the community from exposure to biological material. The term “biocontainment” is also used in this context.
Containment barrier*	The physical structures or barriers that create a boundary between “clean” and “dirty” areas or between areas of lower contamination and higher contamination (e.g., between the laboratory work areas, large scale production areas, animal rooms, animal cubicles, or post mortem rooms, and outside that containment area). The containment barrier itself is created by the walls, doors, floors, and ceilings of a room that physically enclose the areas within containment, as well as inward airflow at critical doors (where inward airflow is required).
Containment level (CL)*	Minimum physical containment and operational practice requirements for handling regulated materials safely in laboratory, large scale production, and animal work environments. There are four containment levels ranging from a basic laboratory (i.e., CL1) to the highest level of containment (i.e., CL4).

Containment zone*	A physical area that meets the requirements for a specified containment level. A containment zone can be a single room (e.g., a Containment Level 2 [CL2] laboratory), a series of co-located rooms (e.g., several non-adjoining but lockable CL2 laboratory work areas), or it can be comprised of several adjoining rooms (e.g., a CL3 suite with dedicated laboratory areas, and separate animal rooms or animal cubicles). Dedicated support areas, including anterooms with showers and “clean” and “dirty” change areas where required, are considered to be part of the containment zone.
Controlled zone	A designated area surrounded by a physical or perceived boundary, which clearly separates it from non-controlled spaces.
Critical support system	Critical equipment supporting the function and security of the containment zone. Examples of critical support systems include heating, ventilation, and air conditioning (HVAC), air handling, effluent decontamination systems, supervisory control and data acquisition (SCADA) systems, security systems, and information technology (IT) systems.
Exporting*	The activity of shipping (e.g., transferring, transporting) regulated materials from Canada to another country or jurisdiction. In the context of the <i>Canadian Biosafety Standard, Third Edition</i> , this term does not apply to any activity to which the <i>Transportation of Dangerous Goods Act, 1992</i> applies, or to the export of pathogens or toxins authorized under the <i>Export and Import Permits Act</i> .
Facility*	Structures or buildings, or defined areas within structures or buildings, where regulated materials are handled or stored. This could include individual research and diagnostic laboratories, large scale production areas, or animal housing zones. A facility could also be a suite or building containing more than one of these areas.
Handling or storing*	“Handling or storing” regulated materials includes possessing, handling, using, producing, storing, permitting access to, transferring, importing, exporting, releasing, disposing of, or abandoning such material. This includes all controlled activities involving human pathogens and toxins specified in subsection 7(1) of the <i>Human Pathogens and Toxins Act</i> . All tenses and variations of “handling or storing” are also used in this context.

Hazard*	A source of potential damage, harm, or adverse effects. In the context of biosafety, examples include objects (e.g., sharps, needles), materials (e.g., pathogens, toxins), animals (e.g., bites, scratches), and situations (e.g., containment system failure).
<i>Human Pathogens and Toxins Act</i> (HPTA) Security Clearance*	An authorization following verification of an individual's background and reliability status issued by the Public Health Agency of Canada under section 34 of the <i>Human Pathogens and Toxins Act</i> .
Importing*	The activity of bringing (e.g., transferring, transporting) regulated materials into Canada from another country or jurisdiction. In the context of the <i>Canadian Biosafety Standard, Third Edition</i> , this term does not apply to any activity to which the <i>Transportation of Dangerous Goods Act, 1992</i> applies.
Intrusion detection system (IDS)*	A technology that allows for monitoring and analysis of alarm devices for signs of unauthorized access and malicious activities. An IDS alerts security personnel when it detects suspicious patterns or behaviours at and within physical and logical biosecurity barriers.
Inventory*	A list of (biological) assets associated with a containment zone identifying regulated materials in long-term storage (i.e., beyond 30 days) both inside and outside the containment zone.
Key control*	A mechanism for preventing unauthorized duplication of, or unauthorized access to, keys or key cards (i.e., access cards) and for documenting authorized individuals who have been issued a key or key card. Key control may include the use of keys or key cards that cannot be copied or that are not readily available on the market, or procedures to prevent keys or key cards from leaving the building (e.g., exchanged for a personal item [e.g., identification card, device], electronic tracking system that records when a key or key card was issued and returned, and to whom).
Laboratory*	An area within a facility or the facility itself where biological material is handled.
Licence*	See "Pathogen and Toxin Licence".
Long-term storage*	In the context of the <i>Canadian Biosafety Standard, Third Edition</i> , the possession of regulated materials beyond 30 days of receipt or creation.
Mechanism*	A physical or operational measure.

Movement*	The action of moving (e.g., bringing, carrying, leading, relocating) people, material (including regulated materials), or animals from one physical location to another physical location in the same building. This can include movement within the same containment zone, to a different containment zone, or to another location within the same building.
Need-to-know*	A fundamental principle of security that restricts access to specific areas, regulated materials, and related assets (e.g., sensitive information, equipment, critical support systems) to individuals who need it as part of their job responsibilities. Only individuals who have a legitimate reason or authorization based on their job responsibilities may access specific areas and related assets.
Notification report*	A tool used to notify the Public Health Agency of Canada and document preliminary information for an incident (e.g., exposure; inadvertent possession, production or release; missing, stolen or lost pathogen).
Pathogen*	A microorganism, nucleic acid, protein, or other infectious agent that is transmissible and capable of causing disease or infection in humans or animals. Classified human and animal pathogens can be found on the Public Health Agency of Canada's ePATHogen – Risk Group Database.
Pathogen and Toxin Licence*	<p>An authorization issued by the Public Health Agency of Canada:</p> <ul style="list-style-type: none"> a) under section 18 of the <i>Human Pathogens and Toxins Act</i> to conduct one or more controlled activities with human pathogens or toxins; and/or b) under paragraph 51(a) of the <i>Health of Animals Regulations</i> for the importation into Canada of terrestrial animal pathogens (except for emerging animal disease pathogens and non-indigenous terrestrial animal pathogens). <p>“Licence” is also used in this context.</p>
Premises	The physical locations, buildings, and associated areas under the ownership, control, or operation of an individual or organization. Premises encompass all facilities, land, and spaces where organizational operations, activities, or assets are present.

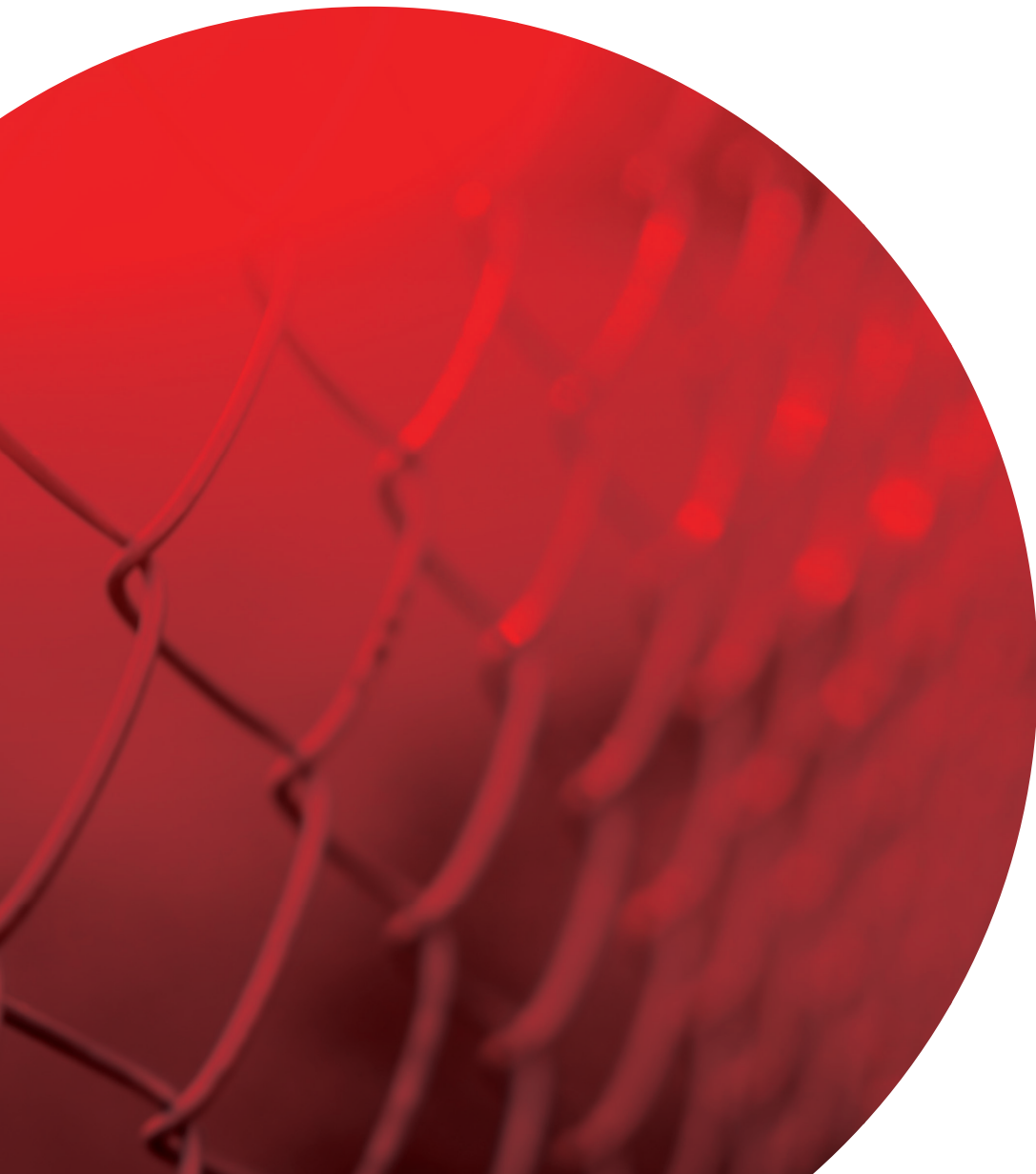
<p>Regulated animal*</p>	<p>In the context of the <i>Canadian Biosafety Standard, Third Edition</i>, regulated animals include:</p> <ul style="list-style-type: none"> • animals experimentally infected or intoxicated with a human pathogen or toxin (under the <i>Human Pathogens and Toxins Act</i> and <i>Human Pathogens and Toxins Regulations</i>); and • animals naturally or experimentally infected or intoxicated with a terrestrial animal pathogen or part of one (e.g., toxin), including those known or suspected to be infected or intoxicated (under the <i>Health of Animals Act</i> and <i>Health of Animals Regulations</i>).
<p>Regulated material*</p>	<p>In the context of the <i>Canadian Biosafety Standard, Third Edition</i>, regulated material includes:</p> <ul style="list-style-type: none"> • human pathogens and toxins (under the <i>Human Pathogens and Toxins Act</i> and <i>Human Pathogens and Toxins Regulations</i>); • terrestrial animal pathogens (under the <i>Health of Animals Act</i> [HAA] and <i>Health of Animals Regulations</i> [HAR]); and • terrestrial animal pathogens in animals, animal products, animal by-products, or other organisms (under the HAA and HAR).
<p>Release*</p>	<p>The discharge of regulated materials from a containment system or containment zone (e.g., resulting from leaking, spraying, depositing, dumping, vaporizing).</p>
<p>Risk group (RG)*</p>	<p>The classification of a biological agent (i.e., microorganism, protein, nucleic acid, or biological material containing parts thereof) based on its inherent characteristics, including pathogenicity, virulence, communicability, and the availability of effective prophylactic or therapeutic treatments. The risk group describes the risk to the health of individuals and the public, as well as the health of animals and the animal population.</p>
<p>Security sensitive biological agents (SSBAs)*</p>	<p>The subset of human pathogens and toxins that have been determined to pose an increased biosecurity risk due to their potential for use as a biological weapon. SSBAs are identified as prescribed human pathogens and toxins by section 10 of the <i>Human Pathogens and Toxins Regulations</i> (HPTR). This means all Risk Group 3 and Risk Group 4 human pathogens that are in the <i>List of Human and Animal Pathogens and Toxins for Export Control</i>, published by the Australia Group, as amended from time to time, with the exception of Duvenhage virus, Rabies virus and all other members of the Lyssavirus genus, Vesicular stomatitis virus, and Lymphocytic choriomeningitis virus; as well as all toxins listed in Schedule 1 of the <i>Human Pathogens and Toxins Act</i> that are listed on the <i>List of Human and Animal Pathogens and Toxins for Export Control</i> when in a quantity greater than that specified in subsection 10(2) of the HPTR.</p>

<p>Security sensitive biological agent (SSBA) zone*</p>	<p>Part of the facility where controlled activities with SSBA are authorized as defined in the <i>Human Pathogens and Toxins Act</i> (HPTA). This zone can be an enclosed room, combination of rooms, or equipment where SSBA are handled or stored and to which access is restricted to authorized personnel who hold a valid HPTA Security Clearance issued by the Public Health Agency of Canada.</p>
<p>Security system*</p>	<p>The array of security technologies within a defined area designed to monitor for signs of unauthorized access and malicious activities against an organization's assets, individuals, and information.</p>
<p>Sensitive information*</p>	<p>In the context of the <i>Canadian Biosafety Standard, Third Edition</i>, documents and any other information pertaining to regulated materials or related assets, of which the unauthorized disclosure, access, use, modification, or destruction could be reasonably expected to:</p> <ul style="list-style-type: none"> • compromise biosecurity; or • cause undue risk to the health or safety of the community.
<p>Terrestrial animal pathogen import permit*</p>	<p>A permit issued under paragraph 51(a) and (b) of the <i>Health of Animals Regulations</i> by the Public Health Agency of Canada or the Canadian Food Inspection Agency for the importation into Canada of terrestrial animal pathogens or part of one (e.g., toxin); or animals, animal products, animal by-products (e.g., tissue, serum), or other organisms carrying a terrestrial animal pathogen or part of one (e.g., toxin).</p>
<p>Terrestrial animal pathogen transfer permit*</p>	<p>A permit issued under paragraph 51.1(a) of the <i>Health of Animals Regulations</i> by the Public Health Agency of Canada or the Canadian Food Inspection Agency for the transfer of terrestrial animal pathogens or part of one (e.g., toxins); or animals, animal products, animal by-products (e.g., tissue, serum), or other organisms carrying a terrestrial animal pathogen or part of one (e.g., toxin).</p>
<p>(Microbial) Toxin*</p>	<p>A poisonous substance that is produced by or derived from a microorganism and can lead to adverse health effects in humans or animals. Human toxins are listed in Schedule 1 and Part 1 of Schedule 5 in the <i>Human Pathogens and Toxins Act</i>.</p>
<p>Training needs assessment*</p>	<p>An evaluation performed to identify the current and future training needs of the facility (i.e., organization, containment zone), including training, refresher training, and retraining, and to identify gaps in the current training program.</p>

Transfer*	A change in possession of regulated materials between individuals from the same or different facilities (i.e., the movement from the place or places specified in the licence or terrestrial animal pathogen import permit to any other place).
Transportation*	The act of transporting (e.g., shipping, conveyance) regulated materials to another building or location (i.e., different address), within Canada or abroad, in accordance with the <i>Transportation of Dangerous Goods Act and Regulations</i> .

Chapter 1

Introduction



CHAPTER 1 – INTRODUCTION

The *Canadian Biosafety Standard, Third Edition* (CBS) establishes requirements for the design, structure, and operation of **containment zones** to protect humans, animals, and the environment from the risks posed by certain **pathogens** and **toxins**.

This *Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition* (the *Biosecurity Addendum*) aims to strengthen **biosecurity** oversight of the highest **containment facilities**. It outlines the physical, operational, and information technology (IT) mitigation measures to protect **regulated materials**, including **regulated animals**, and related assets from loss, theft, misuse, diversion, sabotage, or unauthorized intentional **release**. The purpose of this document is to specify conditions related to biosecurity for **Risk Group 4 (RG4) Pathogen and Toxin Licence, terrestrial animal pathogen import permit, and terrestrial animal pathogen transfer permit** holders. The requirements found in the *Biosecurity Addendum* apply not only to the containment zone, but the **premises** in which the containment zone is housed.

As research in the life sciences expands, the protection of regulated materials and **sensitive information** is paramount. The *Biosecurity Addendum* establishes biosecurity requirements that aim to protect biological **laboratories** against threats, ultimately protecting the health and safety of the **community**.

1.1 Scope

Facilities that have been issued an RG4 Pathogen and Toxin Licence (hereafter, licence) under the *Human Pathogens and Toxins Act* (HPTA) and the *Human Pathogens and Toxins Regulations* (HPTR), as well as facilities that have been issued an RG4 terrestrial animal pathogen import permit or a terrestrial animal pathogen transfer permit under the *Health of Animals Act* (HAA) and the *Health of Animals Regulations* (HAR) must comply with the applicable requirements set out in the CBS, including the *Biosecurity Addendum*, as a condition of their licence or permit.

It remains the responsibility of the licence or permit holder to understand their obligations under the HPTA, HPTR, HAA, and HAR, in addition to the conditions of their licence or permit, which include abiding by the applicable requirements set out in the CBS and the *Biosecurity Addendum*. Should there be any perceived conflict between the acts, the regulations, the CBS, and the *Biosecurity Addendum*, the acts and regulations prevail.

1.2 Biosecurity Concepts

1.2.1 Protection, Detection, Response, Recovery (PDRR)

The four pillars of biosecurity mitigation measures are protection, detection, response, and recovery:

- **Protection:** deter, deny, delay threats
- **Detection:** detect and monitor
- **Response:** assess and investigate alarms, engage threats or call for service from off-site response force (e.g., local law enforcement)
- **Recovery:** return to normal operations

These can be achieved through a combination of physical and operational mitigation measures. A performance-based approach to meeting biosecurity objectives offers flexibility in applying different combinations of PDRR mitigation measures, which takes into consideration an organization's unique circumstances and the environment in which it operates. The PDRR cycle is depicted in Figure 1-1.

Figure 1-1: PDRR cycle



1.2.2 Sensitive Information

Sensitive information covers documents and any other information pertaining to regulated materials or related assets, of which the unauthorized disclosure, access, use, modification, or destruction could be reasonably expected to compromise biosecurity or cause undue risk to the health and safety of the community. Traditionally, physical security enclosures have been used to secure hard copies. Today, most sensitive information is created and stored in electronic format. Sensitive information is only available to individuals with the **need-to-know** and appropriate security clearance or **baseline security check**. The compromise of any format may affect the confidentiality, integrity, and availability of sensitive information in the possession of an organization. Information found in, and about, **critical support systems** may also be considered sensitive and needs to be safeguarded to maintain biosecurity. Having appropriate measures in place to safeguard sensitive information ultimately protects the health and safety of the community.

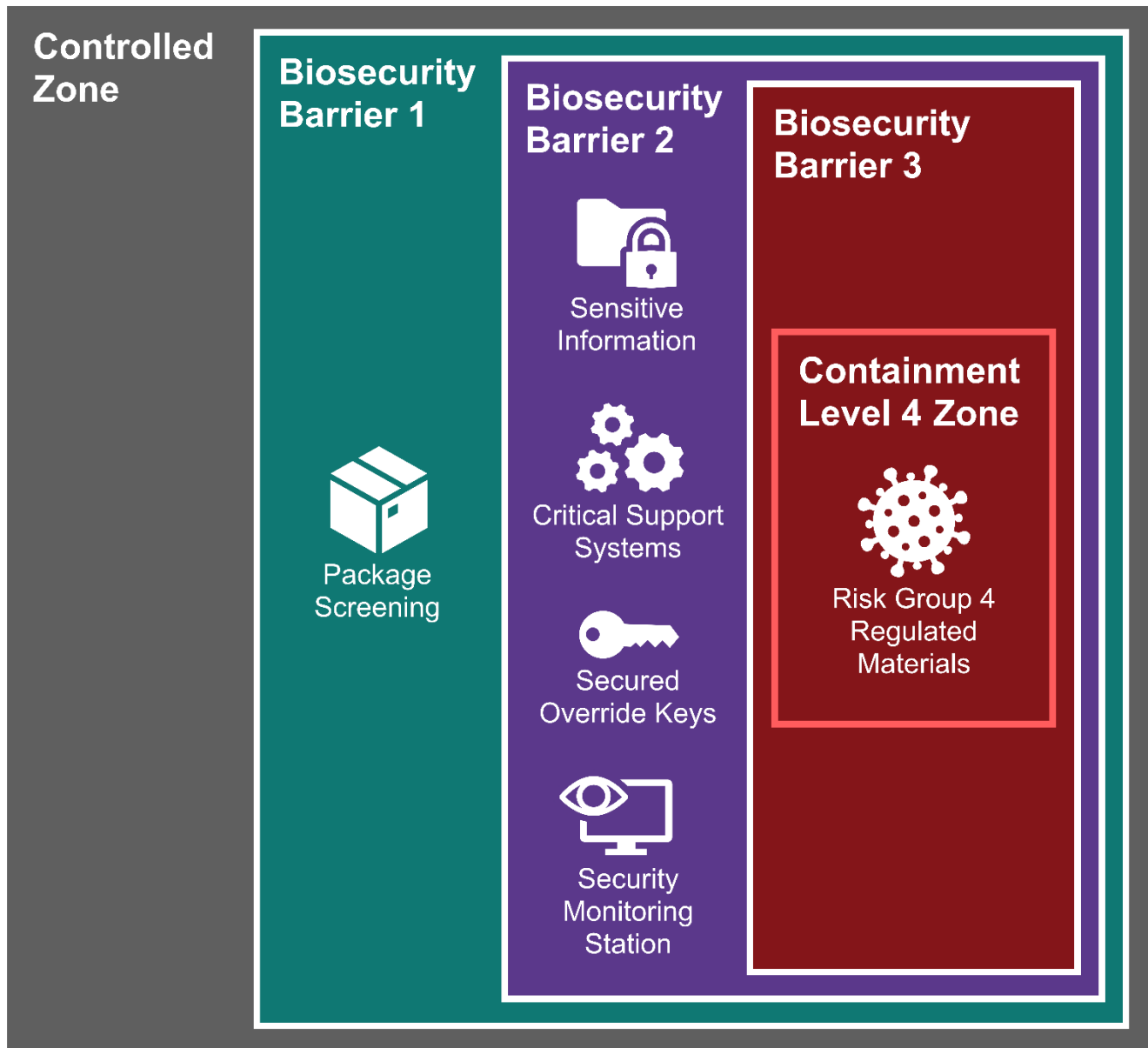
1.2.3 Biosecurity Barriers

Biosecurity barriers are obstructions that serve to deter, deny, and delay access to regulated materials, sensitive information, and critical support systems. Establishing a sequence of biosecurity barriers collectively denies and delays unauthorized access into increasingly secure areas. The robustness of each biosecurity barrier must provide delay to allow for a security response. This is commonly referred to as graded protection, which is an effective way to decrease the likelihood of a successful attack.

Physical biosecurity barriers can be active (e.g., doors, gates) or passive (e.g., fences, walls). Logical biosecurity barriers are cybersecurity controls that protect computer networks from unauthorized access. Logical biosecurity barriers include measures for credential authentication, authorization, and accountability within digital systems.

Figure 1-2 illustrates the nesting of zones and provides a visual representation of the three-barrier model used in the *Biosecurity Addendum*.

Figure 1-2: Nested biosecurity barriers to protect increasingly secure areas and assets



The solid white line around each zone represents biosecurity barriers. The solid red line around the **Containment Level 4 (CL4)** zone represents the **containment barrier**.

Table 1-1 provides a non-exhaustive visual representation of the security measures at each biosecurity barrier.

Table 1-1: Security measures for different biosecurity barriers

Security Measures	Controlled Zone	Biosecurity Barrier 1	Biosecurity Barrier 2	Biosecurity Barrier 3
Access Control (Two-Factor Authentication [2FA])				✓
Access Control		✓	✓	✓
Intrusion Detection Mechanisms (x2)		✓	✓	✓
Alarmed Emergency Egress		✓	✓	✓
Closed circuit video equipment (CCVE)	✓	✓	✓	✓
Adequate Lighting	✓	✓	✓	✓

1.3 Risk-Based Exemptions to Biosecurity Requirements

Exemptions to specific biosecurity requirements will be considered by the Public Health Agency of Canada (PHAC) and the Canadian Food Inspection Agency (CFIA) on a case-by-case basis, provided that it can be demonstrated that the intent of the requirement in question has been met through an alternative **mechanism**, as determined by a **biosecurity risk assessment**.

1.4 How to Use the *Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition*

The structure of the *Biosecurity Addendum* is aligned with the CBS. This section summarizes how to use this document. For more information, refer to [Section 2 of the CBS](#).

A detailed list of all abbreviations and acronyms used throughout this *Biosecurity Addendum* is located at the beginning of this document. A comprehensive glossary for technical terms is located at the beginning of this document; words defined in the glossary appear in **bold type** upon first use in each chapter and, in Chapter 2, in each section or matrix. The terminology used in this *Biosecurity Addendum* is to be interpreted according to the corresponding definitions provided in the glossary. A list of additional resources is provided at the end of the document.

The requirements for facilities and surrounding premises where RG4 regulated materials are **handled and stored** are provided in Chapter 2. The requirements are risk- and evidence-based, and, where possible, more performance-based than explicitly prescriptive. Chapter 2 describes the requirements that are to be met in order to uphold biosecurity in CL4 facilities.

The requirements in Chapter 2 are presented in a series of matrices (or tables) in which the applicability of each requirement to specific containment levels is indicated. In alignment with the CBS, the requirements are grouped by topic into multiple matrices that contain separate CL2, CL3, and CL4 columns. **It is important to note that, in the context of the *Biosecurity Addendum*, the applicability to a containment level extends to the premises in which the facility is located.**

Throughout Chapter 2, the following symbol is used:

- Required for all containment zones, including work areas where activities with prions and **security sensitive biological agents** (SSBAs) are conducted

The absence of a symbol in a column indicates that the element is not required for that containment level.

The Explanatory Notes, located under the requirements, provide additional information on the intent of the requirement, specifically how the risks are being mitigated by each requirement. The Explanatory Notes also include examples of how the requirement can be achieved. These are not considered specific requirements or recommendations; rather, they are provided for clarification and represent typical means of meeting a requirement.

Chapter 2

Biosecurity Requirements



CHAPTER 2 – BIOSECURITY REQUIREMENTS

Matrix A.1 – Biosecurity Documentation

An organization’s **biosecurity risk assessment** is an essential reference point for their **biosecurity** posture. It involves the establishment of risk tolerance, assessment of threats and consequences, and determination of biosecurity mitigation measures. It shapes an organization’s biosecurity plan, which is kept up to date and implemented to uphold biosecurity.

A.1	Biosecurity Documentation	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.1.1	A biosecurity risk assessment to be conducted every three years, or more frequently as necessitated by changes to the threat environment.					■

Assessing and documenting new and emerging risks allows organizations to have the capacity and capabilities to protect, detect, respond to, and recover from **biosecurity incidents**. The biosecurity risk assessment considers threats that manifest through physical or cyber attack vectors. The biosecurity risk assessment is conducted by a team of internal experts, external experts, or a combination of both. This supports the assessment of risks that may impact **facilities with regulated materials, sensitive information**, and operational technology supporting **critical support systems**, as well as the implementation of appropriate mitigation strategies. The biosecurity risk assessment also informs the choice of third-party products and services (e.g., contracts, procurement of goods) by evaluating their potential to compromise the organization’s biosecurity. The results of a biosecurity risk assessment contain sensitive information (e.g., asset **inventory**, vulnerabilities, mitigation strategies) and must be safeguarded from unauthorized access. This requirement expands on CBS requirement 4.1.5.

A.1.2	Review of the biosecurity plan to be conducted annually, documented, and approved by senior management.					■
-------	---	--	--	--	--	---

Security systems and related procedures can become obsolete or antiquated with time, or when new and emerging threats are introduced. A cyclical review of the biosecurity plan allows the organization to assess their current biosecurity mitigation measures and identify whether they need to be updated, or if new measures need to be implemented. Reviewing the biosecurity plan also promotes the continual improvement and evaluation of the biosecurity program and enhanced accountability for regulated materials. This requirement expands on CBS requirements 4.1.5 and 4.1.8.

A.1	Biosecurity Documentation	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.1.3	<p>The biosecurity plan to be reviewed and updated following:</p> <ul style="list-style-type: none"> • exercises and drills; • failures of security systems; • biosecurity incidents; • changes in the threat environment; • the conduct of a new or updated biosecurity risk assessment; or • a request from PHAC or CFIA. 					■

In addition to the annual review cycle, the biosecurity plan is reviewed following specific situations, biosecurity incidents, a change in risk, or a request from PHAC or CFIA. When applicable, the biosecurity plan is updated to confirm that mitigation strategies address new or increased physical biosecurity and cybersecurity risks. This requirement expands on CBS requirement 4.1.8.

Matrix A.2 – Perimeter Security

A perimeter is established to indicate where the **controlled zone** begins. Security measures at the perimeter are the first visible signs of an organization’s **biosecurity** posture and demonstrate that the **premises** are protected. Strong perimeter security also serves as a deterrent against potential biosecurity threats. Perimeter security measures may include perceived boundaries or physical barriers, signage for entry and exit, and landscaping design.

A.2	Perimeter Security	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.2.1	A controlled zone to be established.					■

Establishing a clear perimeter around the premises indicates that it is well protected. This can be achieved with perceived boundaries or physical **biosecurity barriers**. Perceived boundaries include hardscapes and landscapes, whereas physical biosecurity barriers include fences and gates, which deny access to all or parts of the controlled zone. A controlled zone with active monitoring, during the day and night and in all weather conditions, serves to detect imminent or immediate threats. Continuous and uniform lighting, along with appropriate lighting intensity, allows for observation and assessment of any person within the controlled zone through visual observation or **closed circuit video equipment (CCVE)**.

A.2.2	The presence of the following to be minimized in the controlled zone: <ul style="list-style-type: none"> • objects and features that offer opportunities to gain unauthorized access through openings, windows, and doors; and • features, landscapes, or hardscapes that allow persons or objects to be concealed. 					■
-------	---	--	--	--	--	---

Objects and features within and around the controlled zone can offer opportunities for concealment and may increase the risk of biosecurity barriers being breached. Loose objects could be used as projectiles to breach biosecurity barriers. A maintenance plan and removal of such objects reinforce the security of the controlled zone.

A.2.3	Signage to be posted to direct traffic to designated points of entry and exit.					■
-------	--	--	--	--	--	---

Directional signage provides clear guidance for individuals and vehicles to designated parking, shipping and receiving, and reception areas. This allows security personnel to focus their detection, denial, delay, and response efforts to designated corridors within the controlled zone. Signage is not to conflict with provincial, territorial, and local laws, regulations, and bylaws for exterior signage.

A.2	Perimeter Security	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.2.4	Strategies to be developed, documented, and implemented to mitigate vehicle- and pedestrian-borne threats in the controlled zone.					■

Following a **biosecurity risk assessment**, mitigation strategies are implemented to address vehicle- and pedestrian-borne threats. Additional passive barriers such as natural barriers, concrete planters, Jersey barriers, or bollards are considered where a vehicle ramming into the building envelope, **critical support systems**, and pedestrians is possible.

A.2.5	Procedures to prepare for and respond to imminent or elevated threats to be developed, documented, and implemented.					■
-------	---	--	--	--	--	---

Information suggesting that a threat to the **facility** is imminent or elevated may come from actionable open source or other intelligence sources. Rapid implementation of effective lockdown measures allows the organization to deny and delay entry to all unauthorized individuals at the first biosecurity barrier. Examples of procedures to respond to elevated threats include searches of individuals, equipment, and baggage upon entry and exit at the first biosecurity barrier (e.g., using metal detectors, other procedures that allow security personnel to assess threats). This prevents the introduction and removal of objects that could be used to threaten the security of **regulated materials**, **sensitive information**, and critical support systems.

Matrix A.3 – Biosecurity Barriers

Biosecurity barriers are obstructions that protect **regulated materials**, **sensitive information**, and **critical support systems**, allowing access only to those who are authorized. Physical biosecurity barriers include active barriers such as doors and gates, and passive barriers such as walls and fences.

A.3	Biosecurity Barriers	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.3.1	Containment zone to be located behind three biosecurity barriers.					■

Establishing a sequence of biosecurity barriers collectively denies and delays unauthorized access into increasingly secure areas. The combined biosecurity barriers provide enough delay to allow for a response prior to an unauthorized individual gaining access to a secure area. A **biosecurity risk assessment** will determine the types of materials to use and whether additional biosecurity barriers (e.g., perimeter fence) are needed. Figure 1-2 illustrates the biosecurity barriers surrounding each zone.

A.3.2	When at rest outside the containment zone, regulated materials to be locked in a secondary, non-movable enclosure behind three biosecurity barriers.					■
-------	--	--	--	--	--	---

Once regulated materials have been packaged for **transportation** or **movement**, they are secured within the containment zone or in a dedicated area when at rest outside the containment zone and awaiting carrier pickup. Access to this dedicated area is limited to those with a **need-to-know**. **Authorized personnel** can be designated to unlock the dedicated area for package collection. This also applies to received packages until they are moved to the containment zone. In accordance with the CBS, regulated materials cannot be stored outside the containment zone. Enclosures holding regulated materials while at rest must be non-movable, either due to their size (e.g., too heavy or large to be easily moved) or by being fixed in place (e.g., bolted to the wall or floor). The term "at rest" refers to temporary placement while awaiting pickup for transportation or other movements.

A.3.3	Critical support systems to be located behind two biosecurity barriers.					■
-------	---	--	--	--	--	---

Establishing a sequence of biosecurity barriers collectively denies and delays unauthorized access to critical support systems. The combined biosecurity barriers provide enough delay to allow for a response prior to an unauthorized individual gaining access to critical support systems. A biosecurity risk assessment will determine the types of materials to use and if additional biosecurity barriers are needed (e.g., perimeter fencing, multi-factor authentication) beyond the minimum of two biosecurity barriers for critical support systems. Figure 1-2 illustrates the biosecurity barriers surrounding each zone.

A.3	Biosecurity Barriers	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.3.4	A dedicated area for package screening to be located behind one biosecurity barrier.					■

Package screening can reduce the risk of threat objects being introduced where they could compromise **biosecurity**. Access to dedicated package screening areas is limited to those with a need-to-know. Packages are assessed for unusual details such as unexpected points of origin, unusual odours, oily or greasy stains on packaging, excessive wrapping, or no return address. Based on a biosecurity risk assessment, packages may be scanned using imaging technology upon reception.

A.3.5	Active biosecurity barriers to be secured in a closed position.					■
-------	---	--	--	--	--	---

Active biosecurity barriers (e.g., doors, gates) prevent accidental or intentional unauthorized entry, and provide access into secure areas to authorized individuals, objects, and vehicles only. Moving components in active biosecurity barriers close when they are not in use with self-closing and locking components. Passive biosecurity barriers (e.g., fences, walls) are fixed (i.e., without moving components) and continuously obstruct the transition of individuals, objects, and vehicles.

A.3.6	Windows and other openings at biosecurity barriers to be secured in a closed position at all times.					■
-------	---	--	--	--	--	---

Keeping windows locked at all times reduces the risk of them being used for unauthorized passage of persons or objects. Openable windows are avoided in designs and plans. Where windows cannot be locked, physical methods can be used to prevent their opening. Operational procedures can also be implemented to prevent windows from being unlocked or opened. This requirement expands on CBS requirement 3.1.2.

A.3.7	Signage indicating that access is restricted to be posted at physical biosecurity barriers.					■
-------	---	--	--	--	--	---

Signage is the most common way to identify areas where access is restricted to authorized personnel only. Signage indicates that the area beyond a biosecurity barrier is restricted to “authorized personnel only” and specifies conditions of entry such as “visitors must be under continuous escort”. Signage avoids providing a description of the assets (e.g., sensitive information, critical support systems) located beyond a biosecurity barrier to limit the amount of information available to individuals outside the area, as determined by the biosecurity risk assessment.

A.3	Biosecurity Barriers	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.3.8	Signage indicating emergency egress use only to be posted at emergency exit doors located on biosecurity barriers.					■

Signage posted on emergency exit doors indicating that they are to be used for emergency egress only helps prevent unauthorized entry or exit. Signage may also indicate that security personnel will be notified if the doors are used and that visual and audible alarms will be triggered upon opening. This requirement does not apply to doors that are used for multiple purposes in addition to emergency egress.

Matrix A.4 – Access Controls

Access controls are placed at **biosecurity barriers** to allow entry to authorized individuals only. They are a means of controlling access to **regulated materials**, **sensitive information**, and **critical support systems**. Access controls can also be used to track the entry and exit of individuals at biosecurity barriers, which can serve as an investigative tool in the event of a **biosecurity incident**. Examples of access controls include mechanical keys, access cards, and access codes.

A.4	Access Controls	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.4.1	Access at each active biosecurity barrier to be provided through an access control system .					■

Access control systems are designed to permit entry to and exit from areas to **authorized personnel** only. They also serve to prevent accidental, deliberate, or otherwise unauthorized entry past biosecurity barriers. Individuals such as visitors and contractors need to be escorted by authorized personnel who assumes responsibility for their access past the biosecurity barrier. The type of access control system is determined by a **biosecurity risk assessment**.

A.4.2	A record of the entry of all individuals at each biosecurity barrier to be maintained and kept on file.					■
-------	---	--	--	--	--	---

Maintaining records allows the organization to have full traceability of attendance and **movement** of personnel, visitors, contractors, and vehicles (e.g., parking, delivery, loading dock access). It is essential that the information be complete, legible, and include visitor and escort signatures. To maintain visitor traceability, logs include the visitor's name, organization, contact information, date and time of entry and exit, escort name, vehicle plate number (if applicable), areas of access, and visitor identifier number (e.g., visitor card number). Records and documentation are kept on file in accordance with CBS requirement 4.9.1. This requirement expands on CBS requirement 4.9.11.

A.4.3	A mechanism to prevent tailgating and passback at biosecurity barriers to be developed, documented, and implemented.					■
-------	---	--	--	--	--	---

Having a mechanism in place to prevent tailgating (i.e., piggybacking, tag along) and passback (i.e., an authorized user lending their credentials to another individual, leading to successive entries with the same access card) at biosecurity barriers diminishes opportunities for unauthorized or accidental entry.

A.4	Access Controls	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.4.4	Access control systems at the biosecurity barrier providing access to the containment zone to be equipped with two-factor authentication (2FA).					■

2FA prevents accidental or intentional unauthorized access to areas where critical **containment** equipment and regulated materials are located. Authorized personnel authenticate their access with personal identification number (PIN) codes or biometrics, or other secondary means of access that cannot be easily circumvented. The 2FA technology at the biosecurity barrier providing access to the containment zone is determined by a biosecurity risk assessment.

A.4.5	Electronic access control systems at biosecurity barriers, where provided, to be backed up with an alternate access control system or other acceptable mechanism.					■
-------	---	--	--	--	--	---

The use of an alternate mechanism of access control (e.g., mechanical override keys, operational procedures) during an electronic access control system failure reduces the risk of unauthorized entry into secure areas. Security personnel are permitted to authenticate authorized individuals and objects for access into secure areas.

A.4.6	Override keys to be secured behind two biosecurity barriers in a locked enclosure with key control .					■
-------	---	--	--	--	--	---

Securing override keys (e.g., grand master keys, master keys, submaster keys, security panel keys) prevents their use to gain unauthorized access past biosecurity barriers. The locked enclosure is monitored and restricts key access to authorized personnel. The list of authorized personnel, and access to the enclosure, is documented and reviewed on a regular basis to prevent the improper usage of keys.

A.4.7	Means of access to be changed or removed immediately following: <ul style="list-style-type: none"> • change of responsibilities; • dismissal or departure of personnel; or • loss, theft, or compromise to access control credentials. 					■
-------	---	--	--	--	--	---

Changing or removing keys, access cards, and access codes reduces the risk of unauthorized access, which supports the overall **biosecurity** program. Change of responsibilities may include the downgrading of personnel's level of access.

Matrix A.5 – Security Systems and Devices

Security systems and devices support monitoring and intrusion detection, and provide visual oversight from video cameras. An organization’s **biosecurity** posture includes the implementation and monitoring of security systems and devices as well as procedures for continuous oversight in case of failure. Examples of security systems and devices include cameras and video equipment, **intrusion detection systems** (IDSs), monitoring stations, lighting, and equipment provided to on-site security personnel.

A.5	Security Systems and Devices	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.5.1	CCVE cameras to provide coverage: <ul style="list-style-type: none"> • of all active biosecurity barriers; and • throughout the premises, as determined by a biosecurity risk assessment. 					■

The strategic placement of CCVE cameras allows security personnel to assess, investigate, and where possible, detect threats throughout the **controlled zone** and premises. Using high resolution imagery helps with the identification of individuals, assessments (e.g., tripped alarms), and investigations. Software analytics or continuous active monitoring by security personnel support the occupation of secure areas by authorized individuals, vehicles, and objects only. Where possible, the placement, height, orientation, and resolution of CCVE cameras are considered to optimize their efficacy. The placement and configuration of CCVE cameras is not to be in conflict with federal, provincial, and territorial laws (e.g., privacy).

A.5.2	CCVE footage to be: <ul style="list-style-type: none"> • recorded at all times; • kept on file for 30 days during normal operations; and • kept on file for 10 years when related to a biosecurity incident. 					■
-------	--	--	--	--	--	---

The CCVE system records 24 hours per day, 7 days per week. CCVE footage is retained for 30 days. CCVE footage relevant to biosecurity incident investigations is kept on file for 10 years.

A.5.3	CCVE systems to have tamper-evident and tamper-resistant technology and configurations.					■
-------	---	--	--	--	--	---

CCVE systems having tamper-evident and tamper-resistant technology supports their continuous function and safeguards the security of the premises. Tamper-resistant configurations contribute to the security of the video recording system, camera housings, cabling, and system settings. This supports the restriction of access and permits changes to the system made only by **authorized personnel**.

A.5	Security Systems and Devices	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.5.4	Lighting to be provided throughout the premises to support threat detection and identification at all times and in all weather conditions.					■

Lighting throughout the premises is a fundamental component of physical security. Light assessments will determine the proper fixture type, bulb type, configuration, illumination, and placement, which are integral for threat detection, assessment, and response. This supports natural surveillance, natural access control, and territorial reinforcement.

A.5.5	Two independent intrusion detection mechanisms to provide coverage at, and within, each biosecurity barrier.					■
-------	---	--	--	--	--	---

Two independent intrusion detection mechanisms provide redundancy in the event that one mechanism is circumvented or malfunctions. The same mechanism may be used for multiple biosecurity barriers as long as two mechanisms independent from each other are present at each biosecurity barrier. Intrusion detection mechanisms include IDSs and operational alternatives (e.g., personnel occupying the area during working hours).

A.5.6	Intrusion detection mechanism type to be determined by a biosecurity risk assessment.					■
-------	---	--	--	--	--	---

The biosecurity risk assessment will inform the choice of intrusion detection mechanism at, and within, each biosecurity barrier. It is best practice to select equipment that is certified by a recognized certification body, which confirms that a technology has been evaluated by a competent organization. Intrusion detection mechanisms include IDSs and operational alternatives (e.g., personnel occupying the area during working hours).

A.5.7	IDS devices, where provided, to have tamper-evident and tamper-resistant technology and configurations.					■
-------	---	--	--	--	--	---

IDS devices, where provided, are equipped with tamper-evident technology (e.g., tamper switches, double end-of-line resistors). Tamper-resistant technology reduces the risk of a device being compromised either by increasing the time, skill, level of effort, or tools needed to circumvent it.

A.5.8	Electronic access control systems , where provided, to have tamper-evident and tamper-resistant technology and configurations.					■
-------	---	--	--	--	--	---

Electronic access control systems, where provided, are equipped with tamper-evident technology (e.g., tamper switches, double end-of-line resistors). Tamper-resistant technology reduces the risk of a device being compromised either by increasing the time, skill, level of effort, or tools needed to circumvent it.

A.5	Security Systems and Devices	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.5.9	Security personnel to be immediately alerted of active or imminent biosecurity incidents.					■

Mechanisms (e.g., security systems, operational procedures) to immediately alert security personnel allow for rapid assessment and response to disrupt a biosecurity incident. Blue light emergency phones and call boxes, or similar technologies to call for assistance, can be installed at strategic locations throughout the premises. Devices (e.g., under-desk mounted panic buttons) can be strategically placed throughout the premises to provide for immediate notification and response.

A.5.10	Visual and audible alarms to be triggered upon opening of emergency exit doors located on biosecurity barriers.					■
---------------	---	--	--	--	--	---

Visual and audible alarms on emergency exit doors reduce the risk of unauthorized entry or exit through these doors at biosecurity barriers. This requirement does not apply to doors that are used for multiple purposes in addition to emergency egress. The emergency egress path flows from most to least secure areas.

A.5.11	Operation of security systems to be annually verified to function as intended, or more frequently as necessitated by: a) a change, repair, or modification that may affect biosecurity; or b) a biosecurity risk assessment.					■
---------------	--	--	--	--	--	---

Verification confirms that access control systems operate as designed, such that a correct code, card, or biometric trait allows access and an incorrect one does not (i.e., door remains locked). If key locks or electronic card readers are used, verification can include confirming that doors are kept locked, keys and access cards are only distributed to authorized personnel, and the **key control** mechanism prevents duplication of keys and access cards (e.g., electronic tracking or log to record when a key or access card was issued and returned). Other security systems are routinely verified to confirm that they operate as specified. This requirement expands on CBS requirements 5.2.2 and 5.2.3.

A.5	Security Systems and Devices	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.5.12	A central security monitoring station to be: <ul style="list-style-type: none"> • established; • located behind two biosecurity barriers; and • operated by two security personnel. 					■

A central security monitoring station allows the organization to coordinate all security activities from a dedicated and central area. The central security monitoring station provides constant oversight, display, control, and management of all security systems by security personnel. It helps coordinate biosecurity incident response and can serve as a point of contact for emergencies. The biosecurity risk assessment is taken into consideration when choosing a location for the central security monitoring station. It is hidden from view and designed so that no conversations or sounds can be overheard. The central security monitoring station is located behind two biosecurity barriers, and access is limited to authorized personnel only. It is best practice for information technology and security system support equipment, as well as break rooms, to be built adjacent to the central security monitoring station.

A.5.13	Procedures for continuous security oversight in the event that the central security monitoring station is not functioning to be developed, documented, and implemented.					■
---------------	---	--	--	--	--	---

Procedures are followed in the event that the central security monitoring station ceases to function as intended. These allow security personnel to operate critical electronic security systems and provide continued security at all biosecurity barriers. The biosecurity risk assessment determines the maximum allowable downtime before the procedures are activated.

A.5.14	Security systems to operate and be actively monitored at all times by security personnel only.					■
---------------	--	--	--	--	--	---

Operating and actively monitoring security systems 24 hours per day, 7 days per week supports the continuous security of the premises. Security systems under active and direct observation allow security personnel to rapidly detect unusual or suspicious activity and immediately alert occupants or other security personnel of the situation.

Matrix A.6 – Transfer Security

The **transfer** of **regulated materials** from one **containment zone** to another can either be considered **movement** (i.e., a transfer within the same building) or **transportation** (i.e., the shipment of regulated materials from one building to another, domestically or internationally). During a transfer, regulated materials are removed from the containment zone and are at a higher risk of being subject to security threats. Examples of mitigation measures include a transfer security risk assessment, a two-person rule, maintaining a chain of custody, and notifications to PHAC when sending and receiving packages.

A.6	Transfer Security	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.6.1	A transfer security risk assessment to be conducted as part of the biosecurity risk assessment , and mitigation measures to be documented and implemented.					■

The transfer of regulated materials takes place domestically and internationally. Transfer security risk assessments consider the likelihood of **biosecurity incidents** and their potential consequences, and assesses known vulnerabilities at all stages of a transfer. The transfer security risk assessment informs the implementation of new or enhanced mitigation measures to address **biosecurity** risks that threaten regulated materials in transfer. Mitigation measures are documented in a biosecurity plan or related documentation.

A.6.2	Procedures for the movement of regulated materials to be developed, documented, and implemented. Procedures to include: a) a record of the movement; b) a two-person rule when moving the regulated materials outside the containment zone; c) a chain of custody of the regulated materials maintained at all times; and d) access to the regulated materials granted only to authorized personnel .					■
-------	--	--	--	--	--	---

Recording the movement of regulated materials allows for traceability and can provide an investigative support tool in the event that regulated materials go missing. The two-person rule is an accountability measure related to regulated materials while they are in movement outside the containment zone. Having two persons accompanying the regulated materials supports their security when they are removed from the containment zone. Authorized personnel are permitted to move regulated materials. Chain of custody involves documenting who had access to the regulated materials. Every individual moving regulated materials receives training and authorization, and clearly understands their responsibilities prior to moving or preparing regulated materials for transportation. Movement within the building is an essential step prior to transportation.

A.6	Transfer Security	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.6.3	<p>For exports or domestic transfers, the sending organization to notify PHAC at least two business days prior to the export or domestic transfer of regulated materials. Notification to include, as applicable:</p> <ul style="list-style-type: none"> • expected date of export or domestic transfer; • scientific names and quantities of regulated materials; • number of packages; • modes of transportation; • name of the carriers responsible for transportation; • airway bill number, bill of lading number, or tracking number; • name and address of sending and receiving organizations; • a written attestation that the sending organization will confirm receipt of the package with the receiving organization (if exporting); and • a written attestation that biosecurity risks have been assessed and addressed. 					■

Given the risks associated with RG4 regulated materials, sending organizations in Canada submit a notification to PHAC prior to export or domestic transfer. This supports the health and safety of the **community** by strengthening accountability measures for the export or domestic transfer of regulated materials. At minimum, the notification describes the material in sufficient detail (i.e., genus, species, and strain when necessary) to identify the level of risk for humans and for animals (i.e., **risk group**). The notification process is intended to inform PHAC and is not an approval request for the export or domestic transfer.

A.6	Transfer Security	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.6.4	<p>For imports or domestic transfers, the receiving organization to notify PHAC within two business days after the date of receipt of regulated materials. Notification to include, as applicable:</p> <ul style="list-style-type: none"> • scientific names and quantities of regulated materials; • number of packages; • modes of transportation; • name of the carriers responsible for transportation; • name and address of the sending and receiving organizations; and • assessment of seals and package for evidence of tampering. 					■

Receiving organizations in Canada submit a notification to PHAC after regulated materials have been received. This supports the health and safety of the community by strengthening accountability measures for the import or domestic transfer of regulated materials. The notification process is intended to inform PHAC and is not an approval request for the import or domestic transfer.

A.6.5	Procedures for screening and responding to incoming suspicious packages to be developed, documented, and implemented.					■
-------	---	--	--	--	--	---

The screening of incoming suspicious packages serves to detect and deny threat objects from being introduced where they could compromise biosecurity. Packages are assessed for unusual details such as unexpected points of origin, unusual odours, oily or greasy stains on packaging, excessive wrapping, or no return address. If a suspicious package is detected, personnel will follow established internal procedures to resolve the situation.

Matrix A.7 – Personnel Security and Identification

Personnel security and identification allow for identity management and the assessment of reliability and trustworthiness of personnel before they are granted access past **biosecurity barriers**. This includes activities such as **baseline security checks**, **HPTA Security Clearances**, confirmation of **need-to-know**, and issuance of identification (ID) and access cards. Security and identification measures are also in place for other individuals who may be accessing the **premises**, such as visitors and contractors.

A.7	Personnel Security and Identification	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.7.1	Baseline security check to be performed by the organization for all personnel who do not hold a valid HPTA Security Clearance: <ul style="list-style-type: none"> before granting unescorted access past biosecurity barriers; and every 10 years thereafter, or more frequently as determined by a biosecurity risk assessment. 					■

A baseline security check is a mandatory activity conducted by the organization. Personnel who have undergone this security check, the results of which fall within the organization’s risk tolerance, may be granted unescorted access to areas past biosecurity barriers. Valid government of Canada reliability status and security clearances are sufficient to meet this requirement. It is important to note that a baseline security check is not sufficient to be granted unescorted access to an **SSBA zone**.

A.7.2	Baseline security check to include an assessment in accordance with the organization’s risk tolerance for granting or refusing access based on: <ul style="list-style-type: none"> a documented confirmation of the need for site access; a confirmation of identity; and a criminal record check. 					■
-------	---	--	--	--	--	---

A baseline security check includes a documented statement confirming the legitimate need for access to areas where non-sensitive administrative activities take place (e.g., proof of employment), a confirmation of identity (i.e., through valid government issued ID), and criminal record check. A foreign criminal record check is recommended for individuals who resided outside Canada for more than 90 days. A baseline security check may also include a financial inquiry (i.e., credit check) and confirmation of background information, including proof of eligibility to work or study in Canada (i.e., Canadian citizenship or permanent residence status, valid work or study permit or visa) and curriculum vitae review (e.g., affiliations of concern). Valid government of Canada reliability status and security clearances are sufficient to meet this requirement.

A.7	Personnel Security and Identification	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.7.3	Procedures for baseline security checks and HPTA security clearance applications to be developed, documented, implemented, and kept up to date.					■

The organization is responsible for security checks for **authorized personnel**. The organization considers the results of the baseline security check prior to granting access past biosecurity barriers, based on established risk tolerance thresholds. For individuals with access to **SSBAs** or SSBA zones, PHAC is responsible for issuance of HPTA Security Clearances. Diligence is essential to track security check and clearance expiration dates.

A.7.4	All authorized personnel to be issued ID cards that clearly display: <ul style="list-style-type: none"> • their photo to allow identification; • their name; and • the expiry date. 					■
-------	--	--	--	--	--	---

ID cards and access cards can be combined. Temporary cards can be issued to authorized personnel when they have left their cards at home. Exchanging a valid government issued ID card (e.g., driver's licence) for temporary cards helps ensure that they are returned at the end of the workday. Issued cards are not altered, destroyed, or transferred to anyone else for any period of time. ID cards are re-issued as needed to reflect changes in appearance that would prevent identification.

A.7.5	ID cards and access cards to be renewed at least once every five years and returned prior to personnel departure from the organization.					■
-------	---	--	--	--	--	---

Authorized personnel promptly return their cards upon departure from the organization. Personnel also surrender cards while they are on extended leave (e.g., parental, long-term disability, temporary work assignment). This mitigation measure helps prevent unauthorized access with old or expired cards through social engineering.

A.7.6	Visitor cards to: <ul style="list-style-type: none"> • be issued for every visit; • identify the visitor's escorted status; and • be returned at the end of each day. 					■
-------	--	--	--	--	--	---

A visitor card indicates to personnel that the entry is authorized with continuous escort into secure areas past biosecurity barriers. Policies and procedures for visitor card management include exchanging a valid government issued ID card (e.g., driver's licence) for a visitor card, and prohibiting the removal of visitor cards from the premises.

A.7	Personnel Security and Identification	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.7.7	ID cards and visitor cards to be worn visibly at all times past biosecurity barriers unless they pose a safety risk.					■

ID cards and visitor cards are worn visibly at all times by those to whom they were issued. When performing certain functions, ID cards and visitor cards may pose a **hazard** to those who wear them, in which case the cards are securely stored for the duration of the work.

A.7.8	Visitor identity and need for site access to be confirmed and documented before escorted site access is granted.					■
--------------	--	--	--	--	--	---

Confirming a visitor's identity and the reason for their visit diminishes the risk of unauthorized access by individuals using social engineering tactics in an attempt to gain entry. Policies and procedures are established to provide instructions to personnel on granting or refusing visitor access.

A.7.9	Procedures for visitors to be under continuous escort past biosecurity barriers to be developed, documented, and implemented.					■
--------------	---	--	--	--	--	---

Visitors are under continuous escort when entering zones past biosecurity barriers. "Continuous escort" means maintaining direct line of sight and accompaniment of visitors by authorized personnel. This requirement expands on CBS requirement 4.2.3.

A.7.10	A security briefing for all visitors and escorts prior to entry past biosecurity barriers to be provided and documented.					■
---------------	--	--	--	--	--	---

Security briefings provide a short explanation of the relevant policies, procedures, and expected behaviours of visitors and escorts. The security briefing is based on the level of access being given to the visitor under escort. For example, the visitor and escort expectations for entering a **containment zone** may differ from those for a zone where **sensitive information** is located.

Matrix A.8 – Security Procedures and Responsibilities

Clear security procedures and responsibilities provide the organization with the ability to protect against, detect, respond to, and recover from potential **biosecurity incidents**. Security procedures cover normal operations as well as incident response, which may involve an off-site response force (e.g., local law enforcement) to support on-site security personnel.

A.8	Security Procedures and Responsibilities	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.8.1	Procedures for the continuous protection, detection, response to, and recovery (PDRR) from biosecurity incidents, based on a biosecurity risk assessment , to be developed, documented, implemented, kept up to date, and communicated and made available to personnel.					■

Capacity and capabilities for PDRR include a sufficient number of on-site security personnel provided with the knowledge, equipment, and training to protect (i.e., deter, deny, delay), detect, respond to, and recover from biosecurity incidents. PDRR strategies factor in off-site response force (e.g., local law enforcement) to engage threats that exceed the response capacity and capabilities of on-site security personnel.

A.8.2	On-site security personnel to be provided with equipment, tools, or devices to perform their duties, as determined by a biosecurity risk assessment.					■
-------	--	--	--	--	--	---

Equipment being provided to on-site security personnel is fundamental to prepare them for potential biosecurity incidents. Reliable communication tools and devices allow security personnel to efficiently convey information with other on-duty security personnel (e.g., at roving posts, static posts, central security monitoring station). This can be achieved by providing personnel with primary and backup communication devices that perform in all conditions. Equipment for self-defence and night-time observation can help mitigate the risks posed by a physical threat. The organization is responsible for training on-site security personnel on the equipment provided, developing procedures for the proper use and storage of equipment, and, where applicable, providing spaces for the safe storage of equipment so that it cannot be misused or stolen.

A.8	Security Procedures and Responsibilities	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.8.3	Liaison with an off-site response force to be established and documented.					■

Establishing a liaison with an off-site response force (e.g., local law enforcement) helps with incident response when a biosecurity incident exceeds on-site security personnel’s capacity and capabilities. Discussions may include response time expectations after calls for service, site familiarization visits, participation in **biosecurity** drills and exercises, and a surge capacity plan for imminent or elevated threats, as determined by a biosecurity risk assessment.

Matrix A.9 – Training and Exercises

Biosecurity training and exercises are essential in preparing for **biosecurity incidents**, as well as assessing the organization’s capacity and capabilities to respond to them. Training allows individuals to learn and understand their roles and responsibilities, and exercises maintain and refine that knowledge. A well-designed training program and exercise schedule contributes to the prevention of biosecurity incidents and, in the case of a biosecurity incident, allows for a prepared and efficient response.

A.9	Training and Exercises	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.9.1	<p>A biosecurity awareness and training program, based on a training needs assessment and a biosecurity risk assessment, to be developed, documented, implemented, kept up to date, and evaluated and improved, as necessary. A biosecurity awareness and training program includes training on:</p> <ul style="list-style-type: none"> • federal biosecurity requirements; • organizational biosecurity policies and procedures; • relevant provisions of the <i>Foreign Interference and Security of Information Act</i>; • information management security policies related to sensitive information; • visitor management policies; and • access control procedures. 					■

A biosecurity awareness and training program enhances the organization’s biosecurity posture. The organization determines which individuals are best placed to deliver sessions related to the biosecurity awareness and training program (e.g., based on expertise, knowledge of the subject matter). A biosecurity awareness and training program can be tailored to individuals holding specific functions and having access to **regulated materials**, sensitive information, and **critical support systems**. It is essential for personnel to understand prohibited behaviours and activities as well as the risks associated with deviation (e.g., negligence) from biosecurity policies and procedures. Personnel must also understand how to properly label, handle, disseminate, and destroy sensitive information and non-sensitive information in the organization’s possession. Training on information management security policies includes the authorized use of electronic devices, removable media, and use of cloud-based services and social media. Visitor escort requirements and access control procedures (e.g., tailgating) are also included. This requirement expands on CBS requirements 4.2.1 and 4.2.2.

A.9	Training and Exercises	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.9.2	Personnel to demonstrate proficiency in the biosecurity procedures on which they were trained before being granted unescorted access past biosecurity barriers .					■

Demonstration of proficiency is determined by the organization and may include written acknowledgement, certificates of completion of relevant biosecurity training, or testing. Based on the training needs assessment, demonstration of proficiency can be limited to the specific tasks that will be performed or areas that will be accessed by personnel; it may not be necessary to evaluate proficiency on all procedures for which training is available. This requirement expands on CBS requirement 4.2.4.

A.9.3	On-site security personnel to be provided with training on the procedures to support continuous PDRR prior to performing their duties.					■
-------	--	--	--	--	--	---

On-site security personnel are provided with site-specific training on biosecurity policies and procedures. Training covers the relevant tasks and post orders related to site protection, threat detection, incident response and recovery. Examples may include use of force; alarm interpretation and assessment; visual observation and assessment of unauthorized or suspicious individuals or vehicles; and calls for service from an off-site response force (e.g., local law enforcement) when needed.

A.9.4	Refresher biosecurity training to be provided: <ul style="list-style-type: none"> • annually for on-site security personnel; and • every two years for other personnel. 					■
-------	---	--	--	--	--	---

Personnel are provided with periodic refresher training to support their ongoing proficiency on biosecurity policies and procedures. Training on updated biosecurity policies and procedures may be provided, for example, following changes in the threat environment or following biosecurity incidents. Refresher training also provides personnel with an opportunity to clarify any misconceptions or misunderstandings of biosecurity policies and federal requirements.

A.9	Training and Exercises	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.9.5	<p>Discussion-based exercises to test the effectiveness of the biosecurity plan to:</p> <ul style="list-style-type: none"> • be conducted every two years; • be based on the biosecurity risk assessment; • involve individuals playing a critical role in the response to biosecurity incidents; • be documented; and • include an after-action report. 					■

Discussion-based exercises include seminars, workshops, and tabletop exercises. The objective of discussion-based exercises is to test the effectiveness of an organization’s response plans when faced with biosecurity incidents. Discussion-based exercises can involve internal parties responsible for biosecurity and response, and external parties such as first responders. These exercises can be combined with business continuity planning. The outcomes of discussion-based exercises are documented in an after-action report, which captures insights, challenges, areas of improvement, and successes. These exercises are essential for the continual improvement and renewal of a biosecurity plan.

A.9.6	<p>Operations-based exercises to test the effectiveness of the biosecurity plan to:</p> <ul style="list-style-type: none"> • be conducted every three years; • be based on the biosecurity risk assessment; • involve individuals playing a critical role in the response to biosecurity incidents; • be documented; and • include an after-action report. 					■
-------	---	--	--	--	--	---

Operations-based exercises include drills, functional, and full-scale exercises. These exercises simulate biosecurity incidents and test the effectiveness of biosecurity plans. They differ from discussion-based exercises in that they mobilize personnel and third parties involved in the simulated response. The outcomes of operations-based exercises are documented in an after-action report, which captures insights, challenges, areas of improvement, and successes. These exercises are essential for the continual improvement and renewal of a biosecurity plan.

A.9	Training and Exercises	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.9.7	Discussion-based or operations-based exercises involving on-site security personnel to: <ul style="list-style-type: none"> • be conducted every six months; • be based on the biosecurity risk assessment; • be documented; and • include an after-action report. 					■

The roles and responsibilities of on-site security personnel include observing, assessing, reporting, investigating, and engaging threats. When faced with a biosecurity incident that exceeds their capacity and capabilities, on-site security personnel call for service from an off-site response force (e.g., local law enforcement). On-site security personnel (e.g., security guards, security supervisors) participate in realistic exercises to prepare them for plausible scenarios while they are on duty. Through discussion-based or operations-based exercises, security personnel will put their knowledge to the test and understand the limitations of their roles and responsibilities. Exercise formats and content will vary depending on the information being conveyed. Examples include drills for responding to biosecurity incidents, observation techniques for identifying suspicious behaviour and potential threats, and techniques for crisis management and de-escalating tense encounters.

Matrix A.10 – Information Management and Security

Information management and security includes having procedures in place for handling, storing, safeguarding, and destroying **sensitive information**. It also includes policies on the use of digital devices and a cybersecurity plan to protect digital components of sensitive information and **critical support systems**.

A.10	Information Management and Security	CL2	CL2- Ag	CL3	CL3- Ag	CL4
A.10.1	A cybersecurity plan to protect sensitive information and critical support systems, based on a biosecurity risk assessment , to be developed, documented, implemented, evaluated, and kept up to date.					■

A cybersecurity plan describes the measures for continuous PDRR from **biosecurity incidents**. Biosecurity incidents can threaten the confidentiality, integrity, and availability of assets including sensitive information and operational technology embedded in critical support systems. A biosecurity risk assessment takes into account adversaries who target these assets through cyber attacks, which can vary in sophistication. Therefore, cybersecurity measures minimize the opportunities for cyber adversaries to exploit vulnerabilities in an organization’s cybersecurity posture. Examples of operational technology include supervisory control and data acquisition (SCADA) systems, building automation systems (BAS), and information technology servers.

A.10.2	Policies on the use of digital devices to be developed, documented, and implemented, as determined by a biosecurity risk assessment.					■
---------------	--	--	--	--	--	---

Policies governing the authorized use of digital devices protect the security of **regulated materials**, sensitive information, and operational technology supporting critical support systems. Allowing only authorized digital devices to be used within secure areas and networks is critical for the protection of the digital environment. Examples of digital devices are computers, tablets, cellphones, removable media, smart watches, personal medical devices, and any other device with video and audio recording capabilities.

A.10	Information Management and Security	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.10.3	Sensitive information to be labelled, used, disseminated, stored, and destroyed as determined by a biosecurity risk assessment.					■

Protecting sensitive information applies to all stages of its lifecycle. Categorizing information according to the injury it would cause if compromised (i.e., loss of confidentiality, integrity, or availability) is a fundamental first step of protecting sensitive information. Developing policies that govern information categorization involves establishing instructions on the labelling and use of sensitive information and non-sensitive information, including how to disseminate, store, access, and destroy it once it is no longer needed. Header markings or watermarks are examples of labelling sensitive information. Dissemination instructions (e.g., double envelop paper files, encrypt electronic files) describe how to securely transfer and transmit sensitive information in hard copy and electronic format. Destruction of sensitive information can be done by methods such as the use of proper shredder types for hard copies and overwrite techniques (e.g., triple overwrite) for electronic files. Recategorizing (e.g., upgrading, downgrading) information can be done by its author or another subject matter expert if the originator is not available. This requirement expands on CBS requirements 4.9.2, 4.9.3, 4.9.5, 4.9.6, 4.9.7, 4.9.8, and 4.9.11.

A.10.4	Sensitive information to be located behind two biosecurity barriers .					■
---------------	--	--	--	--	--	---

Access to sensitive information is restricted to those with a **need-to-know**. Having this information protected behind multiple logical and physical biosecurity barriers serves to delay the theft or misuse of information, and allows for detection and response to disrupt attempted compromise to sensitive information. Logical biosecurity barriers are measures for credential authentication, authorization, and accountability within digital systems. Having logical biosecurity barriers for digital systems allows for users' physical access and permissions to be instantaneously amended or revoked.

A.10.5	Sensitive information to be accessible only to individuals with a need-to-know.					■
---------------	---	--	--	--	--	---

Access to sensitive information is restricted to those with a need-to-know. Limiting access reduces the risk that unauthorized individuals gain access to the information and limits the risk of this information being shared further. This requirement expands on CBS requirement 4.9.3.

Matrix A.11 – Accountability Measures and Inventory Control

Accountability measures and **inventory** control serve to track **regulated materials**, as well as document any **biosecurity incidents** that may compromise them or related **sensitive information**. Inventory audits allow for the detection of theft, loss, or misuse of regulated materials. Accountability measures include reporting biosecurity incidents to appropriate internal authorities and PHAC.

A.11	Accountability Measures and Inventory Control	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.11.1	<p>Procedures for inventory audits of regulated materials in, or destined for, long-term storage to be developed, documented, and performed by two authorized personnel:</p> <ul style="list-style-type: none"> • annually or more frequently as determined by a biosecurity risk assessment; • following the departure of personnel with access to regulated materials; • following the detection of suspicious activities; and • following biosecurity incidents involving regulated materials. 					■

Frequent inventory audits of regulated materials are an accountability measure to detect unauthorized activities and loss. Inventory audits of regulated materials are conducted by two authorized personnel, who confirm and sign off on their findings. Inventory audits may be complete or partial depending on the circumstances. A partial inventory audit during normal operation may involve a randomly generated selection of items, whereas a complete inventory audit would be appropriate following a biosecurity incident. Procedures also include the actions to take in case of discrepancies (e.g., locate missing regulated materials, notify PHAC of any missing or stolen regulated materials). This requirement expands on CBS requirements 4.9.5 and 4.9.6.

A.11.2	Procedures for internal reporting of biosecurity incidents to be developed, documented, and implemented.					■
--------	--	--	--	--	--	---

An internal reporting system allows for self- and peer-reporting of biosecurity incidents to an appropriate internal authority. Procedures establish clear thresholds for reporting biosecurity incidents, including accidental and deliberate attempts to breach **biosecurity barriers** and compromise sensitive information, **critical support systems**, or regulated materials. Reported biosecurity incidents are assessed for trends and early warnings of insider and outsider threat activity. This requirement expands on CBS requirements 4.1.2, 4.1.7, 4.1.8, 4.8.5, and 4.8.9.

A.11	Accountability Measures and Inventory Control	CL2	CL2-Ag	CL3	CL3-Ag	CL4
A.11.3	Following the detection of a biosecurity incident: <ul style="list-style-type: none"> • a notification report to be submitted to PHAC within two business days; and • a follow-up report to be submitted to PHAC within 30 days. 					■

Notifications include the initial summary of the biosecurity incident such as location, time, implicated parties, and regulated materials, sensitive information, or critical support system involved. New or updated information is included in the follow-up report and may include the status of the incident investigation, root cause analysis, and risk mitigation strategies put in place to prevent recurrence. This requirement expands on CBS requirement 4.8.11.

References



REFERENCES

Legislation

Foreign Interference and Security of Information Act (R.S.C., 1985, c. O-5).

Health of Animals Act (S.C. 1990, c. 21).

Health of Animals Regulations (C.R.C., c. 296).

Human Pathogens and Toxins Act (S.C. 2009, c. 24).

Human Pathogens and Toxins Regulations (SOR/2015-44).

Guidance Documents

Government of Canada. (2018). *Canadian Biosafety Guideline – Conducting a Biosecurity Risk Assessment*. Ottawa, ON, Canada: Government of Canada. Available from <https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance.html>

Government of Canada. (2016). *Canadian Biosafety Guideline – Developing a Comprehensive Biosecurity Plan*. Ottawa, ON, Canada: Government of Canada. Available from <https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance.html>

Government of Canada, Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology*. Ottawa, ON, Canada: Government of Canada. Available from <https://www.cyber.gc.ca/en/tools-services/harmonized-tra-methodology>

General Resources

Crowe, T. D., & Fennelly, L. J. (2013). *Crime Prevention Through Environmental Design* (3rd ed.). Oxford, UK; Waltham, MA, USA: Elsevier Inc.

Fennelly, L. J. (2016). *Effective Physical Security* (5th ed.). Oxford, UK; Cambridge, MA, USA: Elsevier Inc.

Government of Canada. (2024). *Cyber and Infrastructure Resilience Assessments: The Regional Resilience Assessment Program*. Retrieved 2024-10-21 from <https://www.publicsafety.gc.ca/cnt/ntnl-scr/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx>

Government of Canada. (2022). *Canadian Biosafety Standard* (3rd ed.). Ottawa, ON, Canada: Government of Canada. Available from <https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/third-edition.html>

Government of Canada. (2022). *Safeguarding your Research*. Retrieved 2024-10-24 from <https://science.gc.ca/site/science/en/safeguarding-your-research>

- Government of Canada, Treasury Board of Canada Secretariat. (2019). *Directive on Security Management*. Retrieved 2024-10-22 from <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611>
- Government of Canada, Treasury Board of Canada Secretariat. (2019). *Policy on Government Security*. Retrieved 2024-10-22 from <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578>
- Government of Canada, Treasury Board of Canada Secretariat. (2019). *Policy on Service and Digital*. Retrieved 2024-11-01 from <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603>
- Government of Canada, Treasury Board of Canada Secretariat. (2017). *Standard on Security Screening*. Retrieved 2024-10-22 from <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=28115>
- Government of Canada. (2012). *IT Security Risk Management: A lifecycle approach (ITSG-33)*. Retrieved 2024-10-21 from <https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33>
- Royal Canadian Mounted Police. *Royal Canadian Mounted Police Publications*. Available from <https://www.rcmp-grc.gc.ca/physec-secmat/pubs/index-eng.htm>
- Salerno, R. M., Gaudio, J., & Brodsky, B. H. (2007). *Laboratory Biosecurity Handbook* (1st ed.). Boca Raton, FL, USA: CRC Press.

Technical Standards and Codes

- ISO 31000:2018, Risk Management – Guidelines*. (2018). Geneva, Switzerland: International Organization for Standardization.
- Canadian Commission on Building and Fire Codes, and National Research Council of Canada. *National Building Code of Canada*. (2020). Ottawa, ON, Canada: National Research Council of Canada.
- CAN/ULC-S301:2018, Standard for Signal Receiving Centres Configurations and Operations*. (2018). Ottawa, ON, Canada: ULC Standards.

