INTERNATIONAL
WORKSHOP
AGREEMENT

IWA 37-2

First edition
2022-10

Safety, security and sustainability of cannabis facilities and operations —

Part 2:
Requirements for the secure handling of cannabis and cannabis products

Reference number
IWA 37-2:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

International Workshop Agreement IWA 37 was approved at a series of workshops hosted by the Standards Council of Canada (SCC), in association with Underwriters Laboratories of Canada (ULC), held virtually between December 2020 and June 2021.

A list of all parts in the IWA 37 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

While cannabis has been fully legalized in Canada and in many states in the USA, it is a new and emerging industry that is moving at a very fast pace in many other parts of the world. While legalization is being deliberated by governments and legislative bodies, companies are creating their own infrastructure in anticipation of legal approval. Meanwhile, government regulators and the societies they serve are grappling with the lack of consistent rules and guidance to deliver safety, security and sustainability of cannabis facilities and operations, while growers and producers use their own judgment on how to establish and operate facilities.

It has become very clear that the global cannabis market is opening up very rapidly. The cannabis product and the industry will become more and more ubiquitous as the global barriers start to lower and come down. If the current trend continues, it is predicted that well over one third of the globe will accommodate cannabis by 2024.

What is unique about this new and emerging industry is that it is coming from an illicit status into decriminalization and evolving into a legitimate burgeoning business. Due to its pioneering status, very little exists in terms of research, studies, historical experience and best practices. Standardization is likewise very slow on the uptake and the cannabis industry remains severely underserved.

There are therefore distinct challenges for the safety, security and sustainability of cannabis facilities and operations, which the IWA 37 series seeks to address as follows:

- Part 1: Requirements for the safety of cannabis buildings, equipment and oil extraction operations;
- Part 2 (this document): Requirements for the secure handling of cannabis and cannabis products;
- Part 3: Good production practices (GPP).

In addition to the requirements for facilities specified in this document, statutory and regulatory requirements and codes can apply.

Supporting material to accompany the IWA 37 series is available at the following website: IWA 37 — Safety, security and sustainability of cannabis facilities and operations.

A list of workshop participants is available from the Standards Council of Canada (SCC).

Safety, security and sustainability of cannabis facilities and operations —

Part 2:
Requirements for the secure handling of cannabis and cannabis products

1 Scope

This document specifies minimum requirements for the security of sites and facilities that handle cannabis and cannabis products for the purposes of cultivation (indoor and outdoor), processing, storage/distribution, transportation, retail sales, and research and testing, in order to prevent harm and/or unauthorized access to assets including (but not limited to):

- physical assets;
- personnel;
- cannabis and cannabis products;
- records and information.

NOTE Premises covered in this document include indoor and outdoor cultivation, processing/production facilities and retail stores.

The overall security programme and individual security measures addressed in this document incorporate three types:

a) physical controls;

b) technical controls;

c) administrative controls.

This document specifies minimum requirements for general security of cannabis and cannabis products, up to and including:

- physical security design/measures intended to deny, deter, delay, respond to, and recover from unauthorized access;
- design, installation and maintenance of electronic security systems intended to restrict access, detect intrusion and visually monitor/record activity in security-sensitive areas;
- procedural security measures intended to instruct day-to-day security activities, both routine and emergency, across an organization;
- personnel security measures intended to ensure all personnel attending the facility are properly screened, instructed and trained in security awareness;
- the monitoring of the security status of cannabis and cannabis products throughout the product lifecycle, from cultivation to retail sale, including transportation.

This document provides guidelines for:

- the installation, maintenance and inspection of physical and electronic premises security and cybersecurity systems;

- — the implementation of information security governance at organizational level to include policies, procedures, and standards to protect the confidentiality, integrity and availability of records and information.

All requirements in this document are generic and intended to be applicable to all organizations in the cannabis supply chain, regardless of size and/or complexity.

2 Normative references

The following documents are referred to in the text in such a way that some, or all, of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IWA 37-1, *Safety, security and sustainability of cannabis facilities and operations — Part 1: Requirements for the safety of cannabis buildings, equipment and oil extraction operations*

ISO 22005, *Traceability in the feed and food chain — General principles and basic requirements for system design and implementation*

IEC 60839-11-1:2013, *Alarm and electronic security systems — Part 11-1: Electronic access control systems – System and components requirements*

IEC 60839-11-2, *Alarm and electronic security systems — Part 11-2: Electronic access control systems – Application guidelines*

IEC 62368-1, *Audio/video, information and communication technology equipment — Part 1: Safety requirements*

IEC 62676-4, *Video Surveillance Systems for Use in Security Applications — Part 4: Application Guidelines*

ANSI/UL 681, *Standard for Safety Installation and Classification of Burglar and Holdup Alarm Systems*

ANSI/UL 687, *Standard for Safety Burglary-Resistant Safes*

ANSI/UL 827, *Standard for Safety Central-Station Alarm Services*

ASTM D8205, *Standard Guide for Video Surveillance System*

ASTM D8218, *Standard Guide for Intrusion Detection System (IDS)*

CAN/ULC-S301:2018, *Standard for Signal Receiving Centres Configurations and Operations*

CAN/ULC-S302, *Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems*

EN 1143-1, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Part 1: Safes, ATM safes, strongroom doors and strongrooms*

EN 50518, *Monitoring and alarm receiving centre*

UL 972, *Standard for Safety Burglary Resisting Glazing Material*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- — ISO Online browsing platform: available at https://www.iso.org/obp
- — IEC Electropedia: available at https://www.electropedia.org/

3.1

access control system

system designed to grant to authorized persons, or entities, entry to and/or exit from a security *controlled area* (3.15) and deny such entry and/or exit to non-authorized individuals, or entities

[SOURCE: IEC 60839-11-1:2013, 3.63, modified – Second preferred term "electronic access control system" and Note 1 to entry have been deleted.]

3.2

authority having jurisdiction

AHJ

organization (3.35), office, or individual responsible for enforcing the *requirements* (3.44) of a code or standard, or for approving equipment, materials, an installation, or a procedure

Note 1 to entry: Note to entry: Also referred to as "competent authority".

[SOURCE: ISO 7076-5:2014, 3.4, modified – Note 1 to entry has been added.]

3.3

cannabis

genus of flowering plants made up of many different phytocannabinoids and chemical compounds

Note 1 to entry: Research into cannabis by governing bodies and *organizations* (3.35) is ongoing around the world, and drug classifications are constantly under review. Regulation of cannabis legalization frameworks can vary between jurisdictions, based on the levels of tetrahydrocannabinol (THC) available in the plant.

3.4

cannabis derivative

secondary *product* (3.42) that can be extracted or obtained from a *cannabis* (3.3) biomass

Note 1 to entry: Classification of synthetically derived cannabinoids can vary between jurisdictions.

3.5

cannabis edible

food (3.24) which includes *cannabis* (3.3) or *cannabis derivative* (3.4) as an ingredient

Note 1 to entry: Dried cannabis, fresh cannabis, cannabis plants or cannabis plant seeds are not in themselves considered food.

3.6

cannabis product

packaged goods containing *cannabis* (3.3) or *cannabis derivative* (3.4), available in multiple formats for commercial and/or retail distribution

3.7

cannabis waste

solid, liquid or gaseous material that is a *cannabis product* (3.6), contains *cannabis* (3.3) or has come into contact with cannabis, destined for disposal and not intended for sale or for use in any way other than for agronomic purposes such as compost

Note 1 to entry: Definitions of cannabis waste can vary between jurisdictions. For example, in a jurisdiction that sets a specific tetrahydrocannabinol (THC) threshold to define cannabis waste at a specific concentration of THC (e.g. 10 µg/g), waste that has a concentration below that threshold is not considered to be cannabis waste.

3.8

chain of custody

process (3.41) by which inputs and outputs and associated information are transferred, monitored and controlled as they move through each step in the relevant supply chain

[SOURCE: ISO 22095:2020, 3.1.1]

3.9

competence

ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 22000:2018, 3.4]

3.10

complete protection

electronic protection of any point at which entry can be gained without cutting or tearing down any part of the premises structure, in order to detect entry through it, in addition to the detection of the physical removal of any moveable or removable portion of the closure over the opening

3.11

conformity

fulfilment of a *requirement* (3.44)

[SOURCE: ISO 22000:2018, 3.5]

3.12

contamination

introduction or occurrence of a contaminant including a *safety hazard* (3.48) in a *product* (3.42) or processing environment

[SOURCE: ISO 22000:2018, 3.6]

3.13

continual improvement

recurring activity to enhance *performance* (3.37)

[SOURCE: ISO 22000:2018, 3.7]

3.14

control measure

action or activity that is essential to prevent a *safety hazard* (3.48) and/or significant safety hazard or reduce it to an acceptable level

Note 1 to entry: Control measure(s) is (are) identified by *risk* (3.46) assessment/hazard analysis.

[SOURCE: ISO 22000:2018, 3.8, modified — The words “a significant food safety hazard” have been replaced with “a safety hazard and/or significant safety hazard” in the definition; the original Note 1 to entry has been deleted and the words “risk assessment” have been added to the remaining Note to entry.]

3.15

controlled area

room, area, building, premises or parts thereof to which access is monitored, limited, or controlled

3.16

corrective action

action to eliminate the cause of a *nonconformity* (3.32) and to prevent recurrence

Note 1 to entry: There can be more than one cause for a nonconformity.

Note 2 to entry: Corrective action includes cause analysis.

[SOURCE: ISO 22000:2018, 3.10]

3.17

cultivation

process (3.41) of growing *cannabis* (3.3), including drying, trimming, milling and storing

3.18
documented information
information required to be controlled and maintained by an *organization* (3.35) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.30), including related processes;

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

[SOURCE: ISO 22000:2018, 3.13]

3.19
duress alarm
silent alarm signal generated by the manual entry of a designated code at the system keypad in the event that the user needs assistance, such as when being forced to disarm the burglar alarm system against the user's will to enter the premises

Note 1 to entry: A duress alarm can also be referred to as an ambush alarm or a panic alarm

Note 2 to entry: Duress alarms are typically treated as *holdup alarms* (3.24) by *monitoring* (3.31) station personnel and are dispatched upon immediately without the need for any type of alarm *verification* (3.55).

3.20
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 22000:2018, 3.14]

3.21
electronic security system
electronic system or combination of systems that monitor(s) or control(s) activity at a premises, including alarm, access control, video surveillance and unmanned vehicle systems

3.22
extent of protection
designation used to describe the amount of electronic protection installed at a designated area (e.g. *complete protection* (3.10), partial protection)

3.23
extraction
process (3.41) where a substance is removed or separated from other compounds, a solution or a mixture

3.24
food
substance (ingredient), whether processed, semi-processed or raw, which is intended for consumption, and includes drink, chewing gum and any substance which has been used in the manufacture, preparation or treatment of "food" but does not include cosmetics or tobacco or substances (ingredients) used only as drugs

[SOURCE: ISO 22000:2018, 3.18, modified — The original Note to entry has been deleted.]

3.25
greenhouse
building that can have unlimited size, and with more than 50 % of surface area of roofs and/or walls being transparent and/or translucent for the *cultivation* (3.17) of *cannabis* (3.3) plants and other cultivation activities

3.26
grow area
area of the site where *cannabis* (3.3) plants are cultivated, harvested or propagated

3.27
holdup alarm
alarm initiated by an individual who perceives a threat to the *safety* (3.47) and/or security of persons, facilities, or vehicles, or of being coerced

Note 1 to entry: The alarm is typically silent, but can be visible, and/or audible.

Note 2 to entry: The signalling device can be covert or overt.

3.28
interested party
person or *organization* (3.35) that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO 22000:2018, 3.23, modified — The admitted term “stakeholder” has been deleted.]

3.29
lot
defined quantity of a *product* (3.42) produced and/or processed and/or packaged essentially under the same conditions

Note 1 to entry: The lot is determined by parameters established beforehand by the *organization* (3.35) and may be described by other terms, e.g. batch.

Note 2 to entry: The lot may be reduced to a single unit of product.

[SOURCE: ISO 22000:2018, 3.24]

3.30
management system
set of interrelated or interacting elements of an *organization* (3.35) to establish *policies* (3.39) and *objectives* (3.33) and *processes* (3.41) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Note 4 to entry: Relevant disciplines are, for example, a quality management system or an environmental management system.

[SOURCE: ISO 22000:2018, 3.25]

3.31
monitoring
determining the status of a system, a *process* (3.41) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

Note 2 to entry: In the context of *cannabis* (3.3) *safety* (3.47), monitoring is conducting a planned sequence of observations or measurements to assess whether a process is operating as intended.

Note 3 to entry: Distinctions are made in this document between the terms *validation* (3.54), monitoring and *verification* (3.55):

- validation is applied prior to an activity and provides information about the capability to deliver intended results;
- monitoring is applied during an activity and provides information for action within a specified time frame;
- verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.27, modified — The words "food safety" have been replaced with "cannabis safety" in Note 2 to entry.]

3.32
nonconformity
non-fulfilment of a *requirement* (3.44)

[SOURCE: ISO 22000:2018, 3.28]

3.33
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and *safety* (3.47), and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, *product* (3.42), and *process* (3.41).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a food safety *management system* (3.30) objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of food safety management systems, objectives are set by the *organization* (3.35), consistent with the food safety *policy* (3.39), to achieve specific results.

[SOURCE: ISO 22000:2018, 3.29]

3.34
operational technology
OT
hardware and software that detects or causes a change through the direct *monitoring* (3.31) and/or control of physical devices and systems, *processes* (3.41), and events in an *organization* (3.35)

3.35
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.33)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 22000:2018, 3.31]

3.36
outsource
make an arrangement where an external *organization* (3.35) performs part of an organization's function or *process* (3.41)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.30), although the outsourced function or process is within the scope.

[SOURCE: ISO 22000:2018, 3.32]

3.37
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.41), *products* (3.42) (including services), systems or *organizations* (3.35).

[SOURCE: ISO 22000:2018, 3.33]

3.38
physical security
security measures that are designed to deny access to unauthorized persons from physically accessing a building, premises, secured area or security container

3.39
policy
intentions and direction of an *organization* (3.35) as formally expressed by its *top management* (3.52)

[SOURCE: ISO 22000:2018, 3.34]

3.40
potency
amount per unit of the standardized component(s) which further characterizes the quantity of the ingredient

Note 1 to entry: The use of the term potency in this document is not intended to refer to *product* (3.42) efficacy.

3.41
process
set of interrelated or interacting activities which transforms inputs to outputs

[SOURCE: ISO 22000:2018, 3.36]

3.42
product
output that is a result of a *process* (3.41)

Note 1 to entry: A product can be a service.

[SOURCE: ISO 22000:2018, 3.37]

3.43
protected area
protected premises, or an area within, that is provided with means to prevent an unwanted event

Note 1 to entry: Protected areas are imposed in the low security level.

3.44
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.35) and *interested parties* (3.28) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.18).

[SOURCE: ISO 22000:2018, 3.38]

3.45
restricted area
room, area, or building within a site for which access is only permitted for authorized persons

Note 1 to entry: Restricted areas are imposed in the high security level.

[SOURCE: IEC 62128-1:2013, 3.9.5, modified – The word “area” has been replaced with “room, area, or building within a site” and Note 1 to entry has been added.]

3.46
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected – positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

[SOURCE: ISO 22000:2018, 3.39, modified — The original Note 5 to entry has been deleted.]

3.47
safety
assurance that the *product* (3.42) will not cause an adverse health effect for the consumer when it is prepared and/or used according to its intended use

Note 1 to entry: Safety is related to the occurrence of *safety hazards* (3.48) in end products and does not include other health aspects.

3.48
safety hazard
source or situation with the potential to cause an adverse health effect

Note 1 to entry: The term hazard is not to be confused with the term *risk* (3.46) which, in the context of *safety* (3.47), means a function of the probability of an adverse health effect (e.g. becoming diseased) and the severity of that effect (e.g. death, hospitalization) when exposed to a specified hazard.

Note 2 to entry: Safety hazards include allergens and radiological substances.

[SOURCE: ISO 22000:2018, 3.22, modified — The word “food” has been deleted from the term and from Notes 1 and 2 to entry; the words “biological, chemical or physical agent in food” have been replaced with “source or situation” in the definition; the original Notes 3 and 4 to entry have been deleted.]

3.49
secure area
area with defined physical perimeters and barriers, with physical entry controls or access point protection or access point observation

Note 1 to entry: Secure areas are imposed in the medium security level.

[SOURCE: IEC 61162-460:2018, 3.37, modified – The original Note 1 to entry has been deleted and a new Note 1 to entry has been added.]

3.50
security risk assessment
overall *process* (3.41) of identification, analysis and evaluation of *risks* (3.46) to security *objectives* (3.33) and outcomes

3.51
signal receiving centre
SRC
portion, or portions of a building, occupied by the alarm operating company, which encompasses the centre operations area and the facilities essential to the operation of *monitoring* (3.31), processing, and disposition of alarm signals

[SOURCE: CAN/ULC-S301:2018, 3.13]

3.52
top management
person or group of people who directs and controls an *organization* (3.35) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.30) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

[SOURCE: ISO 22000:2018, 3.41]

3.53
traceability
ability to follow the history, application, movement and location of an object through specified stage(s) of production, processing and distribution

Note 1 to entry: Movement can relate to the origin of the materials, processing history or distribution of the *product* (3.42).

Note 2 to entry: An object can be a product, a material, a unit, equipment, a service, etc.

[SOURCE: ISO 22000:2018, 3.42, modified — The word “food” has been replaced with “product” in Note 1 to entry.]

3.54
validation
obtaining evidence that a *control measure* (3.14) (or combination of control measures) will be capable of effectively controlling the significant *safety hazard* (3.48)

Note 1 to entry: Validation is performed at the time a control measure combination is designed, or whenever changes are made to the implemented control measures.

Note 2 to entry: Distinctions are made in this document between the terms validation, *monitoring* (3.31) and *verification* (3.55):

- validation is applied prior to an activity and provides information about the capability to deliver intended results;
- monitoring is applied during an activity and provides information for action within a specified time frame;
- verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.43, modified — The word “food” has been deleted from the definition.]

3.55
verification
confirmation, through the provision of objective evidence, that specified *requirements* (3.44) have been fulfilled

Note 1 to entry: Distinctions are made in this document between the terms *validation* (3.54), *monitoring* (3.31) and verification:

- validation is applied prior to an activity and provides information about the capability to deliver intended results;

— monitoring is applied during an activity and provides information for action within a specified time frame;

— verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.45]

3.56
video surveillance system
video surveillance system based on an IP video network used within a protected site

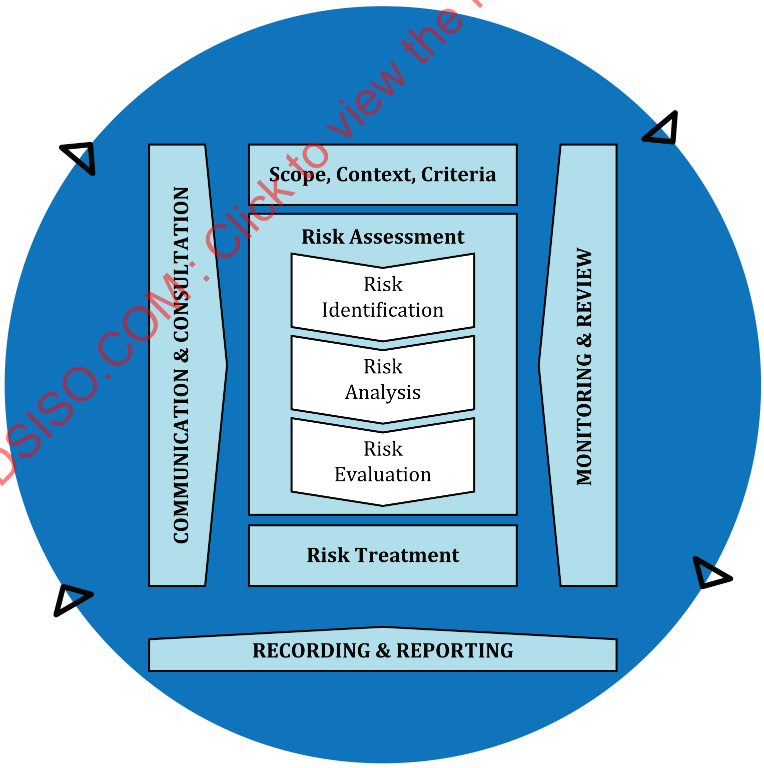
Note 1 to entry: A video surveillance system can consist of closed-circuit television (CCTV) systems and digital imaging devices, *monitoring* (3.31) and recording devices designed to provide visual identification of a person, object or scene in the areas being monitored.

[SOURCE: IEC 62676-2-1:2013, 3.1.64, modified – The original terms "video surveillance system network" and "VSS network" have been replaced with "video surveillance system" and Note 1 to entry has been added.]

4 Risk assessment

4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. See Figure 1.



SOURCE: ISO 31000:2018, Figure 4.

Figure 1 — Risk assessment process

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of interested parties. It should use the best available information, supplemented by further enquiry as necessary.

See Annex A for the threat and risk assessment checklist and instructions.

4.2 Risk identification

The purpose of risk identification is to find, recognize and describe risks that can help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

A range of techniques can be used for identifying uncertainties that can affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

a) sources of risk;

b) causes and events;

c) threats and opportunities;

d) vulnerabilities and capabilities;

e) changes in the external and internal context;

f) indicators of emerging risks;

g) the nature and value of assets and resources;

h) consequences and their impact on objectives;

i) limitations of knowledge and reliability of information;

j) time-related factors;

k) biases, assumptions and beliefs of those involved.

An organization should identify risks, whether or not their sources are under its control. There can be more than one type of outcome, which can result in a variety of consequences.

4.3 Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

Risk analysis should consider factors such as:

a) the likelihood of events and consequences;

b) the nature and magnitude of consequences;

c) complexity and connectivity;

d) time-related factors and volatility;

e) the effectiveness of existing controls;

f) sensitivity and confidence levels.

The risk analysis can be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

4.4 Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

a) do nothing further;

b) risk treatment options;

c) undertake further analysis to better understand the risk;

d) maintain existing controls; or

e) reconsider objectives.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal interested parties.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of an organization.

4.5 Risk treatment

The purpose of risk treatment is to select and implement options for addressing risk. Risk treatment involves an iterative process of:

a) formulating and selecting risk treatment options;

b) planning and implementing risk treatment;

c) assessing the effectiveness of that treatment;

d) deciding whether the remaining risk is acceptable;

e) if not acceptable, taking further treatment.

4.6 Security risk assessment

Procedures shall be established and maintained for the ongoing identification and assessment of security threats and security management-related threats and risks to an organization, threats to the continuity of business operations and the identification and implementation of necessary management control measures and procedures. Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences which shall include:

a) physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;

b) operational threats and risks, including the control of the security, human factors and other activities which affect an organization’s performance, condition or safety;

c) accidents, which can render security measures and equipment ineffective and require the unsupervised entrance of the facility by first responders.

d) natural environmental events (storm, floods, etc.), which can render security measures and equipment ineffective;

e) factors outside of an organization’s control, such as failures in externally supplied equipment and services;

f) threats and risks related to interested parties, such as failure to meet regulatory requirements or damage to reputation or brand;

g) design and installation of security equipment, including replacement and maintenance;

h) information and data management and communications.

The results of these assessments and the effects of these controls shall be considered and, where appropriate, provide input into:

a) security management objectives and targets;

b) security management programmes;

c) the determination of requirements for the design, specification and installation of security controls;

d) identification of adequate resources including staffing levels;

e) identification of training needs and skills;

f) development of operational controls;

g) the overall threat and risk management framework of an organization.

The methodology for threat and risk identification and assessment of an organization shall:

a) be defined with respect to its scope, nature and timing to ensure it is proactive rather than reactive;

b) include the collection of information related to security threats and risks;

c) provide for the classification of threats and risks and identification of those that are to be avoided, eliminated or controlled;

d) provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation.

NOTE See Annex A for specific threats and vulnerabilities to the facility, operations, and organization.

4.7 Selection of risk treatment options

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk can involve one or more of the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

b) taking or increasing the risk in order to pursue an opportunity;

c) removing the risk source;

d) changing the likelihood;

e) changing the consequences;

f) sharing the risk (e.g. through contracts, buying insurance);

g) retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and should take into account all of an organization’s obligations, voluntary commitments and views of interested parties. The selection of risk treatment options should be made in accordance with an organization’s objectives, risk criteria and available resources.

4.8 Risk acceptance

When selecting risk treatment options, the values, perceptions and potential involvement of interested parties should be considered, as well as the most appropriate ways to_communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some interested parties than to others.

Risk treatments, even if carefully designed and implemented, are not guaranteed to produce the expected outcomes and can produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatment can also introduce new risks that need to be managed.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other interested parties should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

5 Physical and technical controls

5.1 General

The criteria for physical and technical/electronic premises security systems designed to prevent and detect intrusion into the premises by unauthorized personnel includes, but is not limited to:

a) identification of areas on the premises that requires security protection and/or access restriction;

b) installing and maintaining electronic security systems to notify and record incident(s) in areas where the probability of unauthorized access can occur;

c) maintaining the premises such that visibility and security monitoring of the premises is possible;

d) installing and maintaining video surveillance systems to monitor and record specified areas inside and outside of the protected premises;

e) installing and maintaining electronic systems to detect and/or prevent unauthorized access;

f) the description of the physical security and electronic security systems provided for the perimeter of the site, perimeter around areas where cannabis or cannabis product is present and the perimeter around the secure storage and IT room on the site;

g) the physical and technical/electronic security controls required for the applicable facility/license type;

NOTE These can be required by regulations within the authority having jurisdiction (AHJ).

h) the physical and technical/electronic security controls shall be implemented as per the findings of the security risk assessment (SRA).

Critical areas defined as, but not limited to, storage areas, perimeters and critical infrastructure spaces shall be monitored at all times, subject to the operational requirements of the facility as identified in the SRA.

5.2 Security risk assessment (SRA)

An SRA shall be developed that forms the basis for the physical security programme, including the design of the electronic security systems, to be provided at the protected premises.

NOTE 1 For requirements relating to transportation, see 7.6.

NOTE 2 The AHJ can require that the SRA is submitted for approval.

The SRA shall address the following critical areas:

a) identify the assets to be protected;

b) identify threats to those assets during operations;

c) the specific security measures to be deployed, commensurate with the value of the assets and level/types of threat, broken into three key areas:

   1) physical security measures;

   2) technical security measures;

   3) administrative security measures.

The findings of the SRA shall include, but not be limited to, the following items as appropriate to the level of security required:

a) identification of the physical barriers to be provided, including fencing, doors, walls, ceilings, roofs, intrusion resistant construction, controlled ingress construction;

b) identification of the extent of protection to be provided for all protected security zones in, on and around the premises (see Table 1);

c) identification of the extent of protection to be provided on delivery vehicles and other vehicles including intrusion detection systems;

d) details on security hardware including locks and keyways, latches, and door closers;

e) description of the holdup alarm and duress alarm equipment to be provided, and the location(s) of protection, if applicable;

f) description of the access control system, including controlled entry points, and authorized personnel who can enter into controlled areas (see Table 1);

g) description of video surveillance system equipment, and fields of coverage;

h) procedures to be followed for notifying the relevant authorities if one of more protection measures has been damaged, compromised or otherwise become inoperable. This procedure shall take into account the extent of the loss of protection and the security risk being imposed as a result;

i) communication equipment:

   1) physical security: access to cabling, demarcation points, communication closets, business continuity, crisis management;

2) electronic security: the AHJ or the SRA can require that equipment that is network connected is in compliance with applicable standards such as ANSI/CAN/UL 2900-2-3;

3) cyber-physical security: where hardware and software detect or cause changes through direct monitoring and/or control of physical components/systems, they shall be in compliance with applicable standards, e.g. the IEC 62443 series, regarding technical and organization capabilities;

4) procedures for recommending corrective actions.

A copy of the SRA shall be regularly updated and maintained in a secured location at the premises.

NOTE 3 The AHJ can require that a copy of the SRA is made available, including to authorized security personnel.

The extent of protection provided to protect the premises, areas within the premises, and security containers such as areas of protection and/or secure storage areas shall be provided as specified in the SRA.

NOTE 4 For additional requirements on the extent of protection provided, see CAN/ULC-S302 or ANSI/UL 681. If the security of a protected premises has been compromised, due to fire, accidents, weather or other uncontrollable conditions such that the required level of protection can no longer be maintained, the relevant authorities shall be advised of the situation, in accordance with the SRA.

Table 1 — Security levels, security zones and access

Security level	Security zones	Access
High	1	Secure cannabis storage and IT/OT infrastructure areas, fire alarm units and security control equipment
Medium	2	Areas where cannabis and cannabis product is present
Low	3	Restricted employee access, approved contractors, or visitors

5.3 Physical controls – Specific requirements

5.3.1 Outer physical barriers

These barriers shall be resilient against unauthorized access based on the SRA.

5.3.2 Cultivation areas

These grow areas shall have a level of physical resilience based on the SRA.

Areas shall be fully enclosed according to the SRA (i.e. no open ceiling).

The design and installation of the barriers around the areas (i.e. walls, ceilings, fencing, etc.) shall result in a level of physical resilience and be based on the SRA.

The design and installation of layers of protection in the automation and energy distribution infrastructure shall include consideration for resilience.

5.3.3 Doors/portals

Doors/portals that can be used to enter or exit the protected areas or restricted areas within the protected premises shall be protected and monitored by either alarm system contact switches or access control systems complying with 5.4.4.

Physical barriers, locks and security hardware shall be maintained in an operational condition at all times. Damage to such construction and equipment shall be repaired in the time frame established in the SRA.

5.3.4 Areas of protection and/or secure storage areas

If the findings of the SRA justify the need of an area of protection and/or secure storage area, they shall be provided.

NOTE In such cases, the area of protection and/or secure storage area must comply with the requirements of the standards identified by the AHJ, e.g. ANSI/UL 608, CAN/ULC-S324 or EN 1143-1.

5.3.5 Lighting

The AHJ can require that lighting is provided.

Lighting requirements with respect to video surveillance can be found in 5.4.6.

5.3.6 Security film

Security film shall conform to the requirements of UL 972.

5.4 Technical/electronic controls - Specific requirements

5.4.1 General

Every site shall have an intrusion alarm system.

Access to each processing area shall be secured by means of an intrusion detection system that operates, and is monitored, at all times and that allows for the detection of any attempted or actual unauthorized access to the area, any unauthorized movement in the area and any attempted or actual tampering with the system.

NOTE For requirements relating to transportation, see 7.6

5.4.2 Electronic security systems

An electronic security system that provides signal transmission to a signal receiving centre (SRC) shall transmit the signals to an SRC complying with CAN/ULC-S301, ANSI/UL 827 or EN 50518.

The electronic security systems shall communicate signalling for verification, dispatch and response.

5.4.3 Installation, maintenance, and inspection of the electronic security systems

Installations and/or modifications shall be tested, maintained, inspected and documented on an annual basis. Records of these activities shall be retained for a minimum of two years.

Access control, video surveillance, and other electronic premises security systems shall be tested, inspected and maintained on an annual basis in accordance with IEC 62676-4, IEC 60839-11-1, CAN/ULC-S302 or ANSI/UL 681.

5.4.4 Intrusion detection systems

The perimeter of the site shall have complete protection.

Premises and perimeter protection identified in the SRA shall be installed in accordance with either CAN/ULC-S302 or ANSI/UL 681.

Where installed, intrusion alarm equipment and devices including intrusion detection units, burglar alarm devices, control units, receiving equipment and accessories shall be in accordance with relevant standards, e.g. IEC 60839-11-1, CAN/ULC-S304, CAN/ULC-S306, CAN/ULC-S318.

NOTE 1 Alternative standards can be authorized by the AHJ.

The intrusion alarm system shall have the following minimum features:

a) detectors to indicate unauthorized attempts to tamper with, open, enter or penetrate perimeter entry points, perimeter windows and secure cannabis or cannabis product storage restricted areas;

b) detectors to indicate unauthorized movement within the premises including the secure cannabis or cannabis product storage restricted areas;

c) capability to detect any attempts to tamper with the system or malfunctions with the system.

The intrusion alarm system shall be monitored by a third-party signal receiving centre in accordance with CAN/ULC-S301, ANSI/UL 827 or ASTM D8218 (see Annex C).

NOTE 2 Alternative standards can be authorized by the AHJ.

Other building systems that require monitoring shall be partitioned and provided with their own independent power supplies in accordance with the manufacturers' installation instructions.

5.4.5 Access control systems

The AHJ can require that electronic access control is provided.

The findings of the SRA can result in the specifications of an access control system.

Electronic access control shall be provided for doors and portals that are used to allow authorized personnel to enter the protected premises, or restricted areas within the protected premises, as specified in the SRA.

Electronic access control systems shall comply with applicable requirements in IEC 60839-11-1 and IEC 60839-11-2.

All access control systems, which includes maglocks, door strikes, and electrified hardware (includes specialized locking requirements) shall be designed and installed in accordance with the requirements for means of egress in IWA 37-1.

Access control systems shall be connected to an emergency power system capable of maintaining the site until normal function is returned as identified in the SRA.

Access to each operations area and storage area shall be restricted to individuals whose presence in the area is required by their duties, i.e. they shall be restricted areas.

Access control systems shall be connected to an uninterruptable power supply that will be sufficient for auto-transfer of electrical power, to allow for continuous operation.

An audit trail log shall be maintained for all activities pertaining to entry and exit of control points and storage areas.

All logs and electronic system data shall be retained for a minimum of two years.

5.4.6 Video surveillance systems

The AHJ can require that video surveillance is provided.

The findings of the SRA can result in the specifications of a video surveillance system.

Lighting shall be sufficient to sustain minimum standard requirements to maintain the video surveillance at all times (i.e. infrared technologies).

Video surveillance systems shall be provided to effectively and clearly monitor and record images of the areas designated for surveillance in the SRA at all times.

Video surveillance systems shall be designed, installed, tested, monitored and maintained in accordance with IEC 62676-4.

Video surveillance equipment, enclosures and mounting brackets shall conform to the requirements in IEC 62368-1.

Video surveillance systems shall be monitored in the location identified in the SRA.

Video surveillance systems shall be connected to an uninterruptable power supply that will be sufficient for auto-transfer of electrical power, to allow for continuous operation.

All visual recordings shall be retained and be available for viewing in accordance with the SRA for a minimum of 120 days. Visual recordings of attempts at unauthorized access, or any illicit activity, shall be retained for a minimum of two years after the day of the attempted or actual unauthorized access to the site, or the detection of illicit conduct.

All visual recordings from video surveillance shall be at a minimum resolution of 1920 x 1080 (i.e. digital, not analogue) and recorded at a minimum frame rate of 15 frames per second (fps) on event. Between events, continuous recording at a minimum of 1 fps at a minimum of 1920 x 1080 resolution shall be maintained.

Where provided, if managed video services are used, the facility processing the signals shall comply to the requirements of CAN/ULC-S301, ANSI/UL 827 or ASTM D8218 (see Annex C).

5.5 Cybersecurity controls for operational technology

5.5.1 General

The IEC 62443 series addressed the need to design a robust and resilient model for operational technology (OT) during the cultivation, processing, packaging, storage and/or transportation of cannabis or cannabis products.

The applicability of the IEC 62443 series for OT starts by identifying components and/or systems whose compromise can result in any or all of the following consequences:

a) endangerment of public or employee safety or health;

b) damage to the environment;

c) damage to the equipment under control;

d) loss of product integrity;

e) loss of public confidence or company reputation;

f) violation of legal or regulatory requirements;

g) loss of proprietary or confidential information;

h) financial loss;

i) impact on entity, local, state, or national security.

The subject of OT cybersecurity is applied in the broadest possible sense, encompassing all types of premises, facilities, and systems in all phases of cultivation, processing, packaging, storage and transportation of cannabis or cannabis products. Automation and control systems include, but are not limited to:

a) hardware and software systems such as DCS, PLC, SCADA, power automation and protection, building automation, networked electronic sensing, and monitoring and diagnostic systems;

b) associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Developing, operating and maintaining robustness and resilience programmes for the cultivation, processing, packaging, storage and distribution of cannabis and cannabis products, requires the contribution of asset owners / operators, service providers for integration and maintenance of the premises OT systems and product suppliers across the various phases of the OT system lifecycle.

5.5.2 Roles and responsibilities

The role asset owner (AO) includes two parts. The first part is the accountability for the OT solution including the protection of the OT solution in operation and the associated risks throughout the lifecycle.

The role AO defines the tolerable cybersecurity risk as an input requirement for all cybersecurity activities along the OT solution lifecycle. While remaining accountable, the entity fulfilling this role delegates the responsibilities and the associated activities to entities fulfilling other roles described in this subclause.

The second part assigned to the role AO is the responsibility to operate the OT solution according to defined security policies and procedures. It includes to keep information used in security measures like virus patterns, firewall rules, active accounts list, or backup and restore data up to date.

The inclusion of these two parts in the role AO considers that in many cases the entity which operates the OT solution is also the legal owner and therefore accountable for the OT solution.

The role maintenance service provider (SM) is responsible for the maintenance and decommissioning of the OT solution. Compared to the actualization of the information used in the security measures, which is included in the role AO, the maintenance activities have the purpose to upgrade and eventually complement the measures of the robustness and resilience programme to follow a change in the threat situation or a modification of the OT solution. A maintenance phase is triggered by the result of a cybersecurity risk assessment showing that the measures of robustness and resilience programme no longer provide the desired level of protection. In general, the upgrade includes technical security measures applied to the OT solution as well as organizational security measures for operation of the holistic protection scheme to keep the desired protection of the OT solution in operation. The role SM includes the responsibility for decommissioning parts or the whole OT solution and ensuring that the tolerable residual cybersecurity risk is still matched during or after decommissioning.

The role integration service provider (SI) is responsible for the design and implementation as well as commissioning and validation of the security measures applied to the OT solution. The activities cover the development and validation of a robustness and resilience programme for the OT solution in operation with the goal to match the tolerable cybersecurity risk. These include the development of technical security measures applied to the OT solution as well as guidelines for organizational measures to be implemented during operation. The base for the guidelines is often given by guidelines provided by the role product supplier. It is not unusual that one or several organizations design and deploy parts or the whole OT solution while another organization is responsible for the commissioning and validation of the OT solution.

The role product supplier (PS) is responsible for the development and support of products used in the OT solution. The activities include the development of product security capabilities to be used in the OT solution following an established product development lifecycle process, including incident handling and vulnerability management processes. The role PS has the responsibility for the provision of product specific integration, hardening and operational guidelines for the product(s) they supply to the asset owner.

Figure 2 illustrates how to apply principal roles from the IEC 62443 series to the cannabis cultivation and processing industry.

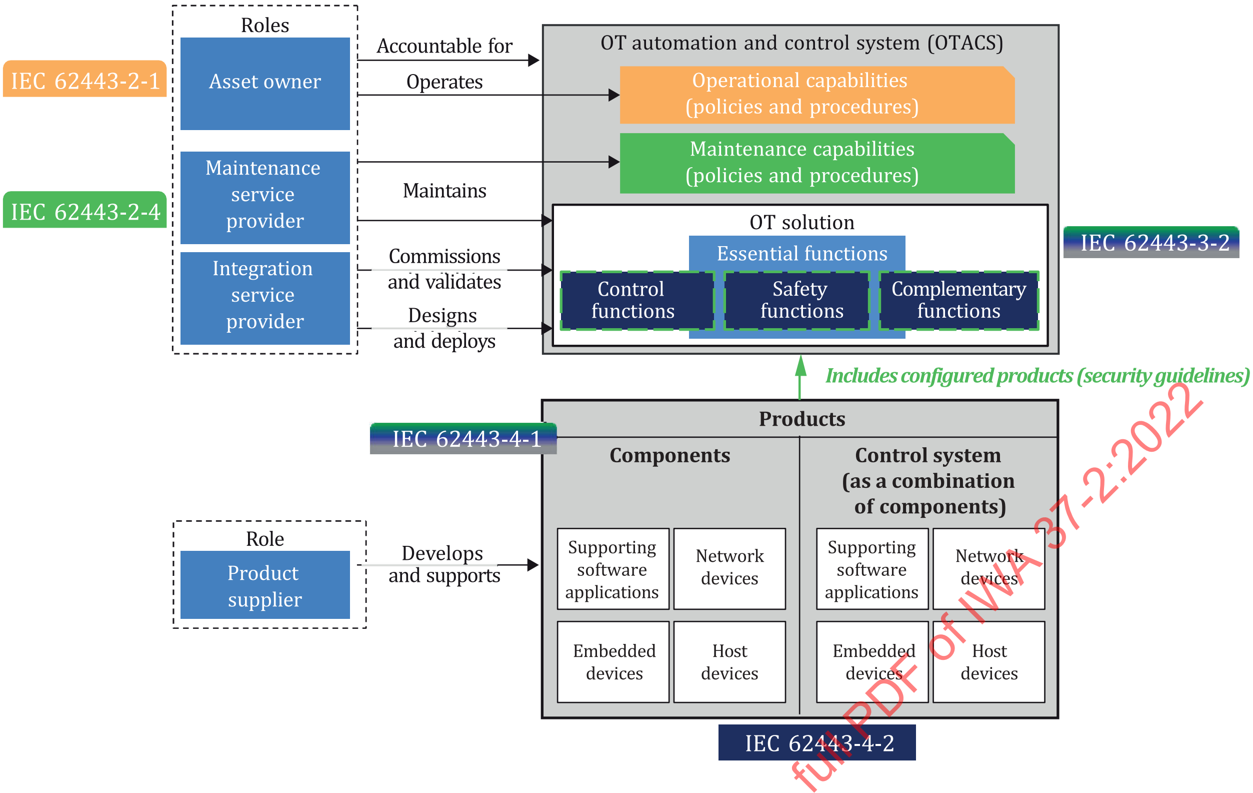

Roles
IEC 62443-2-1
Asset owner
Maintenance service provider
IEC 62443-2-4
Integration service provider
Accountable for
Operates
Maintains
Commissions and validates
Designs and deploys
OT automation and control system (OTACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (policies and procedures)
OT solution
Essential functions
Control functions
Safety functions
Complementary functions
IEC 62443-3-2
Includes configured products (security guidelines)
Products
IEC 62443-4-1
Components
Control system (as a combination of components)
Role
Product supplier
Develops and supports
Supporting software applications
Network devices
Embedded devices
Host devices
Supporting software applications
Network devices
Embedded devices
Host devices
IEC 62443-4-2

Figure 2 — Application of principal roles from the IEC 62443 series to the cannabis cultivation and processing industry

The asset owner is responsible for ensuring that the operation and maintenance of operational technology, including OT systems, industrial automation solutions as well as related components (e.g. greenhouse technology, irrigation, conveyors, packaging), power, lighting and building automation systems, as well as related components, are compliant with the standards and practices required by the IEC 62443 series, including periodic risk assessments and the creation and implementation of a mitigation plan.

5.5.3 Cybersecurity risk assessment

As described in 5.5.2, the asset owner (AO) role risk approach is described in IEC 62443-2-1, IEC 62443-3-2 and ISO/IEC 27001. The identification, prioritization, mitigation and management of cybersecurity risks across an operational technology solution (i.e. irrigation system, building automation system, lighting, HVAC, packaging, labelling) is part of the security programme around the organizational mission.

An initial assessment can be done for a new automation solution design or as part of the maintenance cycle of an existing implementation. The determination of a risk level is defined by IEC 62443-3-2 as “initial risk”. Throughout an iteration of the application of security countermeasures and reassessments, the risk is reduced to a tolerable risk that is deemed acceptable to the asset owner.

The iterative process and workflow are described in IEC 62443-3-2. The requirements to perform periodic assessments and maintenance on the security posture of the operational technology (OT) installation is a requirement to the service provider performing the integration, commissioning and maintenance role in accordance with IEC 62443-2-4.

6 Administrative controls

6.1 General

6.1.1 Continual improvement cycle

A business continuity management system (BCMS) should be implemented to ensure a degree of consistency with the requirements for risk assessment in Clause 4 and with related management systems standards (e.g. ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 and ISO 28000).

Work procedures such as written policies, standards, procedures, rules, supervision, schedules, and training should be maintained under a continual improvement system.

This document applies continual improvement cycle of Plan (establish) – Do (implement and operate) – Check (monitor and review) – Act (maintain and improve) (PDCA) to implement, maintain and continually improve the effectiveness of an organization's BCMS.

In accordance with the continual improvement cycle, the BCMS covers the following components:

a) the requirements necessary to establish the context of the BCMS applicable to an organization, as well as needs, requirements and scope (see ISO 22301:2019, Clause 4);

b) the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations via a policy statement (see ISO 22301:2019, Clause 5);

c) the requirements for establishing strategic objectives and guiding principles for the BCMS as a whole (see ISO 22301:2019, Clause 6);

d) BCMS operations related to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documented information (see ISO 22301:2019, Clause 7);

e) business continuity needs, how to address them and procedures to manage an organization during a disruption (see ISO 22301:2019, Clause 8);

f) the requirements necessary to measure business continuity performance, BCMS conformity with this document, and to conduct management review (see ISO 22301:2019, Clause 9);

g) identification of BCMS nonconformity and continual improvement through corrective action (see ISO 22301:2019, Clause 10).

6.1.2 Administrative controls table

Annex B gives a list of administrative controls.

6.1.3 Security management policy

An overall security management policy shall be authorized by top management. The policy shall:

a) be consistent with other organizational policies;

b) provide the framework which enables the specific security management objectives, targets and programmes to be produced;

c) be consistent with an organization's overall security threat and risk management framework;

d) be appropriate to the threats to an organization and the nature and scale of its operations;

e) clearly state the overall/broad security management objectives;

f) include a commitment to continual improvement of the security management process;

g) include a commitment to comply with current requirements to which an organization subscribes;

h) be visibly endorsed by top management;

i) be documented, implemented and maintained;

j) be communicated to all relevant employees and third parties, including contractors and visitors, with the intent that these persons are made aware of their individual obligations related to security management;

k) be available to interested parties where appropriate;

l) provide for its review in case of the acquisition of, or merger with, other organizations, or other changes to an organization's business scope which can affect the continuity or relevance of a security management system.

NOTE Organizations can choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive a security management system (parts of which can be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its own and other interested parties.

6.1.4 Implementation and operation

An organizational structure of roles, responsibilities and authorities shall be established and maintained, consistent with the achievement of the security management policy, objectives, targets and programmes.

These roles, responsibilities and authorities shall be defined, documented and communicated to the individuals responsible for implementation and maintenance.

Top management shall provide evidence of its commitment to the development and implementation of security management processes and continually improving its effectiveness by:

a) appointing a member of top management who, irrespective of other responsibilities, shall be responsible for the overall design, maintenance, documentation and improvement of the security management processes;

b) appointing at least one member of management with the necessary authority to ensure that the objectives and targets are implemented;

c) identifying and monitoring the requirements and expectations of interested parties and taking appropriate and timely action to manage these expectations;

d) ensuring the availability of adequate resources;

e) considering the adverse impact that the security management policy, objectives, targets, programmes, etc., can have on other aspects of an organization;

f) ensuring that any security programmes generated from other parts of an organization complement the security management processes;

g) communicating within an organization the importance of meeting its security management requirements in order to comply with its policy;

h) ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate;

i) ensuring the viability of the security management objectives, targets and programmes.

6.1.5 Preparing and implementing risk treatment plans

The purpose of a risk treatment plan is to specify how a chosen treatment option will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

A treatment plan should be integrated into an organization's management plans and processes, in consultation with appropriate interested parties.

The information provided in the treatment plan should include:

a) the rationale for selection of the treatment options, including the expected benefits to be gained;

b) those who are accountable and responsible for approving and implementing the plan;

c) the proposed actions;

d) the resources required, including contingencies;

e) the performance measures;

f) the constraints;

g) the required reporting and monitoring;

h) when actions are expected to be undertaken and completed.

6.1.6 Competence training and awareness

Personnel responsible for the design, operation, management and maintenance of security equipment and processes shall be suitably qualified in terms of education, training and/or experience. Procedures shall be established and maintained to make persons working for an organization, or on its behalf, aware of:

a) the importance of compliance with the security management policy and procedures, and to the requirements of the security management processes;

b) their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management processes, including emergency preparedness and response requirements;

c) the potential consequences for an organization's security of departing from specified operating procedures.

A training plan shall be developed and implemented.

Documented evidence of competence and training shall be kept for an appropriate period, and be available for inspection at all times.

NOTE Specific AHJ requirements can apply.

6.2 Traceability system

6.2.1 General

6.2.1.1 General principles

A traceability system shall be implemented in accordance with ISO 22005 to ensure the security of cannabis and cannabis products, in accordance with the context related to the operational requirements and procedures, congruent with an organization's role in the cannabis supply chain and in accordance with IWA 37-3.

Traceability systems should be able to document the history of the cannabis or cannabis product and/or locate a cannabis product in the cannabis supply chain. Traceability systems contribute to the search for the cause of security nonconformity and the ability to trace back and investigate, if necessary. Traceability systems can improve the appropriate use and reliability of information, as well as the effectiveness and productivity of an organization.

Traceability systems should be able to achieve the objectives (see 6.2.1.2) from a technical and economic point of view.

Movement can relate to the origin of the materials, the processing history, or the distribution of the cannabis or cannabis product, and should address at least one step forward and one step backward for each organization in the chain. Upon agreement among all the organizations concerned, it may apply to more than one part of the chain.

A seed-to-sale software should be implemented in order to share information and real time records of the inventory with entities including, but not limited to, law enforcement, tax agencies or certifying bodies or agencies.

Traceability systems should be:

a) verifiable;

b) applied consistently and equitably;

c) results oriented;

d) cost effective;

e) practical to apply;

f) compliant with any applicable policy;

g) compliant with defined accuracy requirements.

6.2.1.2 Objectives

In developing a cannabis traceability system, it is necessary to identify the specific objectives to be achieved. These objectives should take into consideration the principles identified in 6.2.1.1 and allow for trace-back or investigation of any instances of cannabis or cannabis product nonconformity.

Examples of objectives are the following:

a) to identify ingredients; lot number(s); process start/end times and packaging materials;

b) to record chain of custody at critical control points (CCPs) in production (location, time, personnel with custody/responsibility, observations or notes of any standard operating procedure (SOP) deviations by personnel with custody/responsibility);

c) to record cannabis or cannabis product mass at CCPs including material lost constituting both reportable and non-reportable amounts;

NOTE This can be defined by the AHJ.

d) to record cannabis or cannabis product destruction/disposition;

e) to support safety and/or quality objectives;

f) to meet customer specification(s);

g) to determine the history or origin of the lot/batch of cannabis or cannabis product;

h) to identify the responsible organizations;

i) to facilitate the verification of specific information about the lot/batch of cannabis or cannabis product;

j) to communicate information to relevant interested parties and consumers;

k) to improve the effectiveness, productivity and profitability of an organization.

6.2.2 General design considerations

A traceability system is a tool that can be designed within the context of a broader security management system.

The choice of a traceability system should result from balancing the different requirements, the technical feasibility and the economic acceptability.

The traceability system should be verifiable.

Each element of a traceability system shall be considered according to the threat and risk assessment and justified on a case-by-case basis, taking into account the objectives to be achieved.

In the design of a traceability system, the following shall be included:

a) objectives;

b) products and/or ingredients;

c) position in the supply chain;

d) flow of materials;

e) information requirements;

f) procedures;

g) documentation;

h) supply chain coordination.

An organization shall identify the relevant requirements to be met by the traceability system, including the objectives, policy and procedures.

Figure 3 illustrates the five steps in the cannabis supply chain. The steps are cultivation, extraction, testing, distribution and retail. Each phase requires that the process be traceable at all times. These safeguards are paramount and shall be accessible throughout the complete process.

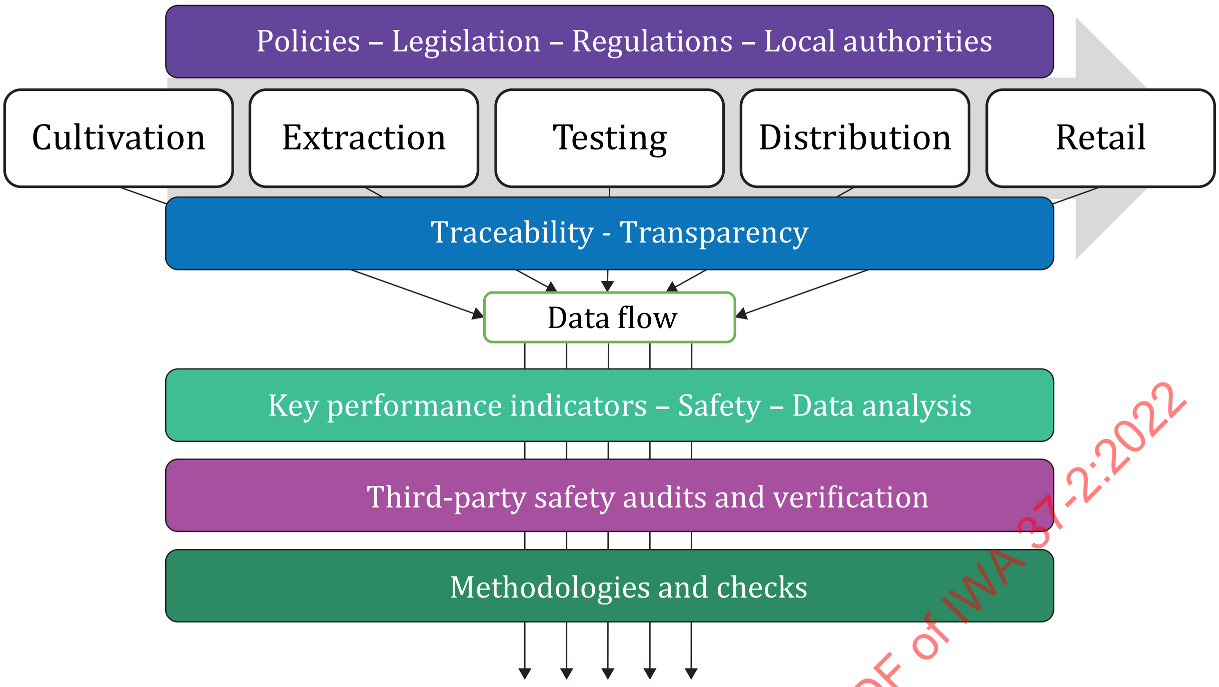

Policies – Legislation – Regulations – Local authorities
Cultivation
Extraction
Testing
Distribution
Retail
Traceability - Transparency
Data flow
Key performance indicators – Safety – Data analysis
Third-party safety audits and verification
Methodologies and checks

Figure 3 — Cannabis supply chain

6.2.3 Minimum requirements

6.2.3.1 Position in the cannabis supply chain

An organization shall determine its position in the cannabis supply chain by at least identifying its suppliers and customers.

6.2.3.2 Flow of materials

An organization shall determine and document the flow of materials within its control in a manner which meets the objectives of the traceability system.

6.2.3.3 Information requirements

6.2.3.3.1 General

In order to meet its traceability objectives, an organization shall define the information:

a) to be obtained from its suppliers;

b) to be collected concerning the product and process history;

c) to be provided to its customers and/or suppliers.

The product tracking activity for cannabis and cannabis products shall record the lot number of an organization, as well as the supplier lot numbers for all materials, ingredients, and packaging materials.

NOTE The information required for a traceability system is influenced by its objectives and by an organization's position in the cannabis supply chain.

6.2.3.3.2 Lot identification

Every lot (or batch) shall be identified with a lot number.

The lot identification process of assigning a unique code or number to a starting material lot shall include real-time visual documented evidence such as pictures or videos to avoid modified or counterfeit information storage.

Lot identification records shall also include:

a) lot identification number;

b) potency (CBD and THC) and certificate of analysis including any mandatory testing;

NOTE This can be required by the AHJ.

c) records of any material removed from lot or determined to be unusable or otherwise destroyed;

d) any additional information required at any step of the supply chain.

6.2.3.3.3 Location

The tracking system should identify, at any point in the supply chain from primary production to consumption, at least the:

a) location;

b) place of production;

c) processing;

d) distribution;

e) storage;

f) handling.

6.2.3.3.4 Data

6.2.3.3.4.1 Types of data

The traceability system shall maintain the totality of data, operations, desired information about a product, and its components, through all of its production and use chain.

6.2.3.3.4.2 Quality of data

The traceability system implemented shall ensure completeness, uniqueness, timeliness, validity, accuracy, and consistency of collected data.

6.2.3.3.4.3 Record and retention

The data shall be stored in a non-proprietary format that is retrievable for a period no less than two years. Records shall be kept for a period no less than two years.

NOTE The AHJ can specify requirements for record retention time.

6.2.3.4 Establishment of procedures

Procedures generally relate to documenting the flow of materials and related information, including document retention and verification. An organization shall establish procedures that include at least the following:

a) product definition;

b) lot definition and identification;

c) documentation of flow of materials, and information including media for record keeping;

d) data management and recording protocols;

e) information retrieval protocols.

In the development and implementation of a traceability system, an organization's existing operation and management processes shall be taken into account.

Procedures to manage traceability information shall include a means to link and record the flow of information concerning materials and products, if needed.

Procedures shall be established to deal with nonconformity in the traceability system. These procedures should include preventive and corrective actions.

6.2.3.5 Documentation requirements

An organization shall determine which documentation is required to achieve the objectives of its traceability system.

Appropriate documentation shall include, as a minimum:

a) a description of the relevant steps in the chain;

b) a description of the responsibilities for the management of traceability data;

c) written or recorded information documenting the traceability activities and manufacturing process, flows and results of traceability verification and audits;

d) documentation addressing action taken to manage nonconformity related to the established traceability system;

e) document retention times.

ISO 22000 provides information on the control of documentation, the control of records and the identified objectives of a traceability system.

6.2.3.6 Cannabis supply chain coordination

If an organization participates in a traceability system with other organizations, the design elements (see 6.2.2) shall be coordinated. Links in the cannabis and cannabis product supply chain are established as each organization identifies its immediate prior source(s) and immediate subsequent recipient(s). When a claim is made about "cannabis supply chain traceability", the relevant steps in the cannabis supply chain shall be identified by the organization making the claim and shall be supported by verification information.

6.2.3.7 Chain of custody

As the responsibility for cannabis or cannabis products is transferred through the supply chain from an organization to another, the tracking system shall be able to carry all batch and lot information and details from the prior organizations to the next steps of the supply chain. The receiver of such information should keep all the given information as per good documentation practices without arbitrary selection.

The traceability system shall carry all the information through the life of the cannabis product and the supply chain sequence of all the stages and operations involved in the production, processing, distribution and handling from primary production to retail sale.

6.2.4 Verification/ mass balance / products reconciliation

At each position in the cannabis supply chain, procedures and equipment should be in place to verify the effectiveness of the traceability system by means of mass balance and/or quantitative product reconciliation between:

- two points within the organization;
- the organization and its immediate prior source(s); or
- the organization and its immediate subsequent recipient(s).

6.2.5 Monitoring

A monitoring scheme shall be established for the traceability system.

6.2.6 Key performance indicators

Key performance indicators shall be established to measure the effectiveness of the system.

6.2.7 Audit scheduled

An organization shall conduct internal audits at planned intervals, to assess the effectiveness of the system to meet the established objectives.

6.2.8 Review

An organization shall review the traceability system at appropriate intervals, or whenever changes are made to the objectives and/or the product or processes. Based on this review, the appropriate corrective and preventive action(s) shall be taken. This allows the establishment of a continuous improvement process. This review shall include, but is not limited to, the following:

a) traceability test results;

b) traceability audit findings;

c) changes to product or processes;

d) traceability-related information provided by other organizations throughout the supply chain;

e) corrective actions related to traceability;

f) customer feedback, including complaints, related to traceability;

g) new or amended regulations affecting traceability;

h) new statistical evaluation methods.

6.3 Security management documentation

6.3.1 General

Processes for security management documentation shall be established and maintained including, but not limited, to the following:

a) the security policy, objectives and targets;

b) a description of the scope of the security management processes;

c) a description of the main elements of the security management processes and their interaction, and reference to related documents;

d) documentation, including records, required by this document;

e) documentation, including records that an organization determines to be necessary to ensure the effective planning, operation and control of processes that relate to its significant security threats and risks.

The security sensitivity of information shall be determined and steps shall be taken to prevent unauthorized access.

6.3.2 Document and data control

Procedures shall be established and maintained for controlling all documents, data and information required by 6.1.4, 6.1.5, 6.1.6 and 6.3 to ensure that:

a) the documents, data and information can be located and accessed only by authorized individuals;

b) the documents, data and information are periodically reviewed, revised as necessary, and approved for adequacy by authorized personnel;

c) current versions of relevant documents, data and information are available at all locations where operations essential to the effective functioning of the security management processes are performed;

d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;

e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified;

f) the documents, data and information are secure, and if in electronic form are adequately backed up and can be recovered.

6.3.3 Operational control

An organization shall identify those operations and activities that are necessary for achieving:

a) its security management policy;

b) the control of activities, and the mitigation of threats identified as having significant risk;

c) compliance with legal, statutory and other regulatory security requirements;

d) its security management objectives;

e) the delivery of its security management programmes;

f) the required level of supply chain security.

These operations and activities shall be carried out under specified conditions by:

a) establishing, implementing and maintaining documented procedures to control situations where their absence can lead to failure to achieve the operations and activities as listed above;

b) evaluating any threats posed from upstream supply chain activities and applying controls to mitigate these impacts to the organization and other downstream supply chain operators;

c) establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors.

These procedures shall include controls for the design, installation, operation, refurbishment, and modification of security related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced that can impact on security management operations and activities, an organization shall consider the associated security threats and risks before their implementation. The new or revised arrangements to be considered shall include:

a) revised organizational structure, roles or responsibilities;

b) revised security management policy, objectives, targets or programmes;

c) revised processes and procedures;

d) the introduction of new infrastructure, security equipment or technology, which can include hardware and/or software;

e) the introduction of new contractors, suppliers or personnel, as appropriate.

6.3.4 Emergency response and security recovery

Appropriate plans and procedures shall be established, implemented and maintained to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them. The plans and procedures shall include information on the provision and maintenance of any identified equipment, facilities or services that can be required during or after incidents or emergency situations.

The effectiveness of an organization's emergency preparedness, response and security recovery plans and procedures shall be reviewed periodically, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats. These procedures shall be tested periodically, where practicable.

7 Requirements for specific activities

7.1 Cultivation

7.1.1 Physical and technical/electronic controls for cultivation

7.1.1.1 General

See 5.1 to 5.4, for requirements on physical and technical/electronic controls for cultivation.

7.1.1.2 Technical/cybersecurity for cultivation

See 5.5 for requirements on cybersecurity for cultivation.

7.1.2 Administrative controls for cultivation security

7.1.2.1 General

Cannabis cultivation is the first phase (see Figure 3) of the cannabis supply chain, and therefore constitutes the first critical step of identifying and integrating required controls.

NOTE Specific AHJ requirements can apply.

Organizations cultivating cannabis should implement policies on background checks for personnel and all candidates for employment proportional to the business requirements, the classification relating to the cultivation security to be assessed, and the perceived risks.

7.1.2.2 Personnel qualifications, training and supervision for cultivation

Personnel with direct or indirect functions on cultivation shall be identified in a documented organizational chart, with built-in redundancy/alternate staff as required, explanatory of the mandate and responsibilities of every member of the team.

At any time during operations hours in the cultivation site the identified and qualified responsible person or identified alternate should be present to supervise and monitor the activities.

Every role of the personnel for the cannabis cultivation should be validated through documented evidence, including but not limited to education, qualifications, training, technical knowledge, skills and experience.

All personnel for the cultivation sector shall act impartially, adhere to confidentiality, adhere to an organization's requirements for quality and have documented competency for all functions that have influence on the cultivation activities. This includes, but is not limited to education, qualifications, training, technical knowledge, skills and experience.

NOTE Specific AHJ requirements can apply.

7.1.2.3 Applicable general requirements

The personnel assigned to cannabis cultivation activities shall be 18 years or older .

Starting material shall be sourced only from authorized organizations. The starting material should carry genetic analysis for the unique identification of such products.

Top management should develop, authorize and implement a quality manual in accordance with the activities performed and which:

a) provides a framework to enable the specific standard operating procedures governing cultivation activities;

b) identifies a person responsible for quality security in addition to quality assurance requirements;

c) complies with the security risk assessment in all applicable parts.

NOTE Specific AHJ requirements can apply.

7.1.2.4 Design minimum requirements

7.1.2.4.1 General

In the design of a cannabis cultivation system, the general design considerations in 6.2 shall be followed.

7.1.2.4.2 Position in the supply chain

Organizations cultivating cannabis shall comply with 6.2.3.1.

7.1.2.4.3 Flow of materials

Organizations cultivating cannabis shall comply with 6.2.3.2.

7.1.2.4.4 Information requirements

Organizations cultivating cannabis shall comply with 6.2.3.3.

7.1.2.4.5 Establishment of procedures

Organizations cultivating cannabis shall comply with 6.2.3.4.

7.1.2.4.6 Documentation requirements

Organizations cultivating cannabis shall comply with 6.2.3.5.

7.1.2.4.7 Cannabis supply chain coordination

Organizations cultivating cannabis shall comply with 6.2.3.6.

7.1.2.4.8 Chain of custody

Organizations cultivating cannabis shall comply with 6.2.3.7.

7.1.2.5 Implementation

7.1.2.5.1 Plan

An organization shall be able to demonstrate with documented evidence at any time the commitment to fulfil identified security standards, quality standards and traceability requirements for cultivation activities.

NOTE Specific AHJ requirements can apply.

Following the design and development of a traceability system, an organization shall implement the steps specified so as to ensure conformity to the security of cultivation activities.

Each organization may choose appropriate tools to trace cultivation records and communicate information to its personnel.

7.1.2.5.2 Procedural controls for cultivation

Organizations cultivating cannabis shall comply with 6.2.

7.1.2.5.3 Responsibilities

An organization shall define and communicate tasks and responsibilities to its personnel.

7.1.2.5.4 Training Plan

An organization shall develop and implement a training plan. Personnel who can affect the traceability system shall be adequately trained and informed.

They shall be able to demonstrate competence to correctly implement the traceability system.

7.1.2.5.5 Monitoring

An organization shall establish a monitoring scheme for the security of cultivation areas and activities.

7.1.2.5.6 Key performance indicators

An organization shall establish key performance indicators to measure the effectiveness of the security of cultivation areas and activities.

7.1.2.5.7 Audit scheduled

An organization shall conduct internal audits at planned intervals, to assess the effectiveness of the security of cultivation areas and activities to meet the established objectives.

7.1.2.6 Review

An organization shall review the security of cultivation areas and activities at appropriate intervals, or whenever changes are made to the objectives and/or the product or processes. Based on this review, the appropriate corrective and preventive action(s) shall be taken. This allows the establishment of a continuous improvement process.

7.2 Processing

7.2.1 Physical controls for processing

See 5.1 to 5.3 for requirements on physical and technical/electronic controls for processing.

7.2.2 Technical/Electronic controls for processing

7.2.2.1 General

See 5.4 for requirements on physical controls for processing.

7.2.2.2 Manual access and tracking systems

Security guards shall be present on the cultivation site at all times and a manual tracking log shall be provided and maintained, unless this function is provided by an electronic access control system.

7.2.2.3 Monitoring and response

Where response and dispatch is performed remotely, it shall be in accordance with CAN/ULC-S301, ANSI/UL 827 or ASTM D8218 (see Annex C).

Where response and dispatch is provided by the security management of the facility, it shall be staffed at all times, in accordance with the SRA.

If an event is detected, the holder of the license shall ensure that a log record is retained for two years that contains the following information:

a) date and time of event;

b) individuals present during time of event;

c) measures taken in response to it, and the date and time they were taken;

d) electronic security system components and architecture that identified and reported the incident.

7.2.2.4 Cybersecurity controls for processing

See 5.5 for requirements on cybersecurity for processing.

7.2.3 Administrative controls for processing

7.2.3.1 Applicable general requirements

Specific documents, or clauses of documents, shall be developed for all cannabis or cannabis derivative processing activities at a site. These shall address risk assessment, security management, continual improvement, administrative controls, traceability, operational control, emergency response and security recovery.

Security operations shall be conducted in accordance with all relevant requirements, such as but not limited to:

a) the presence of an appropriately authorized person;

b) facilitating the rapid and complete recall of specific lots or batches;

c) safekeeping of cannabis or cannabis derivative in-process, including storage between process steps.

7.2.3.2 Procedural controls for processing

Access to each processing area shall be restricted to individuals whose presence in that area is required by their duties.

Record-keeping shall be conducted in accordance with all relevant requirements, such as but not limited to:

a) Intrusion events, as well as the responses, interventions and resolutions;

b) The actual numbers of entries and exits for controlled areas, both total and per individual person, and a comparison to the corresponding Operational Plan values.

Security operations shall be subject to periodic audits. Any identified corrective actions or opportunities for improvement shall be input to the continual improvement cycle.

7.2.3.3 Personnel qualifications, training and supervision for processing

Qualifications of personnel shall be established and maintained in accordance with all relevant requirements, such as but not limited to:

a) security clearance levels (initial, as well as periodic reassessments);

b) character references (initial, as well as periodic reassessments);

c) criminal record verifications (initial, as well as periodic reassessments);

d) Operational training, certification and recertification, as applicable.

A training plan shall be established and maintained for each security staff member or contractor.

Supervision of personnel shall include performance objectives specific to processing activities and facilities.

7.2.3.4 Operational design/plan

The operational design/plan shall:

— include the designated responses, interventions, resolutions and record keeping for any unauthorized intrusion into a processing area;

— include, where applicable, estimates of the anticipated numbers of entries and exits for controlled areas, both total and per individual person;

— include specific instructions for implementation of the applicable clauses of any business continuity plan or emergency action plan;

— identify the respective responsibilities of security specialists, as well as all other personnel, for processing facilities and operations;

— identify the frequency of periodic audits, as well as the scope of the audit plan.

7.2.3.5 Implementation

7.2.3.5.1 Operations

Security operations shall take into account the value-added content of cannabis, cannabis derivative, cannabis edible, and/or cannabis product that is progressing through process steps within the facility.

7.2.3.5.2 Reception of a secure package

7.2.3.5.2.1 Approval of reception / quarantine

Upon arrival at the site, a secure package shall be quarantined, unopened, in a secure storage area, separated from unsecured packages and cannabis or cannabis product intended for outbound shipment in secured packages, until it is transferred to the appropriate controlled area for opening.

The process of transfer of the unopened secure package to the appropriate controlled area for opening shall maintain the chain of custody for the cannabis or cannabis product, including the validity of records.

Opening, unpacking and verification of the contents of a secure package, shall:

a) take place in a controlled area;

b) take place in the presence of one or more authorized persons, as required by the operational design/plan;

c) take place under video surveillance, if required by the operational design/plan;

d) verify the following information;

   1) the type of cannabis and/or cannabis product including applicable quality metrics, in the secure package;

   2) the quantity of cannabis and/or cannabis product in the secure package;

   3) the actual shipment date, transit duration, and arrival date;

   4) the identities of representatives for carriers and any agents;

   5) the identifiers for all applicable documentation included in or with the secure package;

   6) the unique identifier for the secure package and related tracking control measures;

   7) any other information necessary to maintain the chain of custody for cannabis and/or cannabis product.

e) maintain the chain of custody for the cannabis or cannabis product, including the validity of records.

Disposal of packaging materials from an opened secure package shall result in the destruction of bar-coded labels or other materials that present a risk of being diverted to fraudulent use.

Transfer to inventory, cultivation or processing of the contents of a secure package shall maintain the chain of custody for the cannabis or cannabis product, including the validity of records, as well as the corresponding level of security identified in the operational design/plan.

7.2.3.5.2.2 Complaint or Recall

The chain of custody and the tracking system with associated records shall permit the identification of the contents of the received secure package, if this will be subject to complaint or recall, the procedural operations in place shall allow the immediate physical isolation of the cannabis or cannabis products for further investigation and procedures.

7.2.3.5.3 Preparation of a secure package

7.2.3.5.3.1 Coordination with customer, internal or external

Cannabis or cannabis products intended for shipment in a secured package shall be quarantined, in a secure storage area, separated from unsecured packages, and inbound secure packages.

All secured packages shall be subject to coordination with the consignee or customer, as follows.

a) The individuals undertaking the coordination, representing the consigner and consignee, shall be authorized persons.

b) The following information shall be verified by both parties:

   1) the type of cannabis or cannabis product, including applicable quality metrics, in the secure package;

   2) the quantity of cannabis or cannabis product in the secure package;

   3) planned shipment date, transit duration, and arrival date;

   4) the identities of representatives for carriers, and any agents;

   5) the types of all applicable regulatory documentation, with the individuals responsible for completing different parts of the documents;

   6) the unique identifier for the secure package, and related tracking control measures;

   7) procedures to maintain the chain of custody for the cannabis or cannabis product.

Verification of the contents, preparation, packing and final sealing of a secure package, shall:

a) take place in a controlled area;

b) take place in the presence of one or more authorized persons, as required by the operational design/plan;

c) take place under video surveillance, if required by the operational design/plan;

d) include verification of the following information:

   1) the type of cannabis or cannabis product, including applicable quality metrics, in the secure package;

   2) the quantity of cannabis or cannabis product in the secure package;

   3) planned shipment date, transit duration, and arrival date;

   4) the identities of representatives for carriers, and any agents;

   5) the types of all applicable regulatory documentation, with the individuals responsible for completing different parts of the documents;

   6) the unique identifier for the secure package, and related tracking control measures;

   7) procedures to maintain the chain of custody for the cannabis or cannabis product;

   8) maintain the intended security level of the package;

e) maintain the chain of custody for the cannabis or cannabis product, including the validity of records.

7.2.3.5.3.2 Complaint or recall

The chain of custody and associated records shall permit the identification of the contents of a shipped secured package, such that the consignee can use the lot number, batch number, or equivalent information to isolate the cannabis or cannabis product for investigation in the event of a complaint or recall.

7.3 Storage/distribution

7.3.1 Physical and technical/electronic controls for storage/distribution

See Clause 5 for requirements on physical controls for storage/distribution unless the SRA for each stage indicates otherwise.

7.3.2 Cybersecurity controls for storage/distribution

See 5.5 for requirements on cybersecurity for storage/distribution.

7.3.3 Administrative controls for storage/distribution

7.3.3.1 Applicable general requirements

For all sites, operation areas or storage areas, the licensee shall ensure compliance with , but not limited to, the following:

a) location of storage area;

b) restricted access;

c) physical barrier;

d) visual monitoring;

e) visual recording devices;

f) intrusion detection system;

g) monitoring and response;

h) record of detected occurrences.

7.3.3.2 Procedural controls for storage/distribution

An organization shall identify those operations and activities that are necessary for achieving:

a) security clearances and adverse information about employees;

b) physical security;

c) security awareness and training;

d) prevention and mitigation of slip, trip and falls;

e) safe storage and effective inventory control for pesticides;

f) security for machinery and powered industrial vehicles;

g) hazardous waste management;

h) hazmat training and/or awareness;

i) effective resolution for complaint and recall;

j) security of record keeping, reporting and testing.

A plan shall be implemented that covers the items listed above, based on a time cycle, in order to plan the activities and ensure at least the minimum necessary training. After completion of the training, all personnel should demonstrate:

a) knowledge and awareness of potential security risks associated with the site, areas, materials and processes;

b) the ability to recognize imminent security risks;

c) the capacity to remove themselves from work situations that they consider present a security risk;

d) the appropriate response measures to potential or actual security risks.

The plan shall include arrangements for protecting all personnel from undue consequences resulting from initiating response measures to potential or actual security risks.

7.3.3.3 Personnel qualifications, training and supervision for storage/distribution

Personnel responsible for maintaining operation, management and processes shall be suitably qualified in terms of education, training and or experience. Procedures shall be established and maintained to make persons working for an organization, or on its behalf, aware of:

a) the importance of compliance with the security policies and procedures and of its requirements;

b) their roles and responsibilities in achieving compliance with the security policies and procedures and its requirements, including emergency preparedness and response requirements;

c) the potential consequences for the security of an organization of departing from specific operating procedures.

Documented evidence of competence and training shall be kept for an appropriate period, and be available for inspection at all times.

NOTE Specific AHJ requirements can apply.

7.4 Research/Testing laboratory

7.4.1 Physical controls for research/testing laboratory

7.4.1.1 General

See Clause 5 for requirements on physical controls for research/testing laboratory unless the SRA for each stage indicates otherwise.

All perimeter doors shall be secured against unauthorized access. Non-public doors shall remain locked at all times, except for emergencies and deliveries.

All exterior doors shall be equipped with a 180° viewing device to screen persons before allowing entry.

Heavier duty door frames with a three-step locking system shall be provided.

7.4.1.2 Storage for research/testing laboratory

Except as permitted in 5.2, any areas within a research/testing laboratory where cannabis or cannabis products are stored, including any receiving or staging areas where cannabis or cannabis products are present, shall be fully enclosed in a secure environment. This environment can form the external walls of the building, excluding any loading/unloading bays and entry door areas.

Requirements on safe classification shall be in accordance with ANSI/UL 687 or EN 1143-1.

Instead of a storage room, a research/testing laboratory may choose to secure cannabis or cannabis products in a burglary-resistant safe or similar device (such as a locking refrigeration unit) that conforms to the following requirements:

a) The safe shall be rated to a minimum Class TL-15 or equivalent;

b) The safe shall be permanently anchored as per manufacturer recommendations.

7.4.1.3 Site and floor plans

Site plans and floor plans for the research/testing laboratory shall be completed and shall include details for:

a) Secure lobby;

b) Areas of protection and/or secure storage areas;

c) Secure research/testing laboratory.

7.4.2 Technical/Electronic controls for research/testing laboratory

7.4.2.1 Intrusion detection system for research/testing laboratory

The intrusion detection system for the research/testing laboratory and secure cannabis storage restricted areas shall be in accordance with the SRA in Clause 4 and 5.4.

7.4.2.2 Video surveillance system for research/testing laboratory

A video surveillance system shall meet the minimum requirements of IEC 62676-4 or ASTM D8205.

A research/testing laboratory shall have a video surveillance system installed with the following minimum features:

a) Cameras that are enclosed in the ceiling or domes and linked to a monitor and recording system located in a secure area within the premises;

b) Cameras and lighting that are positioned to clearly capture full unobstructed 24 h coverage of activity identifying all individuals:

   1) entering and exiting the premises;

   2) within the premises in areas:

      i) where cannabis is present;

      ii) identified in the SRA (see Clause 4 and 5.2);

      iii) any storage areas for cannabis or cannabis product, such as areas of protection and/or secure storage areas;

      iv) locations, such as:

         — receiving areas;

- offices and other staff areas.

NOTE 1 Some jurisdictions can also require video coverage of the car park, loading areas, exterior sides of the site and adjacent public rights of way.

The system shall be capable of a recording retention of a minimum of 60 calendar-days in a common format that is easily accessible, captured, viewed and capable of producing video and still images that clearly identify individuals and contain a time/date stamp.

All visual recordings from video surveillance shall be at a minimum resolution of 1920 x 1080 and recorded at a minimum frame rate of 15 frames per second (fps) on event. Between events, continuous recording at a minimum of 1 fps at a minimum of 1920 x 1080 resolution shall be maintained.

Recorded video shall be stored in a secure location in accordance with a maintained SRA showing camera numbers, locations, coverage, authorized users list and operating instructions.

Viewing capability shall be accessible within the premises in accordance with a maintained SRA showing camera numbers, locations, coverage, authorized users list and operating instructions.

In cases of an event occurring or of any pending criminal or regulatory investigation, recorded data and relevant information are prohibited to be destroyed for a minimum of a 60 calendar-day period.

NOTE 2 The AHJ can request that the data and information are made available.

The system shall be tested annually or more frequently in accordance with IEC 62676-4, to ensure that all cameras and recording equipment are functioning properly. A log of the test results shall be kept.

NOTE 3 The AHJ can request that the log of test results is made available.

Corrective action of identified deficiencies shall be completed within 30 days.

Video recording shall not require proprietary software for third-party viewing.

7.4.2.3 Lighting

Lighting shall be in accordance with the SRA in Clause 4 and 5.2.

7.4.2.4 Incident log

When an incident occurs at a research/testing laboratory, the details shall be recorded in an incident log. All incidents that adversely affect patrons or staff, or that affect the operation of the research/testing site, as well as "near-miss" incidents, shall be recorded in the log and be available to inspectors.

An incident report shall include key details such as the date, time and description of events, the parties involved, any action taken, and any relevant test records. Where required, other details such as the names of the employees on shift and witness accounts are also to be recorded.

The records in an incident log, including video of the incident, shall be kept for a minimum of 60 calendar-days.

NOTE Certain jurisdictions can require a longer retention policy (e.g. one year).

7.4.3 Cybersecurity for research/testing laboratory

See 5.5 for requirements on cybersecurity for research/testing laboratory.

7.4.4 Administrative controls for research/testing laboratory

7.4.4.1 Applicable general requirements

Organizations testing cannabis, cannabis derivative, cannabis edible, and/or cannabis products should consider having policies on background checks for personnel.

Laboratories analysing cannabis and/or cannabis products should operate in accordance with the requirements of ISO/IEC 17025 to ensure the necessary competence.

Laboratories handling cannabis and/or cannabis products shall demonstrate compliance with the supplementary requirements for cannabis testing facilities specified below.

NOTE In some countries, laboratories handling cannabis and/or cannabis products samples can require a licence to do so.

Top management shall provide a documentation framework with specific operating procedures, policies, work instructions and other documentation governing good laboratory practice specific to cannabis and cannabis material analysis and the prevention of harm and/or unauthorized access, and/or integrity of, and/or establishing security policies for:

a) physical assets including, but not limited to, instrumentation, technology, controlled organisms/isolates, controlled chemical standard material and extraction solvents used for cannabis and cannabis product analysis;

b) personnel including external contractors, including but not limited to, physical safety, confidentiality or non-disclosure surety, qualifications, criminal record verifications, operational training;

c) cannabis and cannabis products received, stored, and disposed of;

d) records and information including, but not limited to, establishing appropriate storage durations and conditions, specific to cannabis and cannabis products, for multiple sources of records of information (training records, video surveillance footage, electronic access records, instrument data (hard copy and data files), chain of custody documentation, extraction records, etc).

7.4.4.2 Security operations procedural controls for research/testing laboratory

Operating procedures (OPs) are required to ensure reliable, reproducible, defensible, and auditable results for security operations. The OPs shall include, but are not limited to, the procedures and tracking forms for:

a) sample reception and sample accessioning (e.g. login and entry into a laboratory information management system (LIMS)), assignment of unique organizational identifier and labelling (barcoded preferable), chain of custody;

b) secure sample storage under appropriate conditions. (i.e. ambient, refrigerated or frozen);

c) maintaining a system to sign out keys to secure areas as well as a list of approved staff;

d) recording and reporting discrepancies at sample receipt;

e) recording and reporting discrepancies during the lifecycle of the sample within the facility;

f) establishing a threshold of material loss that exceeds the amount of loss expected from routine operations and represents reportable loss;

g) establishing a protocol to report theft;

h) security of specimens, aliquots, extracts and records;

i) internal tracking system or chain of custody form documenting the movement of specimens, aliquots or extracts to and from secure locations or to instruments;

j) ensuring that only validated methods are used for testing samples;

k) aliquoting samples by selecting a representative subsample to avoid contamination and carry-over;

l) disposal of samples within legally required timeframe such that they are rendered unusable;

m) disposal of samples documented with signatures and in the presence of a witness;

n) analytical methodology including pertinent literature references, theory and principals, accuracy, precision, analytical sensitivity, analytical specificity (presence analytical interferences), limit of detection (LOD), limit of quantification (LOQ), verification of the reportable range, safety precautions, critical control steps, and frequency and number of QA/QC standards;

o) selection, training, supervision, authorization, monitoring and determining the competence requirements of personnel with respect to security;

p) documenting planned deviations from established security protocols, near misses, , QC failures, equipment failures, etc.

Laboratories shall establish a procedure to document chain of custody to ensure cannabis and cannabis materials are always stored securely, are accessible only by staff, have traceable and auditable movement within a facility from receipt of material submissions to analysis, destruction, or transfer to another licensed laboratory.

A chain of custody for any cannabis and/or cannabis material samples shall be maintained digitally within a LIMS or manually with paperwork or as combination of the two formats from receipt and until destruction or transfer to another licensed laboratory.

The chain of custody shall identify and document:

a) all information required by the laws of the local jurisdiction for the shipment, delivery or transfer of cannabis and/or cannabis products to the laboratory, including but not limited to the following:

   1) name, address and contact information of the submitter;

   2) name, address and contact information of the receiving laboratory;

   3) licensing number of the submitter (if applicable);

   4) mass of material shipped;

   5) verification of product material received at the laboratory;

   6) condition of shipment packaging, internal and external upon receipt at the laboratory;

   7) signature and date of submitter relinquishing custody of material for shipment;

   8) signature and date of laboratory employee accepting custody of the received material;

b) all information specific to custody and handling the cannabis and/or cannabis product within the laboratory as required by the laws of the local jurisdiction, including but not limited to the:

   1) secure storage location(s);

   2) movement of cannabis and/or cannabis products within the facility when not in secure storage including time, date, location, and employee handling the cannabis and/or cannabis product sample(s);

   3) mass and unique identifier tracking for:

      i) time of retrieval from secure storage;

      ii) samples destroyed or delivered to long-term testing;

iii) before return to secure storage;

4) identity of equipment used to weigh, measure and analyse cannabis material;

5) destruction or transfer of cannabis material to another licensed laboratory (time, date, method, responsible employee, and witness signatures).

Cannabis research and/or test result reports should be consistent with the requirements outlined in IWA 37-3. Once reported, a final data package including the report, chain of custody paperwork, destruction paperwork, and raw data shall be filed and retained for two years.

7.4.4.3 Personnel qualifications, training and supervision for research/testing laboratory

Laboratory personnel with responsibilities that impact security shall be identified and documented, e.g. in an organizational chart, with built-in redundancy/alternate staff.

EXAMPLE Laboratory director, Designated alternate, Supervisory analyst, Laboratory testing analyst

Head of laboratory, Designated alternate head(s), Responsible person (must possess a university degree in science related to the work to be carried out, proof includes copy of degree, academic transcripts, resume/CV.)

All personnel of the laboratory shall have documented competency, including training and experience, for functions that have influence on security of cannabis operations.

7.5 Retail/dispensary

7.5.1 Physical controls for retail/dispensary

7.5.1.1 General

A retail site shall be located in a permanent building or structure and shall be enclosed by floor-to-ceiling walls and a permanent ceiling and floor.

Drive-through sales or curbside service may be considered in accordance with the SRA in Clause 4 and 5.2.

NOTE Drive-through sales or curbside service can be prohibited by the AHJ.

Signages of “No Trespassing” and “No Loitering” shall be posted around the retail site. The owner or management shall be responsible for reasonably controlling the conduct of persons on the retail site and shall immediately disperse loiterers.

Storage containers and non-operational vehicles shall not be allowed in the parking area of the site.

Where a retail site with a glass storefront is accessible from the street, methods to prevent vehicle intrusion shall be installed in accordance with the SRA in Clause 4 and 5.2.

7.5.1.2 Physical barriers

All perimeter doors secured against unauthorized access, including non-public doors locked to prevent unauthorized access, shall be designed and installed in conformance with the requirements for means for egress in IWA 37-1. Non-public doors shall remain locked at all times, except for emergencies and deliveries.

The customer entrance shall be constructed of commercial grade material sufficient to secure against unauthorized access.

All exterior doors shall be equipped with a 180° viewing device to screen persons before allowing entry.

7.5.1.3 Cannabis displays

Displays shall not permit self-service by patrons (including dispensing devices).

Cannabis and/or cannabis products displayed in a customer area shall be within a showcase that is locked and accessible only by authorized personnel.

NOTE 1 There is no requirement for cannabis accessories to be stored in a locked retail product case or a locked storage room.

Cannabis and/or cannabis products on display shall be in their original sealed package or in an approved container.

NOTE 2 Where cannabis or cannabis products are provided in smell jars, the original package is retained for inspection purposes until the smell jar contents are destroyed.

Commercial or industrial door frames with a three-step locking system shall be provided.

7.5.1.4 Storage for retail/dispensary

See 7.4.1.2 for requirements on storage for retail/dispensary unless the SRA for each stage indicates otherwise.

7.5.1.5 Site and floor plans

Site plans and floor plans for the retail site shall be completed and shall include details for:

a) secure lobby;

b) secure storage, safes vaults and/or secure storage areas;

c) secure area for transferring cannabis, cannabis products or cash to/ from vehicles.

7.5.2 Technical/electronic controls for retail/dispensary

7.5.2.1 Intrusion detection system for retail/dispensary

See 7.4.2.1 for requirements on intrusion detection systems for retail/dispensary unless the SRA for each stage indicates otherwise.

7.5.2.2 Video surveillance systems for retail/dispensary

See 7.4.2.2 for requirements on video surveillance systems for retail/dispensary unless the SRA for each stage indicates otherwise.

7.5.2.3 Lighting

Lighting shall be in accordance with the SRA in Clause 4 and 5.2.

Exterior lighting shall be white light using LED lamps with full cut-off fixtures to limit glare and light trespass. Colour temperature shall be between 2 700 K and 4 100 K with a colour rendering index of 80 or higher and a light loss factor of 0,95 or better. Light poles shall be no higher than 4,88 m (16 ft).

Entry drives, drive aisles, vehicle parking and bicycle parking shall be illuminated to a maintained minimum of 16 lx (1,5 fc) of parking area at a 6:1 average to minimum ratio.

Exterior walkways, alcoves and passageways shall be illuminated to a maintained minimum of 3,5 lx (0,33 fc) of surface area at a 6:1 average to minimum ratio.

Broken or damaged exterior lighting shall be repaired or replaced within 48 h of being noted.

Exterior lighting shall be shielded or otherwise designed to avoid spill-over illumination to adjacent streets and properties.

All mature landscaping shall be ground cover, 610 mm or less in height, and lower tree canopies of mature trees shall be above 1 800 mm. This increases natural surveillance and eliminates hiding areas within the landscape.

Tree canopies shall not interfere with or block lighting, so as to prevent the creation of shadows and areas of concealment. The landscaping plan shall allow for proper illumination and visibility regarding lighting and surveillance cameras through the maturity of trees and shrubs.

7.5.2.4 Monitoring and response

Critical areas defined as, but not limited to, storage areas, perimeters and critical infrastructure spaces shall be monitored by a signal receiving station at all times, subject to the operational requirements of the facility as identified in the SRA.

Response and dispatch shall be in accordance with CAN/ULC-S301, ANSI/UL 827 or ASTM D8218 (see Annex C).

If an event is detected, the holder of the license shall ensure that a document is retained for two years that contains the following information:

a) date and time of event;

b) individuals present during time of event;

c) measures taken in response to it and date and time they were taken;

d) electronic security system components and architecture that identified and reported the incident.

7.5.2.5 Records and documentation

The secure storage of records and documentation shall be as identified in the SRA.

7.5.2.6 Incident log

When an incident occurs at a retail/dispensary, the details shall be recorded in an incident log. All incidents that adversely affect patrons or staff, or that affect the operation of the retail/dispensary site, as well as 'near miss' incidents, shall be recorded in the log and be available to inspectors.

Examples of these incidents include:

a) refusing entry at the door to a potentially troublesome person or anyone who is causing a disturbance;

b) refusing entry of an intoxicated person;

c) removing an intoxicated person;

d) an injury or accident on the premises, including a physical altercation;

e) any incidents where emergency personnel were called (police, fire, or ambulance);

f) any illegal acts.

An incident report shall include key details such as the date, time and description of events, the parties involved, any action taken, and any relevant sales records. Where required, other details such as the names of the employees on shift and witness accounts are also to be recorded.

The records in an incident log, including video of the incident, shall be kept for a minimum of 60 calendar-days.

NOTE Certain jurisdictions can require a longer retention policy (e.g. one year).

7.5.3 Cybersecurity controls for retail/dispensary

See general requirements in 5.5 for requirements on cybersecurity for retail/dispensary.

7.5.4 Administrative controls for retail/dispensary

7.5.4.1 Applicable general requirements

Retail stores/dispensaries shall develop policies to address risk assessment, security management, continual improvement, administrative controls, traceability, operational control, emergency response and security recovery.

7.5.4.2 Procedural controls for retail/dispensary

Retail stores/dispensaries shall specify procedures to ensure cannabis and cannabis products are stored securely at all times and are accessible only by staff, from receipt of shipment to point of sale, destruction, or return to the supplier.

Retail stores/dispensaries shall develop policies and procedures specifying:

a) the responsibilities of personnel;

b) reception of secure packages of cannabis and cannabis products;

c) implementation of traceability documentation;

d) complaints and recalls;

e) incident reporting;

f) business continuity;

g) personnel training plan;

h) monitoring;

i) key performance indicators;

j) auditing.

7.5.4.3 Personnel qualifications, training and supervision for retail/dispensary

As part of the hiring process, criminal background checks should be obtained from all retail/dispensary personnel.

All retail/dispensary personnel shall act impartially, adhere to confidentiality, adhere to the retail/dispensary's requirements for quality and have documented competency. This includes, but is not limited to education, qualifications, training, technical knowledge, skills and experience.

Where local cannabis regulations require licensing for retail/dispensary personnel in supervisory roles, these shall be documented in an organizational chart with built in redundancy/alternative licensed staff as appropriate.

7.6 Transportation

7.6.1 Physical controls for transportation

7.6.1.1 Applicable general requirements

A security plan, based on a threat risk assessment, shall be in place and executed for shipment of cannabis or cannabis products. The security plan shall identify/address:

a) the assets to be protected;

b) the identified threats to those assets during the phases of the transportation process;

c) the specific transportation security measures to be deployed, commensurate with the value of the assets and level/types of threat, broken into three key areas:

   1) physical security measures;

   2) technical/electronic and cyber security measures;

   3) administrative security measures.

7.6.1.2 Specific requirements

7.6.1.2.1 General

Logistic providers shall provide security awareness training to all vehicle operators and be able to produce certification or training records upon request of contract agency. Security awareness shall consist of:

a) non-threat-based emergency procedural training for the type of material being transported. in countries where cannabis is deemed as controlled or restricted goods, proficiency in controlled or restricted goods handling is required;

b) threat-based emergency procedure training based on individual country threat risk analysis;

c) clear statements of measures, counter measures alternative servicing options in the event of a security risk;

d) current and effective SOPs in the event of security threats and/or incidents.

Logistic providers will not further outsource transportation services to additional third-party logistics (3PL) carriers without express approval of contracting agency. Logistic companies will authorize a contracting agency to conduct an audit of company policies and personnel.

NOTE A contracting agency can be the cannabis producer, a parent company, or another entity. The contracting agency can change throughout the shipment, depending on who is considered responsible for the package at different stages of transportation.

Where the security plan identifies high levels of risk, specialized logistics agencies can be required. These specialized agencies can include:

a) third-party escort or chase vehicles to supervise the primary logistic provider;

b) specialized or fortified vehicles;

c) private armed or police agencies to provide escorts and/or transportation.

7.6.1.2.2 Load security

With respect to sealing, packaging can vary depending on whether the shipment includes cannabis or cannabis product. Shipments shall be secured by appropriate means to ensure both that an accurate count is possible and that signs of tampering are visible to those along the supply chain.

In cases where plastic totes are used, unique seals (two seal per plastic totes with barcodes where appropriate) should be used to ensure both tracking and evidence of tampering.

Where the cannabis or cannabis products are stored in cardboard boxes, tamper evident security tape shall be used to secure the boxes. In cases where boxes are palletized, boxes should be faced in such a manner that all pieces can be counted externally without having to disassemble the pallet. The shipment shall be wrapped with shrink wrap.

7.6.1.2.3 Locks and seals

Dedicated transportation services including the delivery of sea containers, and unit load devices require the container to be securely sealed by high security padlocks, or similar device to prevent access, at each entry point as well as tamper evident uniquely identified seals. It is recommended that transportation service providers do not readily have access to the locking devices provided, unless there is a physical need for further inspection prior to delivery to final destination.

Less-Than-Truckload (LTL) loads, including final mile and work performed by couriers, are an exception. They are not required to have locks or seals installed.

Table 2 — Vehicle types for transportation services

Vehicle type	Description	Application
Cars	Personal type vehicles including taxi's, cars and pick-up trucks	Suitable for LTL personal consumption deliveries.
Cargo van	Cargo box attached to the cab and often interconnected. Often, multiple points of access and used by couriers and postal services.	Suitable for pickup and delivery of LTL personal consumption deliveries and/or retail operations including pharmaceutical outlets.
Straight truck	Also known as a cube truck/van or box truck, the cargo box shares a chassis with the power unit and cab.	Suitable for LTL or dedicated truck transportation of bulk products, transportation between facilities, distribution centres.
Dry van (enclosed) trailer	Fully enclosed trailers protecting freight from the elements and offering a level of "container" integrity as often only the rear doors can be accessed without visual signs of tampering	Suitable for LTL or dedicated truck transportation of bulk products, transportation between facilities, distribution centres.
Conestoga/current trailer/straight truck	Trailers or cargo boxes with a rolling tarp system on either side of the container.	Not suitable for the transportation of cannabis or cannabis product(s).

Vehicles shall be equipped with a means of two-way communication that is effective for the transit route. If travelling extends beyond cellular coverage range, satellite phone or truck-based communication systems are required in the event of an emergency.

7.6.1.2.4 Vehicle loading/unloading

The transportation entity doesn't take responsibility until cannabis or cannabis product(s) are loaded and doors are closed/locked and/or sealed.

The transportation entity releases responsibility once rear doors are opened, and the cannabis or cannabis product starts being removed at the final destination.

Prior to cannabis or cannabis product pick up or drop-off at delivery or pick-up locations, steps shall be taken by the transporter to ascertain all of the relevant security protocols to be followed.