This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.

Designation: D8320 – 21

Standard Practice for Implementing an Information Security Program in a Cannabis Operation[1]

This standard is issued under the fixed designation D8320; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice covers recommendations for implementing an information security program to protect businesses operating in the regulated cannabis industry. An information security program is part of an overall security program that each business should implement.

1.2 This practice applies to any legal business entity that handles cannabis products, including cultivation, processing, manufacturing, transportation, warehousing, lab testing, distribution, retail, home delivery, and waste. This practice will include protections for analog (paper) and digital information assets.

1.3 Actual implementation will vary depending on organizational size and type, information asset types, sensitivity and volume of assets, risk tolerance and resource constraints of the organization, and mandates particular to the organization.

1.4 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.5 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

D8205 Guide for Video Surveillance System
D8217 Guide for Access Control System
D8218 Guide for Intrusion Detection System (IDS)
F3286 Guide for Cybersecurity and Cyberattack Mitigation

3. Terminology

3.1 *Definitions of Terms Specific to This Standard:*

3.1.1 *access control, n*—restricting access to an asset.

3.1.2 *asset, n*—generally refers to anything of value to a business such as an employee, facility, computer equipment, computer system, intellectual property, and other information assets.

3.1.3 *availability, n*—ability of authorized users to access analog or electronic information assets on demand.

3.1.4 *boundary defense, n*—controls the flow of traffic through network borders and polices content by looking for evidence of unauthorized access and attacks. Established multilayered boundary defenses typically include controls that protect perimeter networks, firewalls, and other network tools.

3.1.5 *cannabis products, n*—refers to cannabis seeds, immature plants, flower, cannabis concentrates regardless of form or extraction method and cannabis infused products, such as edibles, etc.

3.1.6 *chain of custody, n*—refers to the process of documenting each person who had access and control of a particular asset from the time of creation through any changes of hands.

3.1.7 *classification level, n*—refers to defined sensitivity levels of information. People are granted access to information of certain classification levels in accordance with their duties. Governments use labels such as top secret, secret, confidential, and unclassified (see role-based access).

3.1.8 *computer system, n*—hardware, software, network, transmission, storage.

3.1.9 *confidential, n*—refers to the legally protected privacy of an information asset.

3.1.10 *controls, n*—refers to physical, technological, and human (end user) measures and countermeasures intended to prevent, detect, or otherwise mitigate system vulnerabilities and potential threats of unauthorized access, misuse, damage, disruption or losses to information system infrastructure or information assets, whether unintentional or by malicious

[1] This practice is under the jurisdiction of ASTM Committee D37 on Cannabis and is the direct responsibility of Subcommittee D37.05 on Security and Transportation.

Current edition approved July 1, 2021. Published August 2021. DOI: 10.1520/D8320-21.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

attack. Controls include threat response and recovery protocols. Examples of controls: limiting access to locations and records, antivirus software, policy and procedures, etc.

3.1.11 *cybersecurity, n*—refers to protections from unauthorized access or malicious attacks on information system architecture, infrastructure or electronic information assets.

3.1.12 *data, n*—facts and statistics collected together for reference or analysis.

3.1.12.1 *Discussion*—By many definitions information is data that has been analyzed and organized into meaningful thoughts, and data is simply a collection of raw facts and statistics. In this practice the use of the terms data and information are interchangeable.

3.1.13 *data breach, n*—refers to electronic information assets that are improperly accessed, used, lost, stolen or released, whether unintentional or malicious.

3.1.13.1 *Discussion*—This term may refer to situations where there is no confirmation the information was accessed, misused, or released (as with a lost or stolen laptop).

3.1.14 *data integrity, n*—refers to protection of the correctness and reliability of data and information retrieval.

3.1.15 *electronic asset, n*—refers to all information assets that are not (only) paper records.

3.1.16 *encryption, n*—a method of secure communication transmission that typically uses symmetric key algorithm, which is a message secured with a key and algorithm and transmitted to the receiver who uses a similar key and algorithm to decrypt and view the message.

3.1.17 *General Data Protection Regulation (GDRP), n*—mandate of privacy data that protects and restricts transfer of data into or out of the European Union.

3.1.18 *Health Insurance Portability and Accountability Act of 1996 (HIPAA), n*—a United States statute to protect health information privacy and security.

3.1.19 *incident, n*—an event of unauthorized access, misuse, damage, disruption or loss of information assets, whether unintentional or by malicious attack and whether electronic or analog.

3.1.20 *incident response, n*—an organized approach to addressing and managing a security breach or cyberattack, which is intended to limit damage and recover data and reliable system operations.

3.1.21 *information asset, n*—includes computer system infrastructure and architecture, paper (analog) and digital data, files, and records.

3.1.22 *information system infrastructure and architecture, n*—refers to equipment, hardware (servers, PC's, routers), operating systems, software (including office, seed to sale, point of sale), networks, connections, and controls, etc. Note that these are also "information assets" for the purpose of this practice.

3.1.23 *information security (IS), n*—refers to the protection of information system assets, which includes infrastructure, architecture, paper (analog) and digital data, files, and records. Information security includes cybersecurity.

3.1.24 *malware, n*—any unauthorized program or file that is potentially harmful to a computer or computer system such as a virus, worm, or spyware.

3.1.25 *organizational readiness, n*—an organization's readiness for change.

3.1.26 *penetration test, n*—simulated cyber-attack against a computer system to determine whether existing protections, such as web application firewall (WAF) is adequate and works as intended.

3.1.27 *phishing, n*—fraudulent attempt to obtain sensitive information such as usernames, passwords, or financial details by disguising oneself as a trustworthy entity in an electronic communication with the intent of illicit use.

3.1.28 *protected health information (PHI), n*—phrase that refers to U.S. HIPAA statutory provisions related to the health-related information of a specific person.

3.1.29 *role-based access, n*—a technique of granting the minimum amount of access to information assets necessary for a person to complete job duties.

3.1.30 *quantitative risk analysis, n*—an analysis of vulnerabilities and threats to information assets that includes cost-benefits of implementing a variety of physical, technological, and human controls to minimize risk.

3.1.31 *sensitive information, n*—any information asset that is restricted from certain staff, the public, or is otherwise confidential.

3.1.32 *short message service (SMS), n*—method of communication that sends text between cell phones, or from a personal computer or handheld computer to a cell phone with a maximum size of the text messages.

3.1.33 *uninterruptible power supply, n*—ensures continuous operation by using a surge protector with a built-in backup battery.

3.1.34 *vulnerability, n*—an existing weakness that may be exposed to a threat.

4. Summary of Practice

4.1 This practice provides the essential elements to establish and manage an information security program for cannabis businesses. It includes guidance on establishing a work group, identifying information assets and potential threats, analyzing levels and types of risk to those assets, selecting appropriate controls to mitigate vulnerabilities, and monitoring implementation of the program for continuous improvement. This practice also provides practical information on implementing physical, technological, and human controls such as active prevention, detection and response techniques, policy and procedures, implementation guidance (training, communications), continuous improvement strategies, and resources to educate information security team members as needed and for further program development.

4.2 The practice also presents considerations specific to the cannabis industry and guidance about types of mandates that may apply (in addition to those of the authority having jurisdiction).

4.3 The primary goals of an information security program are to prevent equipment and data from being lost, corrupted, or stolen; to protect customer, employee, and business records; and to ensure uninterrupted, compliant, and efficient business practices.

4.4 Businesses should establish information security programs with controls that protect information assets (including architecture, infrastructure, records, etc.) from unintentional and malicious unauthorized access, damage, and exposure. Information security program controls can effectively measure and maintain an acceptable level of risk when companies use a team approach to assess and analyze priorities and develop controls and implementation plans. Once controls are in place, organizations should continue the team to audit practices and controls at regular intervals and when incidents occur.

4.5 The major activities to implement an information security program are:

4.5.1 Establish objectives and responsibilities;

4.5.2 Form an information security team;

4.5.3 Provide orientation and education for information security team members as needed;

4.5.4 Conduct an assessment to identify information assets, potential threats to those assets, and the need for controls;

4.5.5 Analyze risks, costs and feasibility of physical, technological, and human controls to mitigate threats (prevention, detection, respond, or recovery);

4.5.6 Select, plan and implement controls; and

4.5.7 Establish and monitor continuous improvement strategies.

5. Significance and Use

5.1 Information security programs and controls should be implemented by all cannabis businesses to protect information assets, which include information system infrastructure, architecture, analog (paper) and electronic data, files and records.

5.2 The cannabis industry is in transition from an unregulated industry to a regulated industry, which involves substantial investment. Implementing an information security program helps organizations manage information security threats and protect the organization, employees, customers, vendors and other business partners from unauthorized access, misuse of information, crime, and costly exposure or loss.

5.3 Cannabis customers and business partners place higher value on keeping information secure and have heightened concerns about information security due to the legal complexities and stigma around the industry.

5.4 Information systems have multiple access points that present opportunities for vulnerabilities, such as user accounts, removable storage devices, internet connections, malicious malware and other attacks, scams, and poorly guided access controls.

5.5 This practice intends to help organizations of all types and sizes find an acceptable balance of risks and costs of threat mitigation, recovery and remediation.

5.6 When planning an information security program, a broad range of input from all departments (or functional areas), levels of staff, and areas of expertise (information technology, legal, compliance, human resources, tax/accounting) is ideal for identifying the highest information security risks to the organization and can make implementation go more smoothly.

5.7 Information assets must be protected throughout the entire lifecycle (creation, transmission, review, storage, and destruction).

5.8 *Users of This Practice:*

5.8.1 This practice is written for cannabis business operations to be used by:

5.8.1.1 Business owners and management to develop security controls to prevent, detect, and mitigate vulnerabilities and risk, enhance business planning, and respond to and recover from incidents;

5.8.1.2 Consultants to provide guidance about information security assessments, analysis, controls and information audits;

5.8.1.3 Authorities having jurisdiction to inspect the adequacy of information security; and

5.8.1.4 Training organizations and certification bodies to train or certify individuals on the body of knowledge related to information security in the cannabis industry.

5.9 *Iterative Implementation Approach:*

5.9.1 Implementing an information security program is not a one-time sequence of tasks. Once an Information security program manager is assigned, team participants are educated, risk assessments and analyses are conducted, iterative cycles of implementing controls can begin. Initial plans will focus on higher priority assets and risks and easy to implement controls. Teams will monitor implementation, make adjustments, and repeat as needed.

5.9.2 An information security audit should be conducted at least once a year.

5.9.2.1 Audits can be assigned to internal or external auditors, depending on need for objectivity, independent review, or in accordance with legal mandates.

5.10 *Unique Business Entities:*

5.10.1 This practice is not a one-size-fits-all model to manage cybersecurity risk. Since each operation's risks, systems, procedures, digital usage, size, and scale are unique, the use of this practice requires ongoing engagement and continuous evaluation of prevention and countermeasures to stay abreast of ever-changing threats. This practice cannot be used by itself as an information security policy, procedure, or program; each entity must develop and monitor its own information security practice. This practice will guide the planning, assessment, implementation, audit, and improvement of an ongoing information security program.

5.11 *Compliance and Legal Considerations:*

5.11.1 Cannabis business mandates are complex and unique to each jurisdiction. Cannabis businesses must consult with legal, compliance, accounting, security, human resources and information technology professionals for guidance about protecting and sharing records.

5.11.2 Multiple levels of jurisdiction can apply (local, state/province, country) and mandates can conflict rendering them unclear. For example, legal experts do not agree on whether U.S. HIPAA laws apply to cannabis businesses that sell to medical patients.

5.11.3 Since remediation efforts are costly, all cannabis business entities must maintain an active information security program to prevent and detect threats with plans to respond and recover from incidents.

5.11.4 Business entities should not rely solely on purchased software vendors for advice, because none can manage all the information security and related compliance, legal and business risks a cannabis business will face.

5.11.5 Businesses should ensure that intellectual property and other business records, operational records, and customer records are considered and protected in consultation with legal and compliance professionals.

5.12 *Insurance, Contracts, and Tax Considerations:*

5.12.1 Cannabis business entities should review insurance policies and contracts to ensure adequate protections.

5.12.2 Businesses should consider including elements such as nondisclosure, privacy and confidentiality, data breach protocols, testing and maintenance requirements, scope of work and functional requirements, using proprietary software, uptime, and clear measures of success in contracts.

5.12.3 Cannabis businesses should ensure finance, budget, and tax professionals are consulted about information security plans to ensure team activities and controls are clearly written and implemented in alignment with those goals.

6. Information Security Program Implementation

6.1 Sections 6 – 15 will establish the foundation of the practice and essential elements for implementing an information security program. Businesses will establish a work group, identify information assets and potential threats, analyze levels and types of risk to information assets, select appropriate controls to mitigate vulnerabilities and threats, and will establish protocols for incident response and recovery and ways to monitor implementation for continuous improvement. The practice will include references to Annex A1 – Annex A3, which are required as part of the practice, and to Appendix X1 – Appendix X6, which are optional, but provide education on risks and controls and recommended policy and procedure elements.

7. Establish the Information Security Program Team (Workgroup)

7.1 Robust information security (IS) programs require participation, understanding, and buy-in from top leadership. Business owners and senior managers should consider organizational readiness and make efforts to establish a culture that actively protects information assets, including architecture, infrastructure, paper and digital data, files, and records.

7.1.1 *Identify Leadership*—Senior management will identify a chief security officer, chief information officer, director of security, or project manager who is responsible for managing the information security program and accountable for all team activities. This role will be referred to as the information manager (IM) in this practice.

7.1.1.1 The IM should report to the highest executive levels and be part of multiple executive planning teams for the organization and not only for the IS program.

7.1.1.2 The IM must work with chains of command to establish reporting and approval processes for the program.

7.1.2 *Identify Team Members*—The IM shall identify team members to participate in the work group.

7.1.2.1 Team members should include representatives from different areas of expertise (security, IT, compliance, operations, HR) and should represent all levels of staff and all functional areas of the business to establish the most successful controls.

7.1.3 *Identify Subject Matter Experts*—At a minimum, teams should invite legal, compliance, tax, and IT specialists to participate after the assessment is completed to ensure the highest risks are addressed. (See Section 9.)

7.1.4 *Initial Team Objectives*—The IS Team will:

7.1.4.1 Conduct assessments to identify information assets that should be protected and vulnerabilities and threats that need controls;

7.1.4.2 Conduct qualitative and quantitative analysis; and

7.1.4.3 Select, design, and implement physical, technological, and human (end user) controls for information asset threat prevention, detection, incident response and recovery.

7.1.5 *Initial Meeting Preparation*—Team leaders will review the entire practice and references, will prepare meeting materials, and distribute resources to educate team participants about information security assets, threats, vulnerabilities, and controls as needed. (See Guides D8205, D8217, D8218, and F3286 and Appendix X1 – Appendix X6 for information security education and recommended policy and procedures.)

7.1.6 The IM will ensure adequate documentation of major decisions made in each phase of the program so that knowledge is formally retained when there are staff changes.

8. Educate the Team

8.1 Implementing an information security program requires knowledge of information security risks and controls that can mitigate those risks. Team members and participants will review Annex A1 – Annex A3 to become familiarized with the tools of the practice and may review Appendix X1 – Appendix X6 for an educational overview of components.

8.1.1 Annex A1 – Annex A3 are tools the team will use for assessment, analysis, and planning.

8.1.1.1 Annex A1: Information Security Self-Assessment Question List

8.1.1.2 Annex A2: Information Asset, Threat, and Control Assessment Worksheet

8.1.1.3 Annex A3: Control Matrix

8.1.2 Appendix X1 – Appendix X6 provides an educational overview on information assets, cybersecurity threats, and different types of controls. Appendix X6 also includes specific policy and procedure recommendations.

8.1.2.1 Appendix X1: Information Security Education

8.1.2.2 Appendix X2: Information Asset Definitions

8.1.2.3 Appendix X3: Vulnerabilities and Threats

8.1.2.4 Appendix X4: Physical (Environmental) Controls

8.1.2.5 Appendix X5: Technological Controls

8.1.2.6 Appendix X6: Human Factor Controls and Recommendations for Policy and Procedures

9. Conduct Assessment: Identify and Prioritize Information Assets and Threats to Control

9.1 An assessment will be conducted to identify and prioritize information assets, vulnerabilities, and threats to determine whether additional controls should be implemented to lower business risks. Annexes must be customized to meet the needs of the business.

9.1.1 First, the team will conduct a self-assessment, using the information security self-assessment questions provided in Annex A1. Answers to these questions will help teams recognize current information assets, threats, and types of controls that could reduce risk to the business.

9.1.2 Next, the team will complete the information asset, threat, and control assessment worksheet provided in Annex A2 to conduct an inventory of information assets, rank priorities, and identify whether (new) controls are needed.

9.1.2.1 To complete an inventory of information assets, teams should list components of information system architecture and infrastructure, and all types of paper and digital files and records. This task should be broken up so that people with direct experience with the assets assist with the inventory.

9.1.2.2 Teams should review organizational structure and work activities for flows of information throughout the lifecycle. Every department and work location should be examined for reports, records, and other files created or maintained by staff.

9.1.2.3 Teams should have knowledge of, or seek out informal practices and review formal policy and procedures [or standard operating procedures (SOPs)], forms, checklists, and job aids; training materials, memos and other directives, and even reminders tacked up in work areas to generate a comprehensive list of existing information assets and controls.

9.1.2.4 Teams should spend more time detailing sensitive information assets and considering threats and controls for those at higher risk levels. Higher risk information assets are typically located around essential and proprietary business functions and records, employee, customer and vendor records, any activities involving handling or moving cannabis products, cash or cash equivalents and any mandates.

9.1.3 Team should address vulnerabilities and threats for each inventory item by reviewing the adequacy of any existing controls to identify gaps.

9.1.4 Information managers may restrict items from the assessment upon approval of the security manager or designee. (These discussions should be documented and retained to verify that more than one person was involved in the decision to restrict information from the team, as established as part of 7.1.1.1.)

10. Gain Consensus on Information Asset and Threat Priorities

10.1 The team will meet to achieve consensus on information asset and threat priorities and whether (new) controls are needed, using the information asset, threat, and control assessment worksheet (Annex A2) and control matrix (Annex A3).

10.2 This section should be completed in conjunction with Section 11.

11. Explore Controls (Physical, Technological, and Human Factor)

11.1 To explore control options, teams will review the information security self-assessment questions (Annex A1); the information asset, threat, and control assessment worksheet (Annex A2); the control matrix (Annex A3); and should review the information security education appendices on information assets, threats, controls, and policy and procedure recommendations (Appendix X1 – Appendix X6).

11.1.1 These documents will help teams identify information assets and types of controls to reduce risk along a continuum of prevention, detection, response, and recovery.

11.1.2 The control matrix (Annex A3) can be used to assist teams with more complex threats, or as a reminder to consider a broad range of control categories (physical, technological, and human factor) on a control continuum (prevent, detect, respond, and recover) during discussions.

12. Conduct Qualitative and Quantitative Risk Analysis

12.1 To conduct analysis, teams will balance the following five factors to analyze risks, needs, and feasibility of implementing identified controls:

12.1.1 Information asset priorities (based on sensitivity);

12.1.2 Vulnerability and threat priorities based on:

12.1.2.1 Likelihood that identified threats will occur;

12.1.2.2 Potential damage or loss of information assets if the threat occurs;

12.1.2.3 Potential impacts on the organization if the threat occurs (lawsuits, loss of sales, etc.);

12.1.3 Physical, technological, and human factor controls that can mitigate risks;

12.1.3.1 Cost estimates for implementing various controls (tangible and intangible); and

12.1.3.2 Organizational values, mandates, resource constraints, and tolerance for risk.

12.2 To get started, teams should select a high priority asset or high priority threat, specific controls from any of the three categories (physical, technological, human factor) that can mitigate risk, and calculate cost-benefit estimates for controls across the continuum (prevention, detection, response and recovery).

12.2.1 Cost estimates should include tangible and intangible elements tailored for the organization's business type, level of IT expertise, mandates, resources and constraints, and organizational tolerance for risk. This step is essential to make decisions about which controls to put into place.

12.2.1.1 Cost estimate considerations include those related to: staff time to design, implement, and monitor prevention, detection, response and recovery controls; staff training; purchasing equipment, hardware, software, electricity, back-ups, and supplies; hiring security, compliance, legal, tax, and IT staff or consultants; time to complete protocols for security incidents; costs involved for potential sanctions and lawsuits, and losing licenses temporarily or permanently; staff time in court or preparing for lawsuits; losing public trust and goodwill, etc. Intangible aspects of risk can be over- or under-estimated, though there are many acceptable methods for estimating these kinds of costs.

12.3 Teams will repeat 12.2 until all high priority assets and threats are addressed.

12.4 At this point, teams should have completed a thorough business process analysis to identify and prioritize assets and threats, explored controls with cost-benefit and risk analysis, consulted with a variety of subject matter experts from operational and support departments (security, compliance, IT, HR, PR, accounting, legal) and gained approval to move forward with final control selections and implementation planning.

13. Select and Design Controls

13.1 Information security controls can include physical controls such as restricting access to the server and surveillance rooms, technological controls such as installing reputable antivirus software, and human controls, such as implementing policy and procedures and training staff not to open executable files from email links.

13.2 *Select Controls*—Teams should initially select controls that mitigate the highest priority information assets and threats, or controls that are cost effective to implement and serve to mitigate many risks. Information security teams should continue to use the control matrix in Annex A3 and information security education appendices (Appendix X1 – Appendix X6) to consider physical, technological, and human (end user) controls for prevention, detection, response and recovery from specific disasters and threats.

13.3 *Design Controls*—Upon approval, team members will be assigned to design and finalize controls, such as developing protocols or metrics for intrusion detection, penetration and recovery testing, writing policy and procedures, training materials, or setting functional requirements for developers.

13.3.1 Design tasks will be completed internally, by contracted vendors, or by outside (hired) auditors or consultants and should include measurable criteria for monitoring, testing and maintenance to evaluate effectiveness.

13.4 Team members should review references and attachments throughout this process to locate additional resources for exploring and designing internal and external controls.

14. Develop Implementation Plan: Communication and Training

14.1 Implementation plans must include strategies for communicating new, updated, and archived policy and procedures and evaluating the need for formal or informal staff training. Staff must be made aware of their role and duties related to all controls in any case. Orientation training, for example, should routinely cover topics such as acceptable use, user accounts, social media, and confidentiality. High risk controls may require signatures from staff indicating they have read and understand the policy and have had the opportunity to ask questions about items that are not clear (see Appendix X5), and lower risk controls may only require discussion with the supervisor at the next staff meeting.

14.2 *Communications:*

14.2.1 Staff should be notified about any new or updated documents in writing (by means of email or paper) and supervisors should review any newly approved documents with staff.

14.2.1.1 *Maintain Policy Library*—Policy and procedure documents and employee handbooks (currently in effect) should be readily available to staff.

14.2.1.2 *Maintain Policy Archive*—Business entities should maintain a policy library of all documents in effect and should maintain all archived or superseded (approved) versions of policy and procedures, forms, job aids, employee handbooks, etc., so they can be retrieved for verification of what was in effect on the date of any incident. Businesses should retain copies of email notifications and other communications that accompany issuance of any policy and procedure updates for the archive. Businesses should generally retain these documents indefinitely, in accordance with a record retention plan.

14.2.1.3 When deemed necessary for high risk controls, written acknowledgements of receipt and understanding of a new or updated policy or procedure should be retained in individual training logs as described below.

14.3 *Training:*

14.3.1 *Frequency*—Training on information security and related policy and procedures or Employee Handbook items must be held for all staff when joining the organization, when new or revised policy and procedures are issued, and at other times when needed, such as after an incident or near-incident. Highest risk controls may require annual refresher training. New roles and job positions may require additional training when jobs change.

14.3.2 Training logs should be kept by employee, by date, and by topic for verification and retrieval. Logs should contain dates, training topics covered, instructor and participant names, and copies of training materials provided to staff. Copies of training materials should be routinely stored with sign in sheets to verify attendance for each formal training session, and supervisors should document informal training and policy discussions with staff. Training logs are often reviewed in the event of any incident, and businesses should be prepared to be able to verify who attended which training and when, and what was covered. Businesses should generally retain these logs indefinitely, in accordance with record retention plans.

15. Monitoring and Continuous Improvement

15.1 Teams should establish measurable ways to monitor the effectiveness and ongoing necessity of all controls.

15.1.1 *Monitor Internal Controls*—The information security team should meet within 48 hours of any information security incident, and at least annually to review testing and monitoring results, policy and procedures, employee handbooks, and any concerns to determine whether controls should be updated, archived, or if new ones are needed.

15.1.2 *Monitor External Controls*—Businesses should carefully review contracts and agreements to ensure controls that address information security are included and updated for customers, vendors, volunteers, etc.

16. Keywords

16.1 access control; analog; analysis; assessment; cannabis; continuous improvement; controls; computer; confidentiality; cyber security; cybersecurity; data; detection; digital; electronic; files; hardware; incident; information; information security; monitoring; notification; prevention; privacy; power supply; procedures; records; recovery; response; risk; security; software; testing; threats; two-factor; uninterruptible

ANNEXES

(Mandatory Information)

A1. INFORMATION SECURITY SELF-ASSESSMENT

A1.1 When considering questions, pull relevant reports, SOPs, contracts, etc., for review.

A1.2 Organizational Culture Questions

A1.2.1 Do you have a written strategic plan or business continuity plan that includes language about information security?

A1.2.2 Are information managers included in executive-level meetings that are not primarily about IT matters?

A1.2.3 Do you believe your organization is ready to make changes related to information security? Leadership? Line staff?

A1.3 Physical (Environmental) Security Controls

A1.3.1 Where are data centers/tech areas located (server room, surveillance room, etc.)?

A1.3.2 Is access to equipment limited to authorized employees? Is this access logged? Is it audited or spot checked? Is more than one person in control of the info? Who is responsible for maintenance and calibration schedule?

A1.3.3 Where are paper (analog) records stored? Are there keys to file cabinets? Does anyone actually lock desks or file cabinets? Who has spare keys?

A1.3.4 Do you have a map/index of information assets (architecture, infrastructure, files/records) and organized maintenance/calibration schedules?

A1.3.5 Describe backup power sources for all servers, computers, printers, cameras, decks, and other equipment (cash registers, extraction equipment, etc.) How often are these backup sources tested?

A1.3.6 Describe the fire detection/suppression systems for facility/facilities.

A1.4 Technological (Network/Application) Security Controls

A1.4.1 Do you have custom software? Do you use seed-to-sale or point-of-sale software from an outside vendor?

A1.4.2 Do you contract for or outsource any IT or IS work (server hosting, website hosting, email marketing management, offsite surveillance)?

A1.4.3 Do contracts include monitoring elements or other metrics related to information security?

A1.4.4 How do you protect intellectual property like product design, processes, genetics, patents, copyrights, etc.

A1.4.5 Are any controls built into contracts for contractors, volunteers, or vendors (off site surveillance, IT, software interfaces, social media fair use, etc.)? If so:

A1.4.5.1 For whom? Describe controls and intersections with the business entity.

A1.4.5.2 Do you know how information security is monitored at any contracted vendor or outsourced company? Is it required in your contracts with them?

A1.4.5.3 Do vendors have access to any files? Monitoring and recording?

A1.4.5.4 Do vendor contracts contain data breach, uptime, fair use, and confidentiality requirements, etc.?

A1.4.6 Do you have a computer network where multiple employees can share the same folders or files?

A1.4.7 Do you monitor access to data, files, and passwords (reviewing logs, user account access controls, periodic review of each employee's access) to see if access is minimum necessary to complete job duties?

A1.4.8 Do you have firewalls in place on all external network connections?

A1.4.9 Do you have an intrusion detection system (IDS) or intrusion prevention system (IPS) in place? If so, is the IDS/IPS system managed in-house or outsourced? Have you had any critical security events?

A1.4.10 Do you have periodic penetration tests performed on your network? Internal or contracted out? How often are these tests performed? What were the results of the last test?

A1.4.11 Describe the antivirus and malware protections you have in place.

A1.4.12 Do you have a wireless network? Have you conducted a scan for rogue wireless access points?

A1.4.13 Are the servers and hardware loaded with security service packs/patches? What is the technology, is it the latest version?

A1.4.14 Is staff permitted to use personal devices or flash drives to access the network?

A1.4.15 Do you test and evaluate hardware (replacement schedule, upgrades)?

A1.4.16 Do you test and evaluate software (static, dynamic, interfaces, misuse case testing)?

A1.4.17 Do you monitor for network and system misconfigurations and security flaws (reviewing code, network, and web penetration testing, etc.)? If so, how? Is it adequate?

A1.4.18 Do you verify backups (functionality)?

A1.4.19 Do you review the effectiveness and technological efficiencies of any existing controls?

A1.4.20 Do you perform any (other) systematic tracking and monitoring or audits?

A1.4.21 Have you had any previous tests or plans for identified risks and vulnerabilities? If so, are there any established (performance) metrics? What were the results?

A1.4.22 Have you had any history of IS incidents, problems, etc.?

A1.4.23 What does staff complain about regarding information assets (all levels of staff)?

A1.5 Technological (Data/Application) Security Controls

A1.5.1 Do you assign access to data/files/records based on sensitivity? (That is, public, company restricted, confidentiality mandates, etc?.) Please describe levels and procedures for assigning access.

A1.5.2 Do you have a process for handling customer confidential information with respect to storing it, transporting it, and disposing of it? Do you have data breach protocols? Please describe processes, legal mandates, and any special protections for certain medical conditions, etc. (like HIV, child records, behavioral health, etc.).

A1.5.3 How often is your data backed up? Where do you store the backup media? Is the media encrypted?

A1.5.4 Do you use a third-party company to manage your backup media? If so, who and where is it stored? Recordings? Cloud storage?

A1.5.5 Do you have a policy for destroying backup media?

A1.5.6 Describe maintenance contract, protocols, and schedule.

A1.5.7 What methods are used to transfer data or to share records between the business entity and (*1*) employees working off site, (*2*) authorities having jurisdiction, (*3*) contracted vendors, (*4*) law enforcement, and (*5*) authorized third parties (patient's physician, courts, law suits, etc.)?

A1.5.8 What are your encryption procedures for handling customer confidential data? Are records redacted?

A1.5.9 How do you protect this data while it is being transferred?

A1.5.10 Is customer data encrypted while at rest?

A1.5.11 Is the system/service accessible by means of the internet?

A1.5.12 Do end users access your system/service by means of browsers, mobile applications, or thick clients?

A1.5.13 Do contracts include monitoring elements?

A1.5.14 Are any other controls built into contracts with contractors, volunteers, or vendors (off-site surveillance, IT, software interfaces, etc.)?

A1.6 Human Factor (User Access) Controls

A1.6.1 Do you have a documented information security policy and procedures that cover social media, user accounts, and use of devices (see Annex A1 and Appendix X2)?

A1.6.2 How often do the employees acknowledge they have read and understand information security policy/SOPs?

A1.6.3 Who has overall responsibility for IT security within your company? Do any staff hold any IT or IS certifications?

A1.6.4 Is access to information assets granted on a need to know basis (facilities, hardware/software, network, files/data/records)?

A1.6.5 Do you grant access to information on your network based on job functions and roles? Describe this process.

A1.6.6 Are customer/user/administrator passwords encrypted when sent over electronic networks or stored in memory? Describe this process.

A1.6.7 Describe your password policy. (That is, password aging and ability to reuse old ones, password complexity?)

A1.6.8 Do you support multi-factor authentication (MFA)?

A1.6.9 Does the system lock the user account after a certain number of failed attempts? Other lock out controls?

A1.6.10 Where is the password table stored and encrypted?

A1.6.11 Are the passwords masked?

A1.6.12 Are there pop-up warnings? (For example, you are about to view….; are you sure you want to delete....)

A1.7 Human Factor (Employee) Controls

A1.7.1 Do you perform background checks on applicants before they are hired?

A1.7.2 Do you require new hires to sign non-disclosure and confidentiality agreements related to customer confidential data, other records?

A1.7.3 Do your employees participate in information security training? Describe topics, frequency.

A1.7.4 Is there a process in place for when employees leave or are terminated, what is the process for terminating their computer/network access?

A1.7.5 Do you have policy and procedures related to information security?

A1.8 Policy and Procedure Checklist (also see Appendix X5)

A1.8.1 *Employee Handbook*—Nondisclosure, confidentiality, social media, access to facilities, networks, files, using only your own key card, log-in to enter information, etc.

A1.8.2 *Acceptable Use*—Use of personal and company-issued devices, network, internet.

A1.8.3 *Access Control Systems*—Setting, testing, auditing access controls (physical and electronic) logs, keys, visitor, shipping and receiving, transportation, waste protocols (see Guide D8217).

A1.8.4 Video surveillance system (see Guide D8205).

A1.8.5 Intrusion detection system (see Guide D8218).

A1.8.6 *Managing User Accounts*—Passwords, setting role-based access to locations, networks, programs, files, only using your own account to enter information, etc.

A1.8.7 Onboarding and termination protocols.

A1.8.8 Incident, emergency, and disaster response, notifications, investigation, and reporting.

A1.8.9 Releasing information and sharing records (media, subpoenas, clients, etc.).

A1.8.10 Privacy and confidentiality of records.

A1.8.11 Record storage, record retention schedules, destruction.

A1.8.12 *Operations*—Data entry, file management, all movements of cannabis products, cash and cash equivalents.

A1.8.13 Consultant, vendor, and volunteer agreements and access.

A1.8.14 *(If you do research):* informed consent forms, institutional review board (IRB) protocols.

A1.9 External Controls: Software Development (for custom software or software vendor contracts)

A1.9.1 Does software testing include: information security code review? Vulnerability testing?

A1.9.2 Have you ever had an independent test (vulnerability assessment) of your software performed? If so, what were the results?

A1.9.3 Do you maintain an application test or development environment separate from the production system?

A1.9.4 Do software developers have the ability to access or change the production environment?

A1.10 Information Security Incident Management

A1.10.1 Do you have any Incident response plans or protocols in place? Describe data breach (records, customer) and unauthorized exposure (internal, external) protocols.

A1.10.2 Have you had any IS incidents? Please explain.

A1.11 Business Continuity Management

A1.11.1 Do you have a written business continuity plan that covers loss of data, hardware failure, and loss of use of premises, due to attack, emergency, and natural disaster?

A1.11.2 Have you contracted with a disaster recovery service provider for alternate facilities in the event of a disaster? Or, do you have your own alternate facility for use in a disaster?

A1.11.3 How often do you test your disaster recovery plan? When was the last test performed and what were the results?

A1.11.4 Do you maintain business interruption insurance?

A1.11.5 Do you have an employee help desk? Customer support center? What is the availability of support? Phone (certain hours, 24–7)? Email? Web-based?

A1.12 Regulatory Compliance

A1.12.1 Were you ever cited or asked to write a corrective plan of action by the authority having jurisdiction related to information security (records, surveillance, access)?

A1.12.2 Do you/did you have in-house or contracted legal or compliance professionals review your IS policies and procedures and employee handbook?

A1.12.3 Any independent reviews (external auditing firm, etc.)? Were any deficiencies noted?

A1.12.4 What standards were audit(s) based on?

A2. INFORMATION ASSET, THREAT AND CONTROL ASSESSMENT

A2.1 See Table A2.1.

TABLE A2.1 Information Asset, Threat, and Control Assessment Worksheet

Use to set priorities for information assets and threats, and to identify whether new controls are needed.

Instructions:

Information Asset—List information assets including architecture, infrastructure, files and records (analog and electronic).

Information Asset Priority—Enter low, medium, or high based on asset sensitivity. For high ratings (only), enter facts to justify high priority (internal/external mandates, etc.).

Threat Priority—Enter low, medium, or high. To evaluate the priority, consider: (*1*) vulnerabilities and threats to the corresponding information asset, (*2*) likelihood the threat(s) may occur, (*3*) potential damage to the asset if the threat should occur, and (*4*) likely costs to the business if the threat occurs. Enter justification for high threat ratings.

Controls Needed—Answer yes or no for high priority information assets and high priority threats to indicate whether more controls are needed. Enter comments about any existing controls, comments about the adequacy of existing controls, and suggestions for potential controls, if known. Controls include physical, technological, and human factor (end user, policy and procedure) categories along a continuum for prevention, detection, response, or recovery.

When preparing the assessment, consider the entire life cycle of each information asset: data collection, data entry, data usage (creating documents, reports, databases), when/where/how information is collected, accessed, compiled, used, tracked, moved or transferred (as when signatures are required for approval), stored (short and long term, network, cloud, portable devices), archived, shared and destroyed (deleted or shredded). It may be useful to review existing access control documentation to locate categories of information assets.

Architecture/Infrastructure

	Info Asset Priority *(low, med, high)*	**Threat Priority** *(low, med, high)*	**New Controls Needed?** *(yes, no)*
Input and output devices: • Computers, printers • Surveillance			
Secondary storage devices			
Servers (physical, virtual)			
Data warehouse			
Memory devices			
Mobile devices • Company issued • Personal			
Limited or embedded systems			
Processor capacity of operation at one or multiple security levels			
Operating system, tasks performed and specific programming			

TABLE A2.1 *Continued*

Architecture/Infrastructure	**Info Asset Priority** *(low, med, high)*	**Threat Priority** *(low, med, high)*	**New Controls Needed?** *(yes, no)*
Equipment and software maintenance and license schedules			
Network system protocols and logs (patch, configuration, change management processes)			
Current testing methods and previous exploits, attacks, or excessive outages			
Vendor authorizations and access requirements			
Privilege authorizations			
Emergency security concerns and response requirements			
Uninterrupted power supply (backup)			
Storage methods for logs, drives, surveillance tapes and records, investigation and incident reports			
Media marking, handing, storing, and disposal			
Back up locations and media			
Virtual software and storage			
Protect cloud based stored data and know responsibilities			
Maintenance schedules, service-level and outage agreements			
Lease requirements			