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