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.