



Designation: D8320 – 21

Standard Practice for Implementing an Information Security Program in a Cannabis Operation¹

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.