

Security, Preventing Unauthorized Intrusions & Deescalating Dangerous Situations

Massachusetts

We work with a high-value product and a lot of cash. Although it's uncommon for a dangerous situation to occur, it's **important to feel safe and secure while you work in a licensed facility or are transporting/delivering cannabis**. AND, important for our patients, caregivers and customers to feel **safe and secure while shopping** at our dispensaries **or consuming** at our Social Consumption Establishments.

Be familiar with your facility and unique security details. Always be **attentive to your surroundings**. If you see something suspicious, report it. If you see someone in the facility you don't recognize, introduce yourself and make sure they have their employee identification properly displayed or if they are a visitor, that they have been properly checked in as a visitor and are wearing their licensee-issued visitor identification. As required by the CCC, all visitors must be escorted by an employee.

If you **feel unsafe or threatened**, remove yourself from the situation. If possible, **reach out to a manager and/or call the police**.

Be aware of where your **duress/silent alarms/panic buttons** are located. Only permit employee access to areas of the facility that are necessary for their workflow.

Being **aware and proactive** are imperative to recognizing potentially dangerous situations.

Security Professionals

Your facility may have third-party security guards on site. Even if they are present, it's important to remember, security is a focus for all employees. The safety of everyone in and around the facility is dependent upon each employee following all security protocols and paying attention.

Security Equipment

We also have the following:

- Well-lit indoor and outdoor areas
- Alarms
- Panic buttons/duress alarms
- Cameras with motion detection
- Locked commercial doors
- Secure rooms
- Safes/Vaults

Security Camera Recordings

Cameras record 24-hours a day, 365 days a year without interruption. They capture activity almost everywhere (except bathroom/changing rooms) at a resolution that reveals clear and certain identification of any person.

Cameras are placed in the following locations at a minimum:

- Safes/Vaults/Cash Handling Areas
- Cultivation/Processing Areas
- Sales areas/Each POS
- Storage areas
- Destruction areas
- Storefronts
- Entrances/Exits

Security, just like compliance, is ALL of our jobs!

Preventing Unauthorized Intrusion

A best practice to avoid potentially dangerous situations is to prevent unauthorized access to the facility.

Tailgating

One of the most common types of unauthorized access is tailgating, which occurs when one or more people follow an authorized user through a door. Often the user will hold the door for an unauthorized individual out of

Security, Preventing Unauthorized Intrusions & Deescalating Dangerous Situations

Massachusetts

common courtesy, unwittingly exposing the building to risk. Decrease the likelihood of tailgating by training your team on security and awareness. An effective reduction technique is to implement “mantraps” that restrict entry to one individual at a time and don’t permit anyone to circumvent them.

Door Propping

Similar to tailgating, propping doors open, most often for convenience, is another common way unauthorized individuals gain access to a location and potentially create a dangerous situation for the people and assets within. Some access control systems include the capability to detect when doors are propped, alerting security personnel or managers who can respond and investigate the situation as needed.

Levering Doors

You might be surprised to know how easily many doors can be levered open using something as small as a screwdriver or as large as a crowbar. Advanced access control systems include forced-door monitoring and will generate alarms if a door is forced open. They are highly effective at detecting door levering.

Keys

Whether stolen, lost or loaned out, keys can pose a major problem. They are often impossible to track when lost, forgotten, stolen or loaned to someone else, and if an individual tends to tailgate to enter the building, they may not notice missing keys for several days. Electronic key management solutions can be deployed to track keys, with the added benefit that many of these systems can be integrated with access control for an added layer of security. Keys *may not* be left in locks or stored or placed in a location accessible to individuals who are not authorized to access cannabis or cannabis products.

Access Cards

With the added advantage of identifying authorized users who swipe in with an access control reader, electronic key cards are a more high-tech alternative to traditional keys. They are prone to the same risks associated with keys, namely the potential to be lost, stolen or shared with an authorized or unauthorized person.

There are four main categories of access cards: Magnetic stripe, proximity, proximity smart cards and contact smart cards. Magnetic stripe cards are the easiest to duplicate and are susceptible to wear and tear or damage from magnetic fields. Proximity cards and smart cards are much less susceptible to duplication, and smart proximity cards can be programmed with much more information than access cards, allowing them to be used for a variety of interactive applications in addition to physical access, including network access. Some proximity smart cards, however, require a small battery, which can diminish their lifespan.

The effectiveness of access control cards can be improved if they also serve as photo ID cards, which decreases the likelihood that individuals will forget them at home. Complementary technologies and solutions, such as individual identification cards and/or biometrics, bring even greater reliability and effectiveness to access cards.

Biometric Access Control

Biometrics are the analysis of biological data using technology. Typically, this data relates to specific physical traits that an individual might have. So, biometric access control is the use of this biological data to either grant or deny access to a building or area of a building. Biometric access control systems may use unique characteristics like fingerprints, facial features, retina, or voice to allow entry to certain properties, buildings, or rooms.

Unauthorized access can create dangerous situations for any business or organization. If your organization is susceptible to any or all of these risks, it’s important to seek access solutions that will address those specific risks to reduce or even eliminate the possibility of unauthorized access and ensure the highest level of security for your facility.

**Security, Preventing Unauthorized Intrusions
& Deescalating Dangerous Situations**

Massachusetts

Deescalating Potentially Dangerous Situations

Be **attentive to verbal and non-verbal signs** of potential violence and pay attention to your “gut instinct.”

Your intuition can be a great support to you. This “gut feeling” may show up in our body as; increased heart rate, perspiration, nausea, feeling indecisive and/or hair rising on the back of your neck.

Some *verbal* warning signs of a potentially dangerous situation:

- Threats – Direct or Veiled
- Threats – Conditional
- Boasts of prior violence or of losing control
- Confused thinking
- An increase in pitch when speaking – indicates throat is tightening
- Repetitive word use, parroting and or echoing
- Forced or strained speech
- A nervous laugh or laughing at inappropriate times (Laughing may be a way for a body to shed emotions)
- Yelling or screaming
- Non-stop profanity

Some *non-verbal* signs of a potentially dangerous situation:

- Personal space violation
- Standing toe to toe
- Finger pointing
- Making fists
- Staring through you
- Face flushing
- Heavy breathing and/ or flaring nostrils
- Person refuses any eye contact
- Someone blocks egress

Non-Physical / Non-Contact De-escalation

Use your words, voice, and body language (never physical contact) to calm a tense situation and keep everyone safe. Pair these steps with the Verbal Do’s and Don’ts below.

- **Stay calm first.** Take a breath, keep your voice low and slow, and don’t take insults personally.
- **Keep your body language non-threatening.** Hands open and visible, a relaxed face, and stand at an angle with at least an arm’s length of space.
- **Listen and acknowledge.** Let the person vent, then name the feeling: “I understand this is frustrating.” Avoid saying “Calm down” and don’t argue.
- **Set respectful limits and offer choices.** Say what you can do before what you can’t, and give two reasonable options.
- **Use your team.** Signal a manager early, and let only one person do the talking.
- **Never touch, block, or restrain anyone.** Let the person leave, and never block their exit or follow them outside.
- **Know when to stop and get to safety.** If there is a threat or a weapon, or the person advances or blocks your exit, move toward other staff, a locked area, or an exit, use the panic button, and call 911. If someone demands cash or product, comply.
- **Afterward,** notify a manager, document what happened in the incident log, and follow house SOPs for reporting to police and the Cannabis Control Commission.

*For the full set of techniques, see the **Deescalating Potentially Dangerous Situations** summary.