3796:3-2-05 **Processor security.**

(A) The department shall determine the appropriate storage and security requirements for all processor facilities, and may require additional safeguards to ensure the security of medical marijuana. A processor shall comply with the security plan submitted as part of its processor provisional license application. At a minimum, the processor shall:

(1) Install an adequate security alarm system around the perimeter of the facility to prevent and detect diversion, theft, or loss of medical marijuana, utilizing commercial grade equipment;

(2) Maintain or construct fencing and gates that surround the facility to prevent unauthorized entry to the facility or unauthorized access to waste disposal containers located outside the facility;

(3) Utilize a video surveillance recording system installed by a vendor that is approved by the department and that meets the standards required by the department to prevent and detect diversion, theft, or loss of medical marijuana;

(4) Maintain all security system equipment and video surveillance systems in a secure location so as to prevent theft, loss, destruction, or alterations

(a) A processor shall limit access to surveillance areas to type 1 key employees that are essential to surveillance operations, law enforcement agencies, security system service employees, the department, and others when approved by the department; and

(b) A processor shall make available to the department, upon request, a current list of type 1 key employees and contractors who have access to the surveillance room. A processor shall keep all on-site surveillance rooms locked and shall not use such rooms for any other functions.

(5) Keep all approved safes, vaults, or any other approved equipment or areas used for processing or storing of plant material, medical marijuana extract, and medical marijuana products securely locked and protected from unauthorized access;

(6) Ensure the outside perimeter of the facility is well-lit and in accordance with the processor's plan in its license application;

(7) Restrict access to any area within the facility containing plant material, medical marijuana extract, or medical marijuana products to all persons except licensed employees and agents or an individual permitted to access the facility under the supervision of a licensed employee or agent in accordance with the visitor authorization procedures set forth in rule 3796:5-2-01 of the Administrative Code;

(8) Limit the use of combination numbers, passwords, or electronic or biometric security systems to licensed, authorized employees, and prevent the sharing of any employee-specific access credentials; and

(9) Not allow keys to be left in the locks and not store or place keys or badges in a location accessible to persons other than licensed, authorized employees.

(B) The processor shall install a security alarm system and a video surveillance recording system under paragraph (A) of this rule. A security alarm system and video surveillance recording system shall, at a minimum, contain the following:

(1) A system designed to detect motion and identify unauthorized access to the facility;

(2) Video cameras that capture the entire facility, including direct placement near the entrances, exits, and parking areas to capture a clear and certain identification of any person entering or exiting the facility, which shall be appropriate for the normal lighting conditions of the area under surveillance;

(3) Video cameras shall be directed at all approved safes, approved vaults, marijuana sales areas, and any other area where plant material, medical marijuana extract, or medical marijuana products are being processed, stored, or handled;

(4) The video surveillance recording system shall comply with the following minimum capabilities:

(a) Provide a direct feed and login capabilities to the department to allow for real-time access and monitoring of the facility via the live video surveillance recording system.

(b) A display monitor with a minimum screen size of twelve inches shall be connected to the electronic recording security system at all times.

(c) Installed in a manner that will prevent cameras from being readily obstructed, tampered with, or disabled.

(d) The ability to immediately produce a clear color still photo that is a minimum of 9600 dpi from any camera image, live or recorded.

(e) A date and time stamp embedded on all recordings. The date and time shall be synchronized and set correctly and shall not significantly obscure the picture.

(f) Cameras installed outdoors and in low-light interior areas shall be day/night cameras with a minimum resolution of six hundred lines per

inch (analog) or D1 (IP) and a minimum light factor requirement of 0.7 LUX. The installation of additional lighting may be required to increase picture clarity and brightness. Cameras shall be calibrated and focused to maximize the quality of the recorded image.

(g) Allow for the exporting of still images in an industry standard image format, including .jpg, .bmp and .gif. Exported video shall have the ability to be archived in a proprietary format that ensures authentication of the video and guarantees that no alteration of the recorded image has taken place. Exported video shall also have the ability to be saved in an industry standard file format that can be played on a standard computer operating system. All recordings shall be erased or destroyed prior to disposal.

(h) Security recordings shall provide an image resolution of at least D1, and the image frame rate shall be at least three frames per second during alarm or motion based recording.

(i) Repair or replace any failed component of the video surveillance recording system within twenty-four hours, unless notice is provided to the department and an extension is approved.

(5) Twenty-four hour live feed with motion-activated recording capabilities from all video cameras, which the processor facility shall make available for immediate viewing by the department upon request and shall retain the recordings for at least forty-five days. If a processor is aware of a pending criminal, civil or administrative investigation or legal proceeding for which a recording may contain relevant information, the processor shall retain an unaltered copy of the recording until the investigation or proceeding is closed or the entity conducting the investigation or proceeding notifies the processor that it is not necessary to retain the recording;

(6) Silent alarm, which can be utilized in the event of a holdup or other instances of duress, which notifies law enforcement;

(7) Panic alarm, which for purposes of this subsection means an audible security alarm system signal generated by the manual activation of a device intended to signal a life threatening or emergency situation requiring a law enforcement response;

(8) Automatic voice dialer, which for purposes of this subsection means any electrical, electronic, mechanical, or other device capable of being programmed to send a prerecorded voice message, when activated, over a telephone line, radio or other communication system, to a law enforcement, public safety or emergency services agency requesting dispatch;

(9) A failure notification system that provides an audible, text or visual notification

of any failure in the surveillance system. The failure notification system shall provide an alert to the processor facility within five minutes of the failure, either by telephone, email, or text message; and

(10) The ability to comply with the security requirements of this rule for a period of at least forty-eight hours during a power outage.

(C) In addition to the requirements listed in paragraph (B) of this rule, each processor shall have a back-up alarm system approved by the department that shall detect unauthorized entry during times when no employees are present at the facility and that shall be provided by a company supplying commercial grade equipment, which shall not be the same company supplying the primary security system.

(D) A processor shall keep all security equipment in good-working order and the systems shall be inspected and all devices tested on an annual basis.

Effective:

Five Year Review (FYR) Dates:

_____

Certification

_____

Date

Promulgated Under:	119.03
Statutory Authority:	R.C. 3796.03
Rule Amplifies:	R.C. 3796.03