Access Control

A critical element of any layered security plan is addressing access control – monitoring and controlling entry points, so only those with the right permission can access certain areas.

- Access control starts at the furthest point possible. If there is a perimeter fence, the gate is the first point of control. If the gate is left open, consider installing a camera to monitor visitors.
- A license plate reader in the parking lot can be helpful in identifying security threats. Although private entities are not allowed access to the DMV database to identify vehicle owners, you can track frequent visitors and receive alerts if known threats enter, such as disgruntled former employees.
- Ensure that exterior lighting provides full coverage for the parking lot and walkways, and does not leave any dark areas vulnerable to criminal activity. Use LED lights in the 4K to 5K range for more natural light.
- Maintain landscaping to create clear sightlines and remove hiding spots. Shrubbery should be no higher than two feet, and tree canopies should be trimmed to hang no lower than six feet. This will provide better sightlines, enhance feelings of safety for employees and visitors, and increase territorial reinforcement, as it indicates to an observer that the property is well-maintained and monitored.
- Whenever possible, maintain a single point of entry for the public. All other doors and windows should remain closed and locked, in accordance with fire codes.
- Entrances should be monitored to prevent unauthorized access. The amount of public access will depend on the facility, but any restricted area should be kept locked.
- Scan visitor IDs on entry. Visitor control systems can run an instant background check against the sex offender registry or local law enforcement data.
- Provide visitors with a lanyard or sticker that immediately communicates they have the correct access. Train employees to respond when they see someone without the appropriate access ID.