

IAPE STANDARDS SECTION 8 – SECURITY

Standard 8.1: Security – Policy

Standard: Written policy should require access controls that will ensure that unauthorized persons do not enter secure areas. These controls include, but are not limited to: key control, changing locks or access codes with changes of personnel, access logs, after-hours procedures, use of surveillance cameras and alarms.

Definition: A written policy that defines all issues related to the security of the various property and evidence storage areas.

Reasoning: Enforceable written policies are needed compelling employees to adhere to security requirements that, if violated, can jeopardize the integrity of the property room and interfere with the chain of custody.

A written directive should require that only authorized personnel have access to the areas used by the agency for storage of property and evidence. Policy should define who has access to keys, access control, key duplication, changing of locks or access code with changes of personnel, access logs, after-hours procedures, and alarm testing.

It should be clearly stated in the agency's policy that anyone who has keys or access to the keys will be questioned and may be considered as a suspect in an investigation relating to any missing evidence. If the Chief/Sheriff/CEO has a key, it may also negate his/her ability to oversee a criminal and/or administrative investigation.

Standard 8.2: Security – Access

Standard: A written policy should permit only authorized personnel to have access to the property room storage areas, and no one other than property unit personnel should have keys or mechanical/electronic access to the property storage areas.

Definition: Access refers to the process that controls entry into restricted areas.

Reasoning: Entry into restricted storage areas should be closely controlled to prevent accusations of alteration, unauthorized removal, theft, or tampering with property or evidence stored by the agency. Access restriction protects the proper chain of custody. Those permitted access should include the property officer(s), and the supervisor. All other persons who enter the property room/storage areas must be documented in an Access Log with the reason for needing access and they should be escorted at all times while within the room and/or storage areas.

The manager/administrator who has oversight of the property unit and the Chief/Sheriff/CEO of the agency should not have independent, unescorted access into the property room and/or storage areas. If one of those individuals has a key or access, the agency should establish a system that requires another authorized person to disarm the alarm, thereby creating a two-person rule.

As noted in Standard 8.1, having independent/unescorted access into the property room/storage areas may adversely impact an administrative inquiry and/or a criminal investigation. The agency's policy should clearly articulate that anyone, including the Chief/Sheriff/C.E.O., who has independent/unescorted access into the property room/storage areas may be investigated if there is any breach of security in those areas.

Standard 8.3: Security – Access Logs

Standard: An access log should be maintained for documenting any entry by anyone that is not assigned to the Property Unit.

Definition: An access log is a document that records the entry of non-assigned personnel into the property room, and why the entry was necessary. The log should record name, ID number, reason for the entry and which employee assigned to the property unit escorted the person.

Reasoning: Personnel outside the property unit may occasionally have a need to enter the storage locations of the property unit. Detectives may need to view a large piece of evidence that cannot be easily moved outside of the permanent storage location, or some type of building maintenance issue might require access. These persons should not be allowed access without immediate supervision at all times.

Supervisors should review the access log on a monthly basis and it should also be inspected as part of a periodic audit by the agency or outside consultants. The purpose of the inspection is to ensure that the department policy is being complied with.

Evidence or property is often discovered missing years after the actual theft. Therefore, it is imperative that access logs be maintained for at least 10 years so that they are available to investigators. Additionally, in the event of a defense challenge in court, the retention of the logs should reflect the time period for the oldest item of evidence in the property room in the event it is challenged in court.

Standard 8.4: Security – After Hours Access

Standard: It is always suggested that an assigned property officer be called in for after-hours entry or the key-holding supervisor if the property officer is not available. If this is not practical, a two-person rule is necessary, which would include the completion of the access log.

Definition: After-hours access to the secure property room means anytime an assigned property officer is not available for call-out, and there is a compelling reason for immediate access that cannot wait for the property officer or supervisor to arrive.

Reasoning: After-hours access by non-assigned personnel should be discouraged. In the event that after-hours access is necessary and assigned property room staff are not available for recall, policy should restrict the method of entry into the property room. At no time should one person enter alone, two individuals should be present.

Standard 8.5: Security – Key Control / Electronic Access Control

Standard: All keys, access codes, combination numbers, and proximity cards should be closely monitored, and accounted for annually. Keys should not be available to anyone other than property room personnel.

Definition: Key and electronic access control refers to accounting for all keys and access cards on a scheduled basis to guard the integrity of the evidence.

Reasoning: Conducting periodic audits of a key-holding persons' keys/access cards ensures that authorized employees have possession of them and that all are accounted for.

Backup keys to the evidence storage areas should not be utilized unless they are kept by the **Unit** Commander, or designee, in a locked safe or drawer. Entry of the Unit Commander into the property room without a second person may result in the Commander becoming part of the investigation in the event evidence is missing.

Under no circumstances should an unsecured key to the property room be kept in a location where multiple persons have access to it, such as the Watch Commander, Patrol Sergeant, or the Officer in Charge's office.

Standard 8.6: Security – Lock Changes

Standard: Locks, access codes, and combinations to the property room should always be changed with any resignation, termination, retirement or transfer of Property Unit key-holding personnel.

Definition: Lock changes refers to changing the locks, keys, combinations or other electronic access devices which secure the storage and office areas of the Property Unit. Locking systems include, but are not limited to keys, access codes, combinations and locks.

Reasoning: Locking systems should be changed whenever personnel reassignments occur to ensure that a departing employee no longer has access to the various storage and office areas.

The property room should be equipped with high quality locks that can be replaced whenever personnel changes occur. One way to achieve this is to use interchangeable core locks that permit the keys to be changed easily and inexpensively.

Alternatives to traditional keys are either electronic locking systems or mechanical systems that may include a personal identification number (PIN) which records who accessed the door and includes date/time of entry.

When locks, access codes, or combinations are changed by an employee outside of the property unit (facilities manager) or an outside service (locksmith), the process needs to be closely monitored to ensure that the third party doesn't have the ability to gain access to secure areas. One safeguard may be to have an independent alarm system that the third party or contractor can't control or defeat.

Standard 8.7: Security – Alarms

Standard: All storage areas should be alarmed and monitored on a 24-hour basis. Storage rooms that contain guns, money and drugs should be separately alarmed or independently zoned area whenever possible.

Definition: A security alarm system may include an audible or silent signal that is activated anytime there is an unauthorized entry.

Reasoning: Intrusion alarms need to be installed so as to alert other department personnel in a 24-hour monitoring position that there has been a breach of security in a specific area.

Alarm technology now permits many different activation methods, including, but not limited to: motion, thermal, sound, contact points, pressure pads, seismic alarms, and even laser beams.

The activation of any alarm should be monitored in a communications center, front desk, Watch Commander's office, or at a private alarm company. Having a third party such as a private alarm company receiving the activation signal is a good practice as the alarm company provides an outside source for the

notification process and reduces the likelihood of other station personnel from compromising the system.

Many alarm systems are capable of sending a text message alerts directed to a manager or property officer's cell phone or computer.

Rooms that contain high-profile items, such as firearms, narcotics and money should be provided with enhanced security that may be achieved with alarms for separate storage areas.

Refrigerators and freezers should be equipped with alarms that indicate if the temperature changes above a designated level. The alarm should be monitored in a 24-hour location, such as the communications center, for example.

Standard 8.8: Security – Duress Alarms

Standard: Property release counters without the presence of a sworn officer should have a duress alarm to summon assistance quickly, if needed.

Definition: An audible or silent duress alarm may be used to summon assistance when a person becomes boisterous or threatening while conducting business at a public release counter.

Reasoning: Civilian personnel are occasionally called upon to release property to persons who may disagree with departmental policy, property description, or legal constraints. When this occurs at a public counter that is remote from immediate uniformed assistance, the civilian employee should have some method of discretely calling for assistance. This may be a telephone, a portable radio, a silent alarm, a duress button, or just a buzzer that remains on until it is reset.

Any type of duress alarm should be tested monthly and a record of the tests should be maintained for future reference.

Standard 8.9: Security – Video Surveillance

Standard: Video surveillance cameras should be utilized whenever enhanced security or a long-term record of ingress, movement, and egress is desired.

Definition: Video surveillance systems are used to record who and when anyone has gained entry into specific defined areas.

Reasoning: Installation of video surveillance equipment should be considered to act as both a deterrent for good internal controls and externally to dissuade unauthorized entry without detection.

All doors into a secure area should be equipped with cameras in addition to those areas where guns, money and drugs are stored. Including cameras where evidence is deposited, such as counters and lockers, can validate when evidence was submitted as well as confirming that evidence was indeed submitted. Installation of cameras at any release counter may document the release, memorialize the transaction, and may protect the agency from accusations of mishandling evidence.

Video equipment consisting of controllers and recording devices should be in a secure location and should only be accessible to the manager, as long as he or she does not have independent access to the property room. The suggested restriction is a check and balance designed to prevent any tampering with or altering the permanent record.

New digital technologies now allows the data to be stored on hard drive when there is movement in front of the camera, thus limiting the amount of data needed to be stored.. The recording is initiated based upon the movement and the digital data is stored on a hard drive. Once the person creating the motion leaves, the area the recording stops.

The digital data should be stored for a period of years, e.g. at least three or four years, so that it is available to investigators should it be discovered that evidence is missing.

