# Document Control

## Versioning

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reason** |
| Version 1 | February 1, 2019 | Placed into production |

## Applicable Parties

This document is strictly confidential and should only be distributed or viewed by the following parties:

* HAL Designated Associates
* HAL Regional Employees (Compartmented to the Division)
* HAL Management Team
* HAL Auditing Team

## Review Period

This document is subject to review by the Information Security Policy Committee (ISPC) at a minimum interval of quarterly (every 3 months) at a maximum interval of bi-annually (every 6 months).

### Previous Reviews

|  |  |  |
| --- | --- | --- |
| **Committee** | **Review Date** | **Approval Date** |
| ISPC | 7/15/2018 | 8/1/2018 |
| CEO | 1/21/2019 | 1/22/2019 |
| Corporate CISO | 1/23/2019 | 1/23/2019 |

# Purpose

The purpose of this procedure is to document the procedure used ti implement video surveillance within the outline provided by the HAL Video Use Policy.

# Scope

## Applicability

This procedure applies to all HAL employees and affiliates at all HAL facilities and locations world-wide who are required to implement video surveillance tools and techniques as part of their assigned duties.

## Ownership

This policy is under the direct control of the HAL Corporate CIO with input from other members of management with an interest in the program.

# Procedure

## Business Process

* Conduct an assessment of the need for video surveillance. Do the benefits of surveillance outweigh any potential reduction of personal privacy inherent in the system's use?
* What is the likelihood of the risk occurring, and what other conventional means would be effective in achieving the same level of security, if any?
* There may be a number of situations where it may be reasonable to expect video surveillance to take place, for example, at door entrances and in common areas such as elevators.
* Ensure that video surveillance complies with all applicable laws, in addition to privacy legislation. For example, in order to capture sound as well as images you need to consider the Criminal Code provisions dealing with the collection of private communications.
* Document the location of the equipment, any special capabilities of the system, the rationale and purpose of the locations, who will be authorized to operate the system.

## Video Camera Placement

Tenants, visitors and staff have a reasonable and legal expectation of privacy in, and immediately around, their homes and place of work. Cameras must not be directed to look through windows or doors of adjacent buildings or through the windows or doors of non-vacant residences. The use of security cameras to monitor guests entering and leaving tenant's suites is generally not permitted.

Ensure you know the location of the equipment and any special capabilities of the system, and that this information is documented.

## Signage/Public Notification

Privacy laws require that HAL, Inc. post a clear and understandable notice about the use of cameras on its premises to individuals whose images might be captured by them, before these individuals enter the premises. This gives people the option of not entering the premises if they object to the surveillance. Signs should include a contact in case individuals have questions or if they want access to images related to them.

## Information Collected

Information collected through video surveillance should only be used for the purpose that surveillance is being undertaken, or for purposes that are permitted by law. For example, if cameras are installed in an apartment building parking garage for safety purposes, the information cannot be used to track the movements of tenants. However, if a car is broken into, the information can be disclosed to law enforcement.

If a camera is monitored, the recording function should be turned on only when unlawful activity is suspected or observed (motion detection).

## Audio Recordings

Sound may or may not be recorded. All members of staff are presumed to have given consent for audio recording.

## Disclosure of Recorded Information

Information will only be released when authorized by privacy or other legislation.

Individuals have the right to access images relating to them. When disclosing recordings to individuals who appear in them the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.

Any disclosure of video surveillance recordings outside the organization should be justified and documented. If supplied to the police/RCMP for an on-going investigation, request that the police/RCMP confirm they will confidentially destroy the tape when they no longer have a use for it. That way, Name of Non-Profit is not responsible to keep track of getting the tape back for destruction.

Identify the individual accountable for privacy compliance and who can answer any questions about the surveillance system.

## Storage of Recorded Images

The recorded images must be stored in a secure location, and access should be granted only on a need-to-know basis by authorized individuals in the organization.

Recordings should only be kept as long as necessary to fulfill the purpose of the video surveillance. Recordings no longer required should be destroyed in a secure manner. A reasonable timeframe to keep recordings before they are recorded over is 14 days. Most issues will be brought forward within that time frame and then the recording can be saved for investigation purposes.

## Destruction of Video

When there is no longer a business need for the video tapes they should be securely destroyed through a confidential records destruction company.

# Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.

*NOTE: As part of the SECCDC event, infractions of the rules regarding this policy may result in a point penalty.*