



48025 Fremont Blvd. Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

"Who Owns It?" — Video Surveillance System Policy and Administration Guidelines

Ojo Technology
48025 Fremont Blvd.
Fremont, CA 94538
www.ojotech.com

Abstract:

The purpose of this white paper is to provide general guidelines to organizations about who should be in charge of a video surveillance system and to provide additional administrative recommendations for best practices.

Table of Contents

Abstract	1
Table of Contents	2
Introduction	2
Legitimate Purposes	2
What the System Will Not Be Used For	3
Deciding on "Who Owns It?"	4
System Management	5
Video Image Management	7
Resources	8
About Ojo Technology	9

Introduction

CIO, CTO or Head of IT Often, one of the first questions asked of the installer is, "Who should own the system, Operations or IT?" This paper will provide you with guidelines on how to make that decision.

More importantly, this paper outlines the important administrative functions that each organization should implement to provide maximum effectiveness from their system, as well as assure members of each organization's staff, customers, and the public that the system is being used appropriately.

Legitimate Purposes

Most organization's need for digital video surveillance fall into one of these major categories:

- Protecting the individuals and property on the location from criminal acts
- Providing increased customer service, site operations efficiency, and/or site safety through advanced knowledge of real-time events, including software-analytic-based notification
- Cost savings via less labor required
- Cost savings via less product shrinkage
- Public safety, including video feeds to emergency personnel during a crisis
- Part of an access control system
- Forensic analysis of events to establish true facts
- Improve staff and customer peace-of-mind

The first part of every organization's Video Surveillance Policy Manual should be an explicit and comprehensive listing of the intended purpose of the system. Replace the

above general bullets, if they apply to your system, with specific examples of precisely what you expect the system to accomplish, or what it should prevent.

Although you may not be able to list every possible situation, give as many specific examples as possible, such as "capture the faces of individuals painting graffiti on outside vehicles at night," or "rapidly determine the nature of any pallets or boxes left on the loading dock after the dock doors are closed each day."

Camera usage may roughly be divided into three groups: (1) deterrent, (2) real-time monitoring, (3) forensic recording. It is valuable to indicate for each stated legitimate purpose which of these three usage modes is likely to be used for that purpose.

Note that studies have shown the deterrent effect of cameras on criminals is often non-existent until after at least one prosecution has taken place using video images as evidence. However, employees on locations such as construction sites have been shown to operate more safely due to the presence of operating cameras. If the intent is to use the cameras partially for deterrence, it may be valuable to provide video images, either real-time or recorded, on a regular basis to the target audience.

What the System Will Not Be Used For

The short answer is, "everything not listed above as a legitimate purpose."

The law, established through court cases, says that video surveillance systems may not intrude on an individual's "expectation of privacy." This includes employees, customers, vendors, visitors, and the public. In general, open public spaces, such as a sidewalk, have a lower expectation of privacy than a smaller, private space, such as a cubicle. However, except for legally approved police covert surveillance, the best strategy is to provide signage informing all individuals that a space "is monitored by video cameras." Discuss the exact wording of any signage with either your video system installer or your company attorney. Many retail organizations, such as retail stores, banks, grocery stores, and casinos prefer to not post signs. However, for the most part, customers in these facilities should not expect "privacy."

State laws vary, but most states explicitly prohibit any cameras in bathrooms, locker rooms, changing rooms, medical treatment areas, or any location where people expect this level of privacy.

Video surveillance systems should never be used for any personal purpose, for spying, or for entertainment. Excessive zoom, beyond what is needed for the legitimate purpose, is not permitted. Monitoring conversations or events out of curiosity is not permitted, except those that are specifically believed to be relevant to one of the legitimate purposes.

Should your video surveillance system incidentally or accidentally record something private and/or irrelevant to the legitimate purposes, such video should be deleted, with general entry made in the Logbook, such as "incidental meeting in parking lot deleted."

Deciding on "Who Owns It?"

Your digital video surveillance system needs to have one person who is the "system chief." This chief is likely to delegate most administrative and day-to-day functions to other people. However, the system chief must be the one responsible for assuring that the Policy Manual is kept up to date and that all procedures relating to system operation are followed.

The Video Surveillance System Chief Administrator needs to be formally appointed to this responsibility by the most senior member of the management team on site, such as the CEO, President, or General Manager.

The most common choices for "system chief" are:

- COO
- CFO
- HR Director
- General Manager
- CIO, CTO or Head of IT
- Security Manager

We discuss each of these options, below. It may not be intuitive, but the person selected for this role will have a major impact on long-term system operation. The General Manager, or similar person, who appoints the Video Surveillance System Chief Administrator should think about his or her major goals and concerns around the video surveillance system, then appoint someone whose other job duties are consistent with these goals or concerns.

COO – If the primary purpose of the video surveillance system revolves around use of the facility, and a strong COO is on staff who has other site operational responsibilities (such as safety, access control, and site maintenance), and then selecting the COO as the IPVS system administrator often makes the most sense. Expect the system to be run and integrated into other site policies. Safety is likely to be a major concern. Detailed logging and employee concerns may be secondary.

CFO – In many organizations the CFO is in charge of contracts, outside vendors, and sometimes HR and access control. In smaller organizations the CFO may end up in charge of the IPVS system "by default." Most CFO's want to have written procedures from the beginning, and be can be expected to enforce procedures and audit trails. Flexibility and responsiveness may suffer.

HR Director – In an organization with many employees, a strong HR department, unions, or where one of the purposes of the system is to encourage employee safety and/or minimize employee theft, the selection of the HR Director as the IPVS system administrator makes sense. Expect the system management to be responsive to the

concerns and the needs of the employees. The IPVS system should have a solid maintenance contract with a quality outside firm, unless the HR Director is unusually IT savvy.

General Manager – The GM should be the IPVS system manager only if there is no one else qualified for this role. This may be the case for smaller organizations. It is particularly important to have an excellent outside vendor, so that the GM can offload tasks such as training new employees, and preventative maintenance.

CIO, CTO or Head of IT – This appears to many people as the logical choice. After all, an IPVS system is built out of sophisticated IT components. If the IPVS network co-exists on the organization's data network, or the IT department helped to specify and install the system, then this is indeed the appropriate choice. However, some IT departments are not comfortable managing high-visibility security cameras, outdoor hardware high above the ground, and are not used to the "human issues" relating to criminal activity and possible privacy concerns. With this choice it may be possible for the organization to do its own first-level technical maintenance. Some IT managers do not understand the importance of HR procedures and audit logs.

Security Manager – If the organization has a large security department, and the Security Manager is comfortable with IT, this may be the best choice. For most such organizations, a good maintenance contract with a quality outside vendor will assure that the system stays in top operational condition. Expect written procedures and log books to be accurately followed.

For all positions except IT Director, a system maintenance contract should be in place with a quality vendor. A modern IPVS system is not only sophisticated IT equipment, the system includes a large physical network, mechanical parts and precision optics, and outdoor components. Even the best system needs some maintenance and upgrades.

System Management

System management issues include the following:

- Who has day-to-day access to the system, and why, and what are their duties?
- What are the rules for managing the day-to-day access, such as issuing passwords, checking logbooks, and training?
- How is physical security for the system components maintained? What is the policy for physical access, and who is in charge of this?
- What, exactly, gets recorded in the IPVS Log Book?
- What are the crisis management procedures?
- How is system maintenance handled?
- How are issues, problems and complaints handled? There should be a process.
- How are video images handled?

Each organization needs a written Digital Video System Policy Manual. The policy manual should clearly answer all of the above questions.

The Policy Manual should be reviewed annually. The General Manager or equivalent senior site manager may wish to appoint a review committee that includes representatives from each of the following parts of the organization:

- Operations
- IT
- Facility
- HR
- Customer Service (if appropriate)
- Brand or company image representative (if appropriate)
- Legal (if appropriate)
- Unions (if appropriate)

Make sure that at least one participant on the review team clearly represents your customers and another participant clearly represents your employees, as a group.

Video Image Management

It is very important that every video or still image exported, removed or archived out of the system is faithfully recorded. Every image should have a written "chain of custody" log, including dated and timed signatures of each individual who handles a copy of an image.

For many organizations, no copy of an image should leave the perimeter of the facility without the signature of the most senior site manager, such as the General Manager.

The room where the Network Video Recorder (NVR) is located should have a locked door, which stays locked and closed unless an authorized individual is going through it.

The Logbook should include a signature, date and time of each person who is provided with a key to the room.

The Logbook should include an entry for all actions that use or change the IPVS system, except for normal day-to-day viewing by people who are assigned this role. Changing camera positions, changing operating parameters, and reviewing stored video, are all actions that should be logged.

All requests to view or copy video images from outside the IPVS Administrator's chain of command should be made on a form for this purpose to the IPVS Administrator, who should approve the request with a signature, and assign someone in his chain of command to implement the request.

All requests to view or copy video images from outside the organization should be made directly to the senior site manager, such as the General Manager.

Many organizations should undertake a quarterly or annual audit of the Logbook. Like any good audit, the auditor should not be in the direct chain of command of the system administrator. For example, if the organization's CFO is not the IPVS Administrator, then the CFO may be a good choice to perform an audit. The purpose of the audit is to determine:

- Are the written procedures being followed?
- Is the Logbook current, complete, and accurate?

The written audit report should be provided directly to the senior site manager, such as the General Manager.

Resources

Guidelines for Public Video Surveillance, The Constitution Project, Washington, D.C.

ABA Standards for Criminal Justice, electronic Surveillance, Section B, 3rd ed. 1999, at 2

About Ojo Technology

Ojo Technology designs, installs, and maintains advanced network based video surveillance systems. A privately held company, Ojo delivers customized solutions utilizing the latest network technologies and the most advanced video surveillance products, delivered with a deep understanding of customer needs and a commitment to customer service.

Ojo Technology is solely focused on delivering standards-based, best of class, 'turn-key' IP Video Surveillance (IPVS) solutions. As a master integrator, Ojo combines the best products, technologies, planning, and implementation to deliver the most reliable and functional network-based video surveillance and remote monitoring solutions available.

Ojo Technology's advanced IP surveillance solutions are ideal for demanding applications requiring video surveillance, security, or remote visual monitoring. Ojo specializes in installations for local government, schools, and manufacturing facilities. Ojo also has experience installing complex systems for retail, military, corporate, and public transportation applications.

www.ojotech.com

Ojo Technology 48025 Fremont Blvd, Fremont, CA 94538
Tel 510-249-9540 email: info@ojotech.com