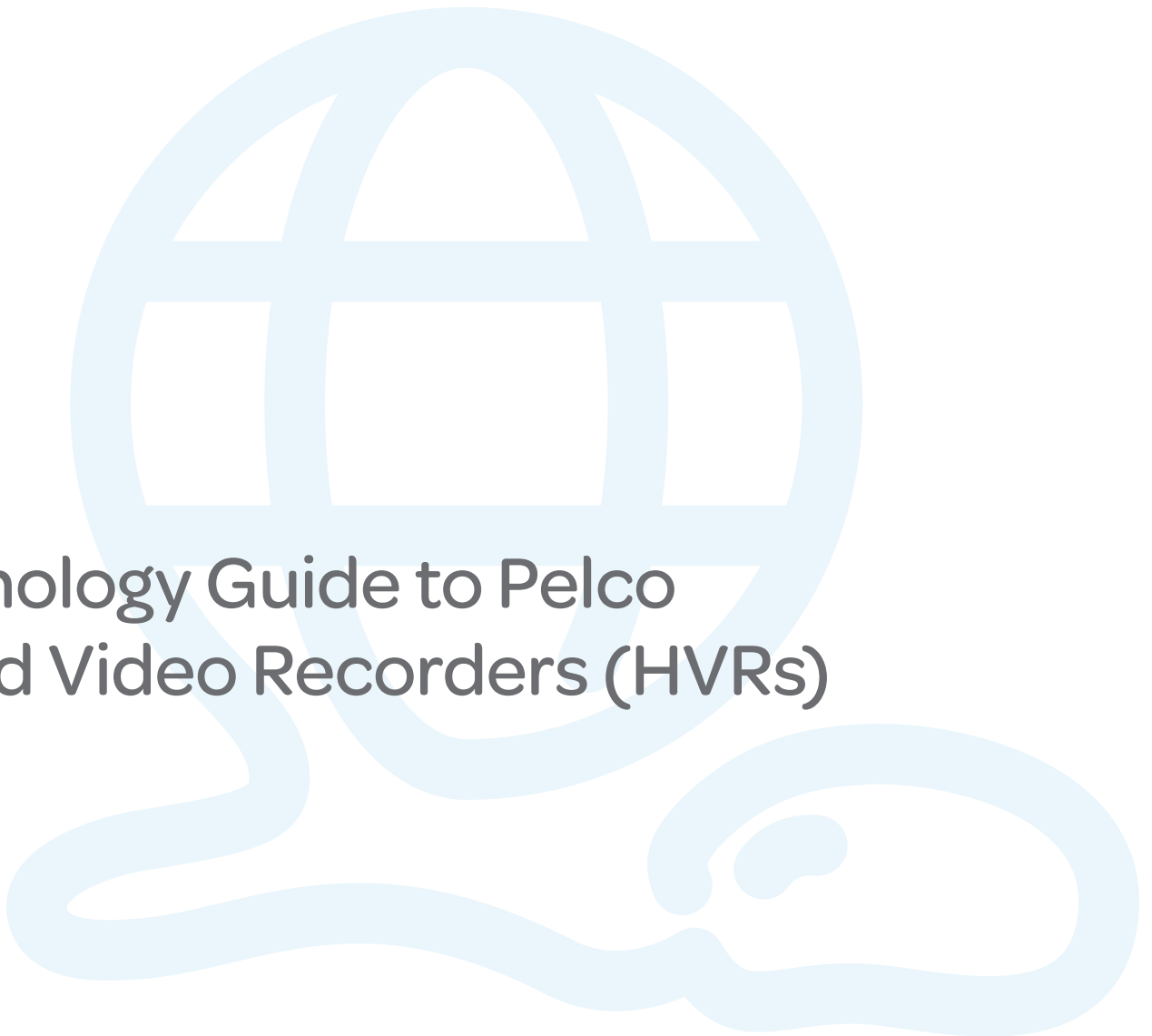




# Technology Guide to Pelco Hybrid Video Recorders (HVRs)



Pelco's DX8100 and Digital Sentry Digital Video Recorder product lines provide customers with a complete solution for live viewing, recording, playback and storage of digital video. This guide presents topics that Information Technology (IT) and physical security professionals will need to know when working with Pelco HVRs.

Pelco HVRs Utilize Many IT Industry standards and technologies such as TCP/IP, HTTP, RTSP, NTP, DHCP, DNS, SMTP, SNMP, SOAP, SSH, etc. Consequently, these HVRs often fall within the domain of IT devices in addition to being physical security devices.

Topics included in this paper are the nature of IP video compression, DVR and HVR deployment topologies, working with HVR Remote Clients, IP Cameras, IT security considerations, and video storage considerations.

### IP Video Terminology

Here are some important technical terms to know when working with IP video:

**Compression** – The technique used to decrease the amount of data required to represent individual frames of video during transmission over the network or storage on an HVR. Video/audio compression is sometimes referred to as the CODEC.

**Bitrate** – The number of bits of data required for a given unit of time to achieve a desired image resolution and frame rate. Bitrates are often expressed in kilobits or megabits per second.

**Resolution** – The number of pixels per image within each frame of video. This is usually represented by an image height and width (i.e, 640x480), or in higher resolutions, by the total number of pixels, in millions (i.e, 3 megapixels).

**Bandwidth** – The amount of data that a network can transmit at any given time. The higher the bandwidth, the more video the network can support. Bandwidth is usually expressed in thousands or millions of bits per second (i.e., kbps or Mbps).

### IP Video Compression

Video communicates massive quantities of information. In analog video systems, electrical signals are transmitted through a dedicated cable for each video source. However, in IP video systems, multiple video signals are transmitted on a single communications link. Raw video must be compressed to provide the same quality of video across shared digital links. The type of compression is sometimes referred to as the CODEC – derived from “compressor-decompressor.”

Three major technologies are used to compress streams of video to a size sufficient to be transmitted across an IP network.

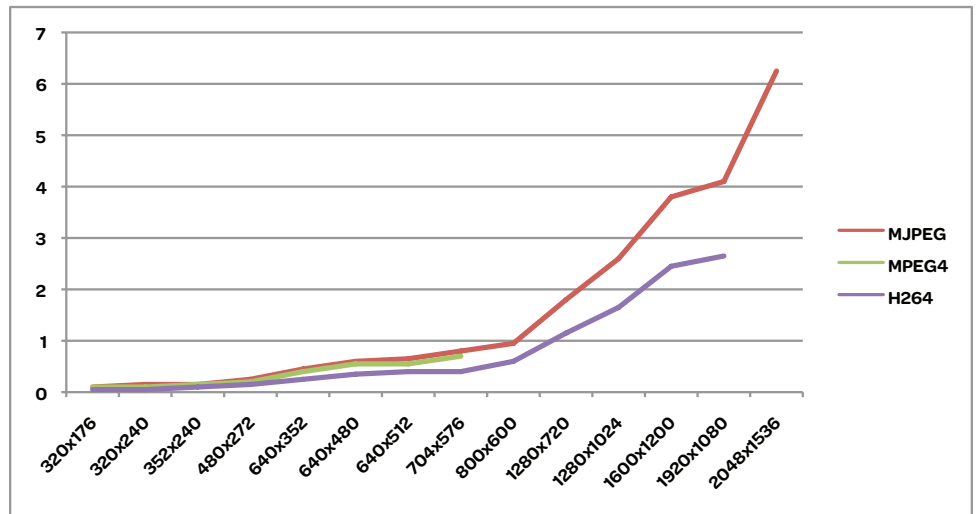
MPEG4 is a video compression standard that provides high quality video at lower bandwidths than MJPEG. This compression scheme not only compresses individual images, but also interleaves sparsely transmitted whole images with smaller frames that represent the differences between the whole images. By only transmitting “what has changed” for a number of frames

DX8100 continues to lead the way in video output flexibility. Dual-Display, Camera View Favorites, Server-to-Server functionality and expanded playback and search capabilities ensure complete coverage for security professionals.

between full frames, the system reduces the amount of redundant data being transmitted across the network. Streams that utilize MPEG4 use less bandwidth than MJPEG for the same resolution and frame rate.

H.264 is a significant refinement of MPEG4 that further reduces the network bandwidth required for a given video stream. The H264 standard employs numerous techniques to achieve lower bitrates than MPEG4, especially as frame rates and resolutions increase. Systems based on H264 are necessary to practically achieve high definition (HD) resolutions in IP video. One tradeoff with H264 compression is the increased expense of decompressing the video for rendering. Systems based on H264 are necessary to practically achieve high definition (HD) resolutions in IP video. One tradeoff with H264 compression is the increased expense of decompressing the video for rendering.

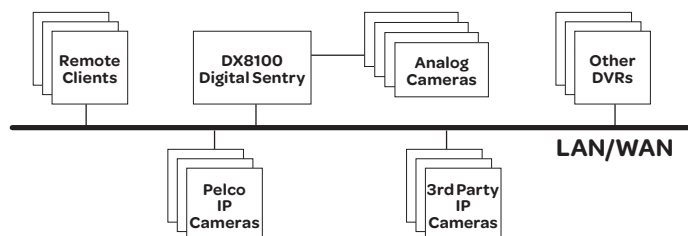
The following graph shows the relative bit rates (in Mbps) for common resolutions at 5 fps.




Data bit rates increase significantly as frame rates and resolutions increase. This trend in bit rate is true even for efficient compression schemes such as H264. This has implications to both network design and storage on HVRs and DVRs.

### DVR Deployment Topologies

Today, Pelco produces both HVR and DVR systems. These HVRs and DVRs include the best of analog video’s maturity, reliability, and low cost, with IP video’s flexibility and increased power. These new HVRs and DVRs allow customers to use encoding on-board the DVR, or to connect IP cameras directly to the HVR. HVRs present new challenges as they become an increasingly integral component of an organization’s IT infrastructure.





In the past, the DVR was a stand-alone device with all camera and user interaction central to the DVR itself. Today the deployment model for HVRs is more complex. HVRs are now a citizen of the network, communicating with their remote clients, Pelco and third party IP cameras, and other DVRs in addition to traditional analog cameras. In essence, the HVR is a distributed system of hardware and software devices.

A key advantage to IP technology is the ability to deploy IP products using a variety of network topologies. IP video can be moved over great distances or routed and rerouted in ways that analog video signals cannot. While the possibilities are limitless, care should be taken to view the entire physical security application as a single system, and to deploy on to the underlying network accordingly.

Remote clients that utilize IP to connect to a remote HVR or DVR provide tremendous flexibility for the operator. However, capacity planning is required to ensure sufficient bandwidth and correct behavior from the application. Additionally, IT security should be a high concern when deploying the remote client – especially when connecting to a HVR or DVR from a different network. More detailed recommendations for remote client deployment are listed below.

Generally, IP cameras should be as logically close to the physical HVR or DVR as possible. These cameras should be connected over reliable, higher bandwidth links than may be necessary for IP traffic in other applications. Further requirements for IP cameras are listed below.

#### Remote Clients

HVR and DVR remote clients allow the operator to monitor live video from any location on their network. Users can play back recorded video and remotely administer HVRs and DVRs.

Remote clients facilitate the control (for example PTZ) of cameras attached to the HVR or DVR. Authentication and configuration dialog between the remote client and the HVR or DVR adds additional overhead.

Two important considerations need to be kept in mind when working with remote clients:

- Capacity planning – To ensure that sufficient network bandwidth will exist to accommodate the application at-hand.
- Potential IT security implications exist when a system is designed with remote client connections in mind.

#### Network Capacity Required for a Remote Client

When viewing recorded or live video on a Pelco HVR or DVR, the remote client pulls frames of video across the network. The amount of network bandwidth used depends on the resolution, the frame rate, and the compression scheme used. As the remote client experiences bandwidth limitations, the remote client will pull fewer video frames per unit of time as needed.

Pelco remote clients will use as much bandwidth as needed/available to achieve the desired frame rate for a given resolution compression scheme. The bandwidth usage can be limited by the HVR or DVR bandwidth throttle or from remote clients that include bandwidth throttles—which effectively limits the frame rate. Higher frame rates are achieved by decreasing the resolution, increasing the available bandwidth, viewing fewer channels, or combinations of all of the above.

When viewing recorded or live video on a Pelco HVR or DVR, the remote client pulls frames of video across the network. The amount of network bandwidth used depends on the resolution, the frame rate, and the compression scheme used.

The remote client plays back video at the recorded compression level used when the video was encoded. So IP cameras recorded in MPEG4 sends streams to the remote client, which plays back the video at MPEG4.

High resolution video uses more bandwidth. Remote clients often use streams at CIF (352x240) to 4CIF (704x480) resolutions (less than 0.3 megapixels) to minimize bandwidth demands per stream. Low bandwidth WAN links (such as T1) can become saturated by a small number of client streams, even at lower resolutions such as CIF.

The customer must consider the application for which they intend to use the remote client when determining the required network capacity. Applications that only require periodic review of recorded video and in which lower frame rates are acceptable, can often use lower bandwidth network links. For example, a T1 WAN link may suffice for this application. Solutions that require live monitoring of multiple, high frame rate, high-resolution video (such as in a control room or at a security guard's station) will require high bandwidth links between the HVR or DVR and the remote client.

With a bandwidth throttle, customers can set a budget for the application, and then not worry about quality of service issues for the other systems that may be using the network link. Lower frame rates are often an acceptable trade-off across the low bandwidth network link.

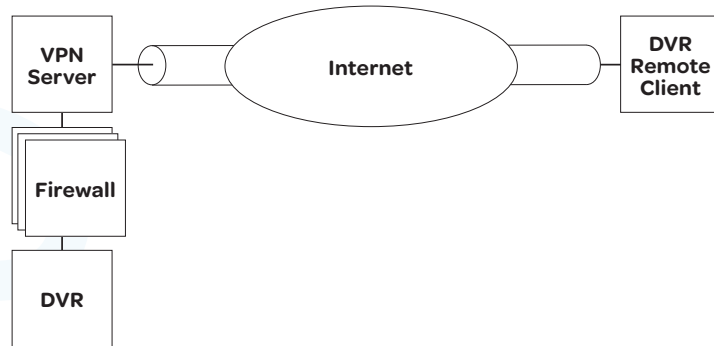
In general, remote clients do not lose critical functionality when network links are unreliable. Most usage of the remote client can survive intermittent drops in network bandwidth, increases in latency, or brief interruptions. With the exception of certain use cases (such as the export of video from a DVR via a remote client), the remote client rarely needs the ability to retrieve every frame of video at all times. In applications in which reliability of the video between the DVR and the remote client is mission critical; the deployment topology should be designed to locate the remote client and the DVR on the same logical or physical network with high bandwidth links.

### [Secure Access to DVR via Remote Client Over a WAN](#)

Remote clients present an opportunity to use the HVR or DVR from a remote physical location. However, remote viewing requires that a network connection be established between the remote client and the HVR or DVR. Typically, the device is located in a secure location, and should be logically located on a secure network. When the remote client is physically and logically close to the DVR, network security is less of a concern. But when the remote client is truly remote, care should be taken to not expose the DVR to insecure wide area networks.

Users are cautioned against attaching HVRs or DVRs directly to insecure networks such as the public internet. While this is the simplest way to provide access to a DVR over the Internet, this practice can expose the DVR to many threats beyond the control of the user. Additionally, this practice could threaten the integrity of the organization's entire network when the attacker uses the DVR as a breach into that organization.

This is a classic problem in IT, which has several solutions. The most common of which is to utilize virtual private network (VPN) technology to create a “secure tunnel” through lower security networks into the network on which the DVR resides.



In this case, the DVR remains protected behind a firewall, and the DVR remote client achieves access to the DVR through a VPN tunnel.

Bandwidth requirements to stream video from an IP camera may be much higher than those to stream video between a HVR or DVR and the remote client

Using a VPN introduces some overhead to the system. Each packet of data to be transmitted must be encrypted at the source, encapsulated into a special network “envelope” and then decrypted at the destination. This implies that more CPU cycles will be used at the source and destination, and some additional network bandwidth will be required. The amount of overhead varies by the VPN technology being used. But this overhead is typically worth the cost for the benefit of added security.

### IP Cameras

An advantage of IP video over analog video is that IP Cameras can be located anywhere on the network. However, attempts should be made to locate IP cameras on the same network to ensure adequate bandwidth, reduce packet loss and latency, and to increase reliability.

The reliability of a Pelco HVR’s recording of a camera can be of critical importance to the business. Thus it is important that variables that may affect streaming of IP video from the camera to the recorder be minimized. IP cameras should be located on the same physical or virtual LAN, if not connected through the same network switch.

There are several ways the functionality of the HVR and its cameras are affected by characteristics of the network:

### Camera IP Discovery and Initial Installation

Most networks are designed to automatically allocate IP addresses to devices using Dynamic Host Configuration Protocol (DHCP). In some cases, network administrators are required to assign IP addresses to individual devices once the camera is added to the network. In either case, the user must first connect the IP camera to the network and know the IP number before that camera’s video stream can be connected to the HVR. In some implementations, an HVR may be able to automatically discover the existence of a new camera on the network — which simplifies configuration of the camera. If automatic camera discovery is not supported, the administrator enters the IP camera’s IP number into a configuration utility on the HVR during initial installation. Be aware that dynamically configured host IP numbers (IP numbers allocated

via DHCP) may have IP numbers that change under certain circumstances. Thus an IP camera may seem to “disappear” on the network when its IP address is changed and will need to be reassociated with the HVR.

Bandwidth requirements to stream video from an IP camera may be much higher than those to stream video between a HVR or DVR and the remote client. This is because it is not acceptable to lose frames of video from an IP camera that is recording to a DVR. Nearly all applications of video recording put emphasis on the reliability of the video being accurately and completely recorded. Care should be taken to ensure that adequate bandwidth exists on the network link between the IP cameras and the DVR to ensure full frame rates at the desired resolutions. Packet Loss and network latency can affect video recordings originating from IP cameras by introducing lost frames or undesirable artifacts within the video (such as pixilation). In severe cases, established connections can be dropped. When viewing recorded video across a remote client, packet loss can be mitigated against by simply replaying interrupted video. However, when recording live video, events the camera observes may never be recorded properly, and thus are forever unavailable for view. This underscores the need to locate IP cameras and HVRs on the same network, and to use reliable physical connections.

Interrupted connections between a HVR and IP camera can happen both physically and logically. Modern networks often carry a variety of network traffic – the majority of which do not depend on keeping connections established 24/7. It is not uncommon for network administrators to interrupt established network connections when doing maintenance on routers, switches, and network links. This implies that work completely unrelated to the physical security system can result in loss of video recording. Care should be taken to understand the HVR and IP camera’s behavior when connections are broken and how they are reestablished. IT personnel should coordinate any outages with physical security personnel to ensure continuity of operations.

When analog video cameras are directly connected to a DVR, the configuration and management of the cameras is a straightforward task. IP cameras provide greater flexibility and power, but require that the DVR administrator now manage a small network of devices. This additional complexity is a major tradeoff when moving from analog cameras on a DVR to IP cameras on an HVR.

### General Bandwidth Considerations

Bandwidth required between components of the system is largely a function of the compression technologies being used. Compression rate is often expressed in kilobits or megabits per second and is itself a function of the compression algorithm, picture resolution, and frame rate. Some examples are shown below for a Pelco Sarix camera:

COMPRESSION	RESOLUTION	FRAME RATE	BIT RATE
MJPEG	352 x 240 (CIF)	30	1.55 Mbps
H.264	1920 x 1080 (HDTV 1080p)	5	2.65 Mbps
MPEG4	704 x 480 (4CIF)	15	1.25 Mbps

The determination of bandwidth requirements is a straightforward task of addition of the various bitrates required across a given network link.

**For example, to determine if the remote viewing requirements will be met by a given network link, the following steps should be followed:**

1. Determine the bandwidth available on the link – this is a function not only of the link’s capacity, but also the budget available for video traffic.
2. Determine the compression, frame rates, and resolutions that will be used. This will determine the bitrates the streams will require.
3. Determine the number of streams to be viewed simultaneously. This is a function of the use cases or application to which the DVR is being applied.
4. Multiply the bitrates per stream by the number of streams to be viewed simultaneously and determine if this falls within the available bandwidth budget.

**For example, to determine the bandwidth requirements of a group of cameras for reliable recording:**

1. Determine the bit rate of each camera based on the compression, resolution, and frame rate.
2. Sum the bit rates for each stream to get the total bit rate required.

### Storage Considerations

The storage occupied by video on a DVR is directly proportional to the bitrates of video streaming into the DVR for recording. Actual storage consumed per unit of time can be calculated based on the bit rate. This can be calculated by taking the bit rate in Mbps and dividing by 8 (bits per byte), multiplying by 3600 (seconds per hour) to achieve MB per hour. Here’s an example calculation. The first step is to look up the bit rate for a given stream’s compression, resolution, and frame rate.

1. MPEG4 compression, 640 x 480 resolution, 25 frames/sec = 1.55Mbps/sec
2.  $1.55\text{Mbps/sec} / 8 \text{ bits} = 0.19375 \text{ MB/sec}$
3.  $0.19375 \text{ MB/sec} * 3600 \text{ seconds} = 697.5 \text{ MB per hour}$
4.  $697.5 \text{ MB per hour} * 24 \text{ hours} = 16,740 \text{ MB/day} = 16.7 \text{ GB/day}$

The above example tells us that this channel of video will consume 16.7 GB each day in storage.

All bitrates used in storage calculations are approximations. In reality, the bit rate varies based on many factors within the video. The nature and complexity of the scene being photographed, the lighting conditions, and the amount of movement, all affect the efficiency of the compression. Most bitrates are reported as being “nominal” so care should be taken to account for extra storage capacity to accommodate changing conditions.

Pelco provides a storage calculator for its HVRs and DVRs which automates the above process and enables customers to determine the appropriate DVR model for their application. These storage calculators provide additional conveniences such as modifying estimates based on recording duration, motion recording, etc.

Keep in mind that all storage calculators provide estimates only. Their results should be accurate enough to appropriately size a DVR, but cannot predict the actual storage that will be used in a given application. Additionally, small changes to the system’s configuration can have significant impact to the bitrates involved and thus the storage used. Where a retention duration target is critical, additional storage capacity beyond that of the estimate should be acquired.

Pelco HVRs and DVRs support some third party storage configurations. This provides the customer an opportunity to add storage capacity to their device using their own mass storage solutions.

### Third Party Storage

Pelco HVRs and DVRs support some third party storage configurations. This provides the customer an opportunity to add storage capacity to their device using their own mass storage solutions. In some cases, customers may have mass storage available over the network and wish to utilize this storage for video recording.

#### **Storage comes in two general favors:**

**Direct Attached** – these storage devices are attached directly to the DVR via an interface such as SCSI, SAS, or USB.

**Network Attached** – these storage devices are made available to the DVR over a network connection.

Note that mass storage of streaming video is not a typical use case in the domain of IT storage solutions. Most IT storage devices are designed to accommodate few write transactions and many random read transactions. Even high performance storage solutions typically used in database applications are tuned to accommodate transactional duty cycles typical to database applications, not continuous, high bandwidth, write cycles. Video storage is often referred to as the “worst possible scenario” regarding stress and performance requirements of mass storage. External storage that is stressed beyond its design can become unreliable or may not function at all under the heavy demands of video recording.

Video storage is often referred to as the “worst possible scenario” regarding stress and performance requirements of mass storage. External storage that is stressed beyond its design can become unreliable or may not function at all under the heavy demands of video recording.

Pelco qualifies storage devices for each of their DVRs. These devices are tested to ensure that they will handle the continuous stream of incoming video and write appropriately. While DVRs may work with other storage solutions, the user is cautioned to test these configurations thoroughly before deployment.

### IT Security

A DVR is a peer device on the network with other IT devices. Thus, it must comply with the IT security requirements that an organization may have for systems on the network.

Security policy governs several aspects of the operation of the IT infrastructure. Some factors that affect physical security systems on these networks:

**Use of firewalls to control ports and protocols on the network** – This will determine what protocols can be used between different DVR components and across which boundaries. For example, an IT organization may not allow certain ports opened in their firewall to enable remote client operation of a DVR from the internet.

**Ensure devices on the network are not vulnerable to well-known security flaws** – A customer may scan their network using a security vulnerability scanner as part of their acceptance test of the device. These scanners look for common security vulnerabilities that can be exploited across the network.

**Encrypt transmission of data across networks whenever possible** – An IT organization may require that business critical data be encrypted while traversing their internal network, and certainly when traversing the public internet. This to protect from “man in the middle” attacks.

**Keep software systems up-to-date with security patches and anti-virus software** – Networks with mature security policy dictate the patch level and corresponding change management required to keep IT systems up-to-date and virus free.

**Carefully maintain and control access, authorization, and password policy** –

Most IT organizations attempt to consolidate their user authentication and (if possible) entitlement management to both simplify administration and provide better security. Pelco recommends that customers use a network dedicated to physical security that is distinct from their corporate or other operational networks. This will allow some level of independent control over the network’s performance and security.

When operating on a corporate network, customers may want to treat Pelco’s DVRs and HVRs that utilize the Microsoft Windows operating systems like any other Windows based system on the IT network. That is, the DVR will be subject to the organization’s Windows update and anti-virus policy, and will need to be secure against any common attacks known to Windows and exposed via security scanners. This presents some administrative challenges to the customer.

#### **Authentication**

Many IT organizations require that systems on the network use a central database of users for all authentication. This to ensure that the lists of authorized users on the network is centrally managed, and to provide an audit trail of all authentication attempts. For systems using Microsoft Windows, the authentication is typically against a Microsoft Active Directory server. Client systems can be joined to an Active Directory domain which provides directory, authentication, and naming and network information services.

Many DVRs also have a local database of users and entitlements to which the user must authenticate to use the local DVR’s software. Likewise, the user may be required to authenticate to the local DVR’s user database in order to utilize the remote client. For example on the Pelco Digital Sentry system, while the operating system user is authenticated to the Active Directory domain, the DVR software utilizes a different authentication scheme to the Microsoft SQL server database itself.

Joining a Pelco DX8100 to an Active Directory domain is not supported because the DVR software needs administrative access to the local machine.

Customers should see Pelco’s web site for tech tips regarding authentication of Pelco DVRs and HVRs to Active Directory.

#### **Microsoft Updates**

To ensure the security of a Microsoft Windows based system, the IT administration may need to apply security updates to the DVR regularly, if not automatically. This best practice ensures that security vulnerabilities are patched as soon as fixes become available from Microsoft.

Many DVRs also have a local database of users and entitlements to which the user must authenticate to use the local DVR’s software. Likewise, the user may be required to authenticate to the local DVR’s user database in order to utilize the remote client.

Pelco regularly tests and includes the latest Microsoft updates in major releases. The application of Microsoft Windows security updates to Pelco DVRs should not affect the functionality of the DVR. However, the customer should apply these updates at their own risk.

Most IT organizations have a change management policy and procedure that dictates how and when changes to the IT infrastructure will be rolled out. This procedure may include tests of major updates or changes to ensure that IT infrastructure does not cause operational problems. This best practice should be applied to the customer's DVRs as well.

Enterprise management servers exist that automatically push Microsoft updates out to Windows computers. These may be used to automatically keep systems up-to-date.

### **Anti-Virus**

To ensure the security of a Microsoft Windows based system, the IT administration may apply anti-virus software to their systems to protect them from infection or malicious attacks over the network or internally.

Anti-virus software can be installed and kept up-to-date manually, or deployed and updated via various "enterprise" class anti-Virus management systems. These products manage anti-virus software from a central server--automatically pushing out updates as necessary.

Note that stored video files are extremely large, and change frequently. Customers should disable anti-virus of video files and the video database to avoid conflicts with normal system operation.

The Pelco DX8100 requires that the anti-virus software be designed to support the Windows XP embedded operating system. This limits the list of known, supported anti-virus systems that will work on the DX8100. Customers should contact Pelco for recommended anti-virus solutions that will work on the DX8100.