NW SECURITY GROUP
ESTABLISHED 2004

Video Security Systems

Information Security Best Practices Guide

Version 1.1
August 2024

nwsecuritygroup.com

Contents

NW SECURITY GROUP
ESTABLISHED 2004

If you need any assistance our expert team are here to help

Telephone 0151 633 2111

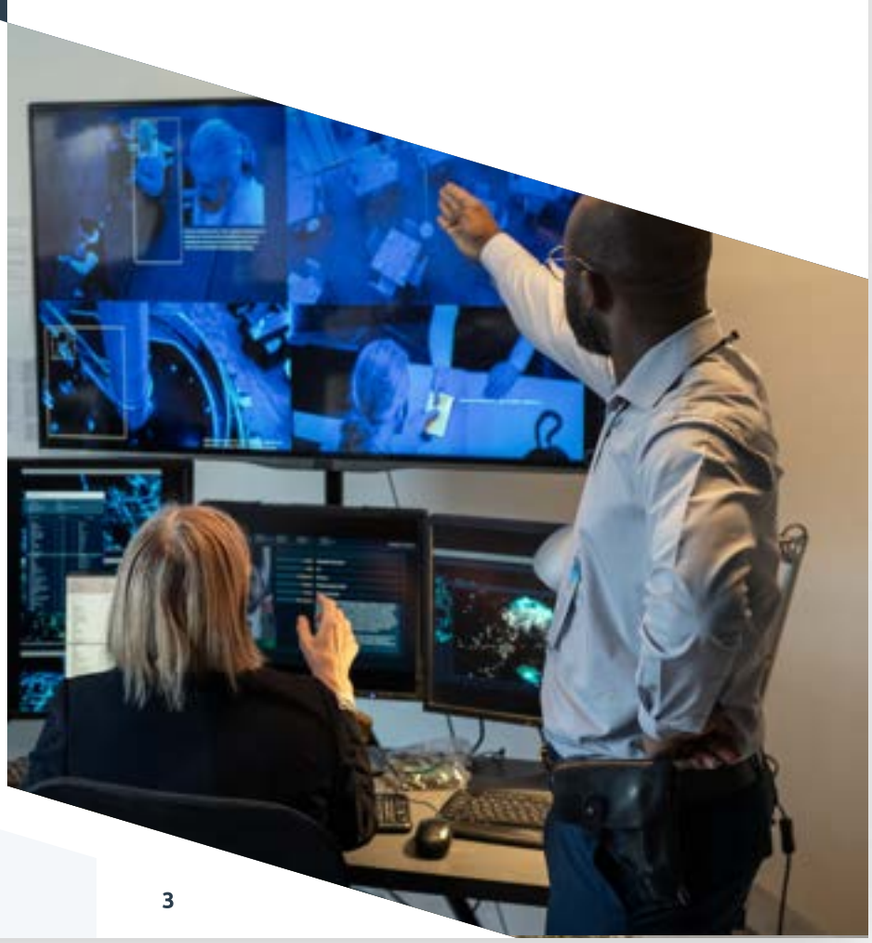
www.nwsecuritygroup.com

About this guide

This guide provides information security recommendations to assist organisations in ensuring that their network and cloud-based video security systems are designed, deployed and supported in a manner which protects the confidentiality, integrity and availability of the systems and the data that's being handled by the system.

This guide has been created per industry best practices and frameworks such as the UK Cyber Essentials Scheme, to which NW Security Group is accredited to Cyber Essentials Plus level since 8th March 2019.

This guide is for companies and organisations that are using or planning to use video security systems within their operations. It advises on best practices in relation to the information security of these systems as a shared responsibility between the chosen vendors, the installation company and the end user.



NW

Product and Vendor Security

First of all, the installer should carry out due diligence on all vendors and products which it introduces to its customers. Installers should not adopt vendor solutions which it considers insecure after assessment, or those that have been banned for usage in UK Government sites or are identified as a high-risk vendor by the National Cyber Security Centre. This includes cameras and other solutions from Hikvision and Dahua.

Ideally, installation companies maintain an approved vendors list. Technology from vendors not on the approved list should not be used. Any new vendors or products should be approved after thorough technical assessment only.

Physical Security of Systems

Physical devices, such as cameras, servers, NVRs, switches and other appliances should be physically situated in a secure manner. Security cameras should be situated and installed securely to protect against risks such as vandalism, tampering, theft and physical alteration.

External infrastructure, such as power units and cabling, should be resilient to environmental conditions. Also, power and data cabling to cameras should be protected to prevent interference.

Servers and NVR appliances should be situated securely to prevent theft or tampering and protect surveillance data in the event of a security incident. Appliances and devices installed in network racks should undergo risk assessment. Where required, adequate power controls (such as UPS) and cooling should be implemented.

Firmware and Software Updates

If the customer is on an appropriate service level agreement (SLA) with the installer, the installer should be responsible for patches and updates to the system devices they install. Where the installer does not manage the system(s) or devices, or where the customer is not on an appropriate SLA, the system user should take responsibility for patches and updates.

The installation company should keep abreast of vendor security bulletins and ensure that any vulnerabilities rated as critical or high on the Common Vulnerability Scoring Standard (CVSS) Version 3 shall be patched within 14 days of a patch becoming available, provided the customer is on an appropriate SLA.

Where possible, patches and software updates should be automatic, though in some cases this may not be possible. System users are also advised to implement a regular regime of vulnerability testing. Where a security system is deployed on a computer or server (such as Windows or Linux), the system user should be responsible for the patching of the computer or server unless otherwise agreed with the installer, or unless supplied by the installation company covered under an appropriate SLA.

PRINT ME
& TICK ME

Authentication and Access Control

Poor authentication and access controls are a significant factor in breaches of security systems.

Considerations regarding secure authentication and access control are listed below:

- ☐ Device default passwords must be changed immediately on setup.
- ☐ Passwords should be a minimum of 12 characters.
- ☐ It is recommended that passwords, as minimum, use three random words such as 'ClubBrooklynMountain' or are randomly generated by a password manager.
- ☐ Changed passwords should not be a re-use of previous passwords.
- ☐ Per the latest guidance from the NCSC, passwords need not be rotated on a regular basis, to avoid password fatigue.
- ☐ Where possible, multi-factor authentication should be enabled and enforced, and in the case of administrator accounts, must be enabled.
- ☐ Passwords for systems should be unique, and not shared across customers.
- ☐ Shared passwords for customer systems should be stored in the organisation's password vault. Staff password vaults should be protected with multi-factor authentication.
- ☐ Access to systems shall be locked down as much as possible. For example, systems open to the internet should be locked down to IP addresses or placed behind a VPN.
- ☐ Access should be granted based on 'least-privilege'. Installers and system users should ensure that accounts used on systems only have the privileges and access rights required for the account's role.
- ☐ Administrator accounts should be restricted, approved and documented.
- ☐ Administrator accounts should not be used for activity such as web browsing or emails to avoid the risk of malware infection.
- ☐ User accounts for administrators or engineers who leave should be disabled immediately.
- ☐ For remote access to end user systems, the installer may use a service such as TeamViewer. Where TeamViewer is used, best practices should be followed as advised in this article.
- ☐ Where unattended access to customer systems is configured, such access must be hardened via the usage of allowlists.
- ☐ Access to staff remote access accounts should meet the password and MFA criteria as set out in both this document and in line with the requirements of the Cyber Essentials standard.
- ☐ The installation company's staff may be authorised to share passwords between devices on an end user's system. However, passwords should never be shared between different end users or systems. Where unattended access to customer systems is configured, such access must be hardened via the usage of allowlists.
- ☐ Access to staff remote access accounts should meet the password and MFA criteria as set out in both this document and in line with the requirements of the Cyber Essentials standard.

Did you know?

Most CCTV systems are not set up to standard practice, let alone best practice?

PRINT ME & TICK ME

Encryption

Where possible, security data, such as video footage, network streams and other data should be encrypted both in transit and whilst at rest. It is recommended that data at rest is encrypted to AES 256 standards, and data in transit is encrypted using TLS version 1.2 as a minimum.

When an installer is accessing a customer system remotely, access to the system should be encrypted using either TLS encryption or by using an encrypted IPsec VPN.
On Milestone XProtect systems recorded footage may be signed and not encrypted depending on the compute capacity available on the system.

Privacy and Data Protection

The system end user is be responsible for understanding the privacy and data protection obligations it has when deploying video security (CCTV) and other security systems.

Some of the privacy and data protection obligations to be considered are listed below:

- ☐ End users are recommended to appoint a data controller with responsibility over the CCTV / security system.
- ☐ Data subjects should be informed that they are being recorded, usually via signage.
- ☐ The customer should identify a lawful purpose for processing the data.
- ☐ Access to security systems should be controlled.
- ☐ Customers should not retain data longer than necessary.
- ☐ Customers are responsible for registering with the Information Commissioner's Office (ICO).
- ☐ Customers should understand the penalties for non-compliance with data protection regulations such as UK GDPR.
- ☐ Where required, the customer should complete a data protection impact assessment (DPIA) or a legitimate interest assessment (LIA).
- ☐ Customers are recommended to hold a CCTV policy, and that their privacy policies include security monitoring.

Further guidance on data protection for CCTV and video surveillance systems can be found on the ICO's website at ***https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/***

Network Security

In most cases, the security of the network which security systems reside on tend to be the responsibility of the system user. In such cases, it is recommended that the end user's network infrastructure is designed to minimise the risk of lateral movement in the network should a vulnerability in a system be exploited.

Video security (CCTV) systems should be deployed in a segmented VLAN and subnet from other production systems such as user computers and servers. Access control lists should be considered to control communications between VLANs.

End users should consider implementing local area network (LAN) security controls to prevent misuse of network connections used by devices such as IP cameras. LAN security controls could include 802.1x RADIUS authentication or MAC address bypass (MAB).

Where the installer or the end user deploy systems on a wireless network, or implement a point-to-point wireless link, systems should connect to a unique or hidden SSID.

Where a system is deployed which is accessible from the internet (for example, on-prem and cloud-based video management systems), the systems should be deployed in a separate firewall zone or DMZ and be locked down as much as possible from other internal systems.

Firewalls should be deployed at the boundary between the end user's network and the internet. It is advised that firewalls feature intrusion detection and prevention services (IPS/IDS). By default, firewalls shall block all inbound services.

Malware Protection

Underlying systems (such as Windows or Linux) which host security software and other systems should be protected from malware intrusion. The system should have anti-malware software installed, where such software is available for that system.

In addition, where necessary, exclusions should be made for processes and programs on the security system to avoid performance problems. This should be coordinated between the end user and the installer.

System Hardening

To minimise the attack surface of the installed system, all systems should be hardened as much as possible to best practices to prevent against attacks.

Below, we have identified some common system hardening techniques for some of the common systems and devices.

PRINT ME & TICK ME

Cameras and Other Devices with IP addresses

Camera systems can be managed by both on-premises and cloud-based platforms, the guidance below is recommended to harden cameras and other devices:

- ☐ Cameras and other associated hardware should be sited securely to avoid physical interference or damage.
- ☐ If required by the customer, devices should be asset tagged and recorded in an associated asset register. Typically devices are recorded by Mac address, serial number and IP address.
- ☐ Power and data cabling should be installed securely, where needed and possible in trunking or other containment to avoid physical interference.
- ☐ Where software is installed on an underlying Windows operating system, the Windows system should be protected by anti-malware technology. Anti-malware technology exclusions should be configured to not scan databases, as this may impact system performance.
- ☐ Windows updates have occasionally impacted on systems. It is therefore recommended that Windows automatic updates are disabled. However, there is a balance to be struck between operational availability and the security of systems. Either the installation company or the end user should implement a regime of testing and deploying Windows patches to systems hosting software. The UK Government Cyber Essentials Scheme advises that critical and high security updates should be installed within 14 days.
- ☐ Accounts for both access and underlying operating systems should be provided based on 'least privilege'. Where possible, user accounts should be individualised for auditing purposes. Administrators of systems shall use accounts with only the required privileges and avoid, wherever possible, using the root account where a less-privileged account is available to them.
- ☐ Where systems are connected to Microsoft Active Directory (AD), it is recommended that AD users accounts, security groups and group policy objects (GPOs) are configured in-line with industry best practices such as:
    - ☐ Enforcing a minimum password length of 12 characters.
    - ☐ Locking accounts after 10 or fewer failed logins to prevent brute-force attacks.
    - ☐ Providing role-based access for accounts to align with the least-privilege model.
- ☐ Where an engineer creates a new password for the 'root' user, this password should be stored in a secure password vault.

Please note this list is not exhaustive and further considerations should be made between the installer and the end user.

PRINT ME
& TICK ME

Continued...

- ☐ Shared passwords across cameras should only be used within a single customer environment; such passwords must not be shared with other customers and passwords should meet the requirements set out earlier in this document and be stored in secure password vaults.
- ☐ There should never be a requirement to open inbound firewall rules to IP cameras or other network devices. Remote access to systems should be provided using secure systems.
- ☐ The Customer should provide a separate VLAN or physical subnet for systems, which should be logically separate from other IT systems and be protected via access control lists.
- ☐ Network security controls such as RADIUS 802.1x and MAC address bypass (MAB) should be configured on network devices to prevent rogue devices connecting to the network.
- ☐ Services such as Telnet, SSH and FTP should not be enabled unless there is a documented and approved business case for doing so.
- ☐ Only TCP and UDP ports required for normal operation (i.e. streaming services) should be enabled on systems. All other ports should be closed by default.
- ☐ Even though some systems can auto-update, this can lead to availability and stability issues. Is should be considered to update systems on a periodic basis as part of its Service Level Agreement (SLA). Vulnerability management outside of an SLA should be dealt with on a case-by-case basis.
- ☐ The installation company should keep abreast of the latest security bulletins from the vendors, and advise their customers (end users) accordingly where systems may need to be patched. However, it is advised that the end user implements a regular vulnerability testing regime to detect vulnerabilities in systems.
- ☐ Data transferred between cameras and management systems should be encrypted where possible.

Please note this list is not exhaustive and further considerations should be made between the installer and the end user.

PRINT ME & TICK ME

Video Management Software (Milestone XProtect, Axis Camera Station and others)

Milestone XProtect or Axis Camera Station video management software (VMS) and systems are normally deployed via an on-site server.

- ☐ VMS software, where installed on Windows machines, should be stored on a dedicated computer to avoid introducing security vulnerabilities and performance issues into the system.
- ☐ The Windows system should be protected by anti-malware technology. Anti-malware technology exclusions should be configured to not scan (Milestone XProtect) databases or processes, as this may impact system performance.
- ☐ Windows devices should be hardened in-line with industry best practices and based upon the customer's requirements. Hardening could include the removal of unused software and accounts, and the disablement of services such as Remote Desktop or SMB, if not required.
- ☐ The underlying hardware should prevent the use of mass storage devices, such as USB pens, and disable the auto play functionality in the operating system.
- ☐ Windows systems should be updated regularly to prevent against the exploitation of vulnerabilities. The UK Government Cyber Essentials Scheme advises that critical and high security updates should be installed within 14 days.
- ☐ When deployed in a Microsoft AD environment, it is recommended that AD users accounts, security groups and group policy objects (GPOs) are configured in-line with industry best practices such as:
  - ☐ Enforcing a minimum password length of 12 characters.
  - ☐ Locking accounts after 10 or fewer failed logins to prevent brute-force attacks.
  - ☐ Providing role-based access for accounts to align with the least-privilege model.
- ☐ It is recommended that an SQL server (management server) (for Milestone XProtect), where possible, is installed on a separate server.
- ☐ Accounts for both the VMS and underlying operating systems should be provided based on 'least privilege'. Where possible, user accounts should be individualised for accounting purposes. Administrators of systems should use accounts with only the required privileges and avoid, wherever possible, using the most privileged account where a less-privileged account is available to them.

NW

Please note this list is not exhaustive and further considerations should be made between the installer and the end user.

PRINT ME
& TICK ME

Continued...

- ☐ The installation company may require accounts with local administrator access to the machine where the VMS is installed. The end user should take precautions to ensure that such accounts are not 'over privileged'. For example, with Domain Administrator rights.
- ☐ Multi-factor authentication should be enabled on the system where possible. Customers should also consider the use of Security Assertion Markup Language (SAML) to provide single sign-on services to users.
- ☐ For Milestone XProtect in particular, it is recommended to use AD Groups for access permissions, where an AD group is assigned to a user role in XProtect. The customer then determines who gets access to the system via the AD Group.
- ☐ The installer should ensure that only the required VMS services are enabled on the system. If services are not used, they should not be enabled.
- ☐ Only TCP and UDP ports required for normal operation (i.e. web app access) shall be enabled on systems. All other ports should be closed by default.
- ☐ Where a Milestone XProtect or other VMS system is exposed to the internet, the system should be deployed in a 'demilitarised zone' (DMZ) which will minimise the attack platform if the server is breached. TCP or UDP ports open inbound to the system shall be minimised where possible and obfuscated (for example, changing port 8080 to a random, higher port).
- ☐ The system should be protected by a firewall at the edge between the internal network and the server. It is advised that such firewalls have intrusion detection and prevention services (IDS/IPS) enabled.
- ☐ The server should also have a software firewall enabled (for example, Windows Firewall).
- ☐ Access to the web interface of the server (via Microsoft IIS), should be encrypted using the HTTPS protocol. It is advised that a publicly signed certificate is installed on the server. HTTPS communications should use TLS version 1.2 as a minimum.
- ☐ Logging should be enabled on the VMS server and logs reviewed regularly by the customer for suspicious events.
- ☐ Mobile clients, where installed on mobile devices should only be downloaded from approved app stores (such as the Apple or Google Play Stores).
- ☐ It is recommended that the end user ensures that mobile devices are secured to best practice and, where possible, managed by a Mobile Device Management (MDM) solution. Such best practices may include:
    - ☐ Preventing the rooting or jailbreaking of mobiles and tablets.
    - ☐ Ensuring devices are protected by PIN or biometrics.
    - ☐ Only allowing access from devices which still receive security updates from the vendors.
    - ☐ Ensuring the Milestone Mobile app, or other VMS app, is regularly updated.
    - ☐ Installing anti-malware technology where that technology is available for the system (i.e. Android).

Please note this list is not exhaustive and further considerations should be made between the installer and the end user.

PRINT ME
& TICK ME

NVRs (Network Video Recorders)

Where the installation company proposes to install network video recorders (NVRs), the following security hardening guidelines should be followed:

- ☐ Only appliances from approved vendors should be installed at customer locations. This is detailed in earlier sections of this guide.
- ☐ Devices should be installed securely to prevent the theft, destruction or tampering of a device. Other considerations should be given to the physical and environmental protection of the system (for example, power and cooling).
- ☐ The default password should be changed immediately on the system, in line with the password guidance in this document.
- ☐ Individual user accounts should be provisioned, where possible, and accounts must be created based on 'least privilege'.
- ☐ It is recommended to update systems on an annual basis as part of an appropriate Service Level Agreement (SLA). Vulnerability management outside of an SLA is dealt with on a case-by-case basis.
- ☐ The installer should keep abreast of the latest security bulletins from NVR vendors and advise accordingly where systems may need to be patched. However, it is advised that the end user implements a regular vulnerability testing regime to detect vulnerabilities in systems.
- ☐ Systems engineers should avoid opening NVR devices directly to the internet (via port forwarding) and prefer a cloud or web-based management solution.
- ☐ Where an NVR is accessible from the internet, it should be deployed in a DMZ and segmented from other network assets.
- ☐ The end user is ultimately responsible for the security of the network in which the NVR resides and should ensure that network security controls such as intrusion detection and prevention, segmentation, firewalls and access controls are in place.

Please note this list is not exhaustive and further considerations should be made between the installer and the end user.

Other Security Considerations

The guidance in this document is highly recommended to secure the installation and maintenance of video security (CCTV) systems. However, further consideration should be given to the end user's in-house IT policies and procedures, as well as wider information security controls to prevent, detect and respond to cyber security incidents.

Logging and Monitoring

It is recommended that logging should be enabled on all systems and sent to a centralised syslog or security information and event management (SIEM) system. Logs should be regularly reviewed by security specialists and alerts set for suspicious events.

Information Security Incident Response Plan

It is recommended that customers establish an information security incident response plan or contract the services of a dedicated third-party to provide managed detection and response (MDR) services. Incident response procedures should follow industry standards such as NIST Special Publication 800-62 Revision 2.

Information Security Awareness and Training

It is recommended for end users to consider the implementation of an information security awareness training regime, which applies to all their staff. Training should cover common topics such as phishing, malware, ransomware, data protection and the use of removable media.

It is recommended that end user also implement an ongoing information security training and awareness program.

Did you know?

60%

of security breaches in video surveillance systems are due to weak or default passwords.

Penetration Testing and Vulnerability Assessments

Penetration testing, or ethical hacking, is the process of legitimate cyber security specialists attempting to discover and exploit cyber security vulnerabilities in technical systems, and then pivot on networks to access other systems. A well-scoped penetration test will identify vulnerable systems before an attacker has a chance to exploit them.

A vulnerability assessment is a partially automated process of scanning networks and devices for common vulnerabilities and configuration issues. Vulnerability assessments can be purchased on an ad-hoc basis, or by purchasing dedicated software.

End users should assess their level of risk and exposure to understand if a penetration test or vulnerability assessment is required on their systems, as well as the scope of any testing.

Security Accreditations and Certifications

End users are advised to consider security accreditations or certifications based upon their risk appetite and customer or contractual requirements. Such accreditations and certifications could include:

- Cyber Essentials (self-assessment)
- Cyber Essentials Plus (audited)
- ISO 27001
- IASME Cyber Assurance

Further Advice and Assistance

NW Security Group can provide advice and assistance via in-house specialists and a specialist security information partner company.

Telephone 0151 633 2111
www.nwsecuritygroup.com

Disclaimer

About NW Security Group

Established in 2004, NW Security Group is a specialist IP video technology company at the forefront of delivering trusted, cutting edge video surveillance solutions that improve the safety, security, and efficiency of businesses and public sector services.

Providing design, installation and support services, NW is committed to delivering the best possible outcomes through working closely with trusted, world-leading technology partners and taking a collaborative approach in the relationships with our customers. Our commitment is to deliver long-term benefits and investment protection to our customers through system lifecycle planning and support. Having delivered over 100,000 camera channels since our inception twenty years ago, NW is recognised as one of the UK's leading video security providers.

NW | SECURITY GROUP

ESTABLISHED **2004**

Telephone 0151 633 2111

www.nwsecuritygroup.com