NIS2 Compliance Guide

GeoVision Inc.

September, 2024

Table of Contents

1 Introduction

1.1 What is NIS 2?

NIS2 is a cybersecurity law from the EU that impacts the surveillance industry. Its goal is to enhance cybersecurity across all EU member states by enforcing stricter security measures for surveillance systems and the data they handle. Companies are required to defend against cyberattacks and report any security incidents. The law is designed to ensure that surveillance technology across Europe is more secure and trustworthy. Failure to comply can result in fines or operational restrictions.

1.2 Who will be Impacted?

NIS2 affects many important organizations in Europe. It covers both public and private companies. This includes firms with 50 or more workers or those earning over €10 million yearly. It also applies to businesses in critical sectors. These companies must improve their cybersecurity. They need to show they are following the new rules. The aim is to make Europe's network and information systems safer overall.

Sector	Essential (Higher Requirements)	Important (Expends to Include)
Energy	X	
Transport	X	
Banking	X	
Financial market infrastructures	X	
Health	X	
Drinking water supply and distribution	X	
Wastewater	X	
Digital infrastructure	X	
ICT service management	X	
Public administration	X	
Space	X	
Postal and courier services		X
Waste management		X
Chemicals manufacturing, production, and distribution		X
Food production, processing, and distribution		X
Manufacturing (specific categories)		X
Digital providers		X

2 NIS 2 requirements

2.1 For essential and important entities

Regular risk assessment and management:

- Conduct ongoing risk assessments to identify and address cyber risks.
- Management must understand and actively participate in risk management efforts.

Security policies and procedures:

- Develop and implement comprehensive security policies for cyber risk management.
- Establish clear procedures for incident handling, resolution, and reporting.

Security of networks and information systems:

- Implement multi-factor authentication and continuous authentication solutions.
- Use encryption for voice, video, text, and internal emergency communications when appropriate.

Cybersecurity training:

- Train employees in basic computer hygiene and cybersecurity practices.
- Ensure all staff are aware of their role in maintaining security.

Crisis management (business continuity):

- Create and maintain plans for managing operations during and after security incidents.
- Ensure up-to-date backups and plans for accessing IT systems post-incident.

Supply chain security:

- Assess and manage security risks in the supply chain, including direct suppliers.
- Choose appropriate security measures based on each supplier's vulnerabilities.

Incident reporting and response:

- Report significant incidents to competent authorities in a timely manner.
- Develop and maintain incident response plans for effective detection, reporting, and mitigation.

3 Financial and Legal Risks of NIS2

Non-Compliance

Suppliers can support NIS 2 entities by addressing the following requirements:

Financial impacts:

1. Fines: Up to €10 million or 2% of global annual turnover, whichever is higher
2. Remediation costs: Expenses for upgrading systems and processes to achieve compliance
3. Business disruption: Potential revenue loss from operational interruptions
4. Reputational damage: Loss of customers and business opportunities

4 GeoVision Compliance Framework

GeoVision's compliance with NIS 2 requirements:

4.1 Continuous updates and maintenance

Geovision is committed to providing regular software updates and patches to address security vulnerabilities, enhance performance, and introduce new features. These updates are essential for maintaining the security and functionality of your Geovision system.

Key Update Features:

- **Security Patches:** Geovision regularly releases patches to address newly discovered security vulnerabilities, protecting your system from potential threats.
- **Performance Improvements:** Updates often include optimizations to improve system performance, reduce resource consumption, and enhance overall efficiency.
- **New Features:** Geovision may introduce new features or enhancements in updates, providing you with additional functionality and capabilities.
- **Bug Fixes:** Updates address known bugs and issues to improve the stability and reliability of Geovision software.

How to Stay Updated:

- **Manual Updates:** You can also manually download and install updates from the Geovision website or through your device management software.
- **Notification Service:** Geovision will notify customers of new software versions available through various means, such as emails, website announcements, etc.

- **Device Management Tools:** Geovision often provides device management tools that can help you easily manage and update your devices.
- **Detailed documentation:** Geovision provides detailed documentation to help customers understand the content of the update, installation steps, and problems they may encounter.

Geovision's Commitment to Security:

Geovision takes security seriously and invests in research and development to ensure that its software is protected against emerging threats. By staying updated with the latest patches and updates, you can help maintain the security of your Geovision system.

4.2 Access control management

To ensure the security and legal use of software, Geovision has introduced strict authentication and authorization mechanisms. This not only prevents unauthorized access, but also effectively protects your system and data.

Role-Based Access Control (RBAC)

- **Granular Permissions:** Geovision allows you to assign specific permissions to different user roles, ensuring that each user can only access the features and data they need.

Centralized Authentication

- **Integration with AD or LDAP:** Geovision can integrate with your existing Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) infrastructure, allowing you to use a single set of credentials for various systems.
- **Software authorization code:** When purchasing software, you will receive a unique set of authorization codes. Once entered, the software can be activated.
- **Hardware lock:** Plug a USB hardware lock into the computer for the software to function properly.
- **Network authorization:** Connect the software to the server and verify the authorization through the server.

4.3 Data encryption

Geovision offers robust data encryption features to protect your sensitive video data from unauthorized access and interception. Here's a breakdown of the encryption methods supported by Geovision:

- **HTTPS Encryption:** Geovision uses HTTPS to ensure secure data transmission between your devices and the Geovision platform. This includes TLS 1.2 or newer standards for strong encryption.
- **AES-256 Encryption:** The video stream connection between Geovision Camera Station and the client is encrypted using AES-256, a highly secure encryption algorithm.
- **RSA Encryption:** By using RSA encryption, Geovision provides a strong layer of security for its users and protects sensitive data from unauthorized access and disclosure..
- **Data export with password protection:** You can export recordings from SD cards or network shares with password encryption, allowing you to securely share sensitive video data without the need for manual encryption.

4.4 Security incident reporting

Geovision is committed to transparency and proactive incident reporting. We prioritize the security of our products and services and take steps to minimize the risk of vulnerabilities.

- **Transparent Communication:** We strive to communicate vulnerabilities in a timely and transparent manner to our customers, providing them with the necessary information to mitigate risks.
- **Professional services & instant returns:** Geovision's official Cyber Security web page allows customers to report information security issues, and Geovision is also a member of TWCERT (Taiwan Computer Emergency Response Team). It has dedicated personnel to quickly respond and handle information security issues and provide corresponding solutions.
- **Timeliness:** Once new security vulnerabilities are discovered, Geovision will immediately solve and improve them to maintain the safety of product use.
- **Professionalism:** Geovision's security team will conduct in-depth analysis of incidents and provide detailed technical reports to help you understand the severity and impact of the vulnerability.
- **Proactive Disclosure:** Geovision is committed to proactively disclosing any company-related cyberattacks or security incidents in accordance with relevant regulations and guidelines.
- **Regular Patches:** We release regular security patches and updates to address vulnerabilities and improve the overall security of our products.
- **Multiple Platforms:** Updates are available for various Geovision software versions and platforms, ensuring that all systems are protected.
- By prioritizing incident reporting and transparency, Geovision aims to provide a secure and reliable solution for our customers.

4.5 Privacy Protection

Data Protection

- **Data Privacy:** Geovision is committed to protecting the privacy of personal data and complies with relevant data protection regulations.
- **Data Encryption**: Geovision employs encryption techniques to protect sensitive data both at rest and in transit.