240-547-5446
info@gkaccess.com
gkaccess.com

NIS2 Compliance - GateKeeper

Why NIS2 Compliance Matters

NIS2 stands for “Network and Information Security Directive”. Introduced in 2020 and effective from January 16, 2023, the NIS2 Directive is a continuation and expansion of the original EU cybersecurity directive, NIS. Proposed by the European Commission, it addresses the deficiencies of NIS by requiring operators of critical infrastructure and essential services to enhance security measures and report incidents to relevant authorities.

Its objective is to create a common level of cybersecurity across the European Union’s Member States. In a union of diverse countries with varying levels of digital maturity, uniform standards are crucial for ensuring that no member state is left behind. This harmonization helps mitigate the risks associated with fragmented cybersecurity approaches, making it easier to manage cross-border cyber threats. The NIS2 directive is designed to limit the risk that cyberattacks against essential and important entities within the EU will impact their ability to provide services to EU citizens.

NIS2 aims to improve cybersecurity across “essential and important entities” in critical sectors such as **energy**, **transport**, **banking**, **health**, **public administration**, etc. It enforces the implementation of holistic and stringent security controls to reduce risk and prevent cybersecurity damage to systems and data. Requirements cover a gamut of IT systems and resources, including securing IT environments against ransomware, phishing, and unauthorized access.

The NIS2 Directive is now expected to affect more than 160,000 companies across 15 sectors, with non-compliance carrying fines of up to €10 million. Achieving compliance with the NIS2 directive by deadlines in Q4 2024 is essential for all affected organizations and requires the implementation of a robust cybersecurity program.

Key NIS2 Security Dimensions

General Guiding Security Dimensions

240-547-5446
info@gkaccess.com
gkaccess.com

Data Privacy & Protection

- Comply with strict regulations (GDPR, HIPAA, etc.).
- Protect sensitive data with encryption, cryptography, and secure handling.

Business Continuity & Seamless Service Delivery

- Ensure uninterrupted access to critical systems and services.
- Detect, prevent, and quickly respond to incidents that may disrupt operations.

Access Control & Authentication

- Enforce **multi-factor authentication (MFA)** and continuous authentication.
- Limit data access to authorized users and log activity to prevent misuse.

Reporting, Accountability & Risk Management

- Hold corporate management accountable for cybersecurity oversight.
- Conduct regular risk assessments, update policies, and meet NIS2's 24-hour reporting requirement.

Industry-specific Security Dimensions

Healthcare	Manufacturing
• **Patient Data Protection**: Protect sensitive patient information in line with GDPR, HIPAA, and related regulations. • **Healthcare Service Continuity**: Deliver medical services seamlessly with minimal disruption. • **Trust & Adoption**: Build patient and provider confidence in digital healthcare platforms through robust security measures.	• **Supply Chain Security**: Identify and mitigate risks from suppliers and service providers. • **Risk Management**: Conduct regular assessments to address vulnerabilities in production and logistics. • **Compliance Support**: Work closely with IT service providers to align with NIS2 security requirements.

240-547-5446
info@gkaccess.com
gkaccess.com

Finance • **Business Continuity**: Guarantee continuous availability of networks and financial systems to minimize operational downtime. • **Access Control**: Implement strict identity and access management to prevent unauthorized access or data manipulation. • **Monitoring & Detection**: Continuously monitor for anomalies, intrusions, and fraudulent activity.	Energy • **Incident Response & Resilience**: Prevent, detect, and respond effectively to incidents impacting energy security and supply continuity. • **Data Protection**: Safeguard critical operational and customer data against breaches and misuse. • **Governance & Compliance**: Appoint a responsible cybersecurity officer and enforce risk assessments to maintain compliance with NIS2.

GateKeeper Enterprise NIS2 Compliance Chart

NIS2 Section	NIS2 Requirement	How GateKeeper Meets It
1. Risk management	Stronger access control - multi-factor authentication (MFA) is mandatory.	Enforces MFA with proximity token + PIN before any access to a workstation.
2. Corporate accountability	Take accountability for cybersecurity failures.	Provides deeper insight into users' computer activity. Records every login, logout, lock/unlock, and visited websites.
3. Reporting obligations	Organizations must provide a 24-hour early warning, a 72-hour incident report, and a final one-month report detailing recovery and improvements.	All records tracked by GateKeeper can be exported to a SIEM server for real-time monitoring. Alerts and Reports can be emailed directly to accountability personnel for analysis.

240-547-5446
info@gkaccess.com
gkaccess.com

4. Business continuity	Ensure uninterrupted access to critical systems and services, even during disruptions.	Provides fast, password-free MFA logins and session continuity with proximity tokens. GateKeeper MFA does not require the internet, ensuring access for remote/mobile teams.

How GateKeeper Strengthens NIS2 Compliance

1. **Automates Access Control & MFA**
    - Enforces multifactor authentication (MFA) and provides proximity-based authentication for all workstation access.
    - Organizations can granularly assign access permissions to individuals/departments on a per-workstation basis.
2. **Prevents Unauthorized Access & Protects Data Privacy**
    - Automatically locks the computer when users are no longer in proximity to their workstation — preventing unauthorized access or data viewing.
    - Automatically locks the computer after a predetermined number of failed login attempts.
3. **Prevents Service Disruption & Ensures Business Continuity**
    - Employees can log in and out of their workstations in seconds, enabling compliance without slowing service delivery or disrupting operations.
    - GateKeeper tokens support multiple form factors — RFID, NFC, and mobile (iOS & Android) to ensure access without requiring internet access.
4. **Enhanced Accountability & Inspection Readiness**
    - Generates complete audit trails of user-specific activity, simplifying periodic inspections and government reporting.
    - Logs can be exported to SIEM for continuous monitoring for abnormalities.

Benefits for EU Companies

- **NIS2-Aligned MFA**: Meets EU cybersecurity standards without adding friction for end users.
- **Instant Session Lock**: Prevents unauthorized access and potential data breaches in real time.
- **Zero Password Sharing**: Improves accountability, especially in critical environments with shared workstations.

GATEKEEPER

240-547-5446
info@gkaccess.com
gkaccess.com

- **Complete Audit Trails**: Simplifies compliance reviews with precise user logs.
- **Seamless Service Delivery**: Ensures that operations never slow down or get disrupted.
- **Operational Efficiency**: Enables fast, secure access in time-sensitive sectors.