

Achieving NIS2 Directive Compliance Requirements with Teleport

NIS2
Directive



Contents

- Understanding the NIS2 Directive 3**
- Who Must Comply with NIS2? 3
- Key Cybersecurity Measures Under NIS2 4
- Non-Compliance Consequences: Significant Financial and Operational Risks..... 5
- NIS2 Compliance is an Opportunity, Not Just an Obligation 6
- Looking Ahead: The Future of Cybersecurity in the EU 6

- How Teleport Can Help with NIS2 Requirements 7**
- Eliminating Credentials and Standing Privileges 7
- Monitoring and Responding to Weak Access Patterns..... 8
- Managing Policy and Incident Intervention 8
- Modernizing Privileged Access: Boosting Productivity Alongside Security..... 9
- Seamless Integration with NIS2’s Reporting and Monitoring Requirements 9

- Conclusion 10**

The EU's revised Network and Information Security (NIS2) Directive has expanded its scope to bolster cybersecurity measures across essential services and critical entities throughout the EU.

While this framework sets the stage for a new era of resilience, it also brings new complexities organizations must navigate in order to earn and maintain compliance.

Understanding the NIS2 Directive

The NIS2 Directive is a groundbreaking regulation designed to bolster the cybersecurity posture of essential and important entities across the EU. By expanding upon its predecessor, NIS1, the directive introduces more comprehensive requirements and extends its reach to cover a broader range of organizations. Whether your firm is a part of the energy, healthcare, finance, or digital infrastructure sectors, if you're operating in the EU and meet certain criteria, NIS2 likely impacts your organization.

NIS2 mandates that covered entities adopt a risk-based approach to cybersecurity with a focus on preventing, mitigating, and reporting security incidents. This shift ensures that organizations are not only prepared to handle the inevitable cybersecurity threats but are also able to minimize the impact of breaches and recover swiftly. Member States have until October 17, 2024 to transpose the NIS2 Directive into national law, which means that covered organizations will be legally obligated to comply in early Q4 2024.

Who Must Comply with NIS2?

The directive applies to organizations with more than 250 employees, annual turnover (revenue) exceeding €50 million, or balance sheets over €43 million. Smaller, but still significant entities with more than 50 employees and a turnover or balance sheet above €10 million are also included. If your organization fits these criteria and operates in a sector deemed essential to societal functions or the economy, you are required to adhere to the stringent cybersecurity and reporting measures set forth by NIS2.

Essential Entities Covered

- Banking
- Digital Infrastructure
- Drinking Water
- Energy
- Financial Infrastructure
- Healthcare
- ICT Service Management (MSPs/MSSPs)
- Public Administration
- Space
- Transport

Important Entities Covered

- Chemicals (Distribution, Manufacture, Production)
- Digital Service Providers
- Food (Distribution, Manufacture, Production)
- Manufacturing
- Research
- Postal and Courier Services
- Waste Management

Key Cybersecurity Measures Under NIS2

Organizations within the scope of NIS2 must implement robust security measures across their network and information systems. These measures aren't just regulatory checkboxes; they represent industry best practices that can significantly enhance your organization's cybersecurity defenses.

Critical NIS2 measures include:

- **Comprehensive Risk Analysis and Security Policies:** Develop and maintain policies that provide a thorough analysis of risks and ensure your information systems are secure.
- **Incident Handling Procedures:** Ensure rapid detection, response, and mitigation of cybersecurity incidents to minimize disruption and damage.
- **Business Continuity and Crisis Management:** Implement backup management, disaster recovery strategies, and crisis response procedures to ensure operations can continue during and after an attack.
- **Supply Chain Security:** Strengthen security relationships with suppliers and service providers to mitigate risks from third parties.
- **Secure System Development and Vulnerability Management:** Ensure that all systems are securely developed, maintained, and that vulnerabilities are handled and disclosed appropriately.
- **Cyber Hygiene and Employee Training:** Establish basic cyber hygiene practices and ensure that staff are trained to recognize and respond to potential threats.
- **Use of Cryptography and Encryption:** Where appropriate, deploy cryptographic measures to protect sensitive data and communications.
- **Access Control and Asset Management:** Implement strict policies for human resources security, access control, and asset management to protect critical infrastructure.
- **Multi-Factor Authentication and Secure Communications:** Adopt multi-factor authentication (MFA) or continuous authentication solutions to protect access, as well as secure communication systems for emergencies.

These measures ensure organizations subject to NIS2 not only meet regulatory requirements, but are positioned to build stronger and more resilient cybersecurity postures that protect critical data and operations.



Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.

