NIS 2 memo

by CHIMERE

What is the NIS 2 Directive?

The NIS2 (Network and Information Security Directive) is a legislative framework of the European Union designed to strengthen cybersecurity requirements for critical infrastructures and essential services in Europe. In response to ever-evolving cyber threats, it expands its scope to include a broader range of sectors and imposes stricter protective measures:

- Robust technical measures
- Access management
- Rapid response to security incidents
- Increased oversight of suppliers and subcontractors
- The goal is to enhance resilience against cyber threats and ensure adequate protection of networks and essential services.

Am I Affected?

Entities in the identified sectors are classified as essential or important entities based on factors such as size, sector, and criticality. The following are affected:

Essential Entities

High-criticality sectors – businesses exceeding the medium-sized threshold.

Qualified trusted service providers and top-level domain registries, regardless of their size.

- DNS service providers, regardless of their size.
- Electronic communications networks (ECN) or electronic communications services (ECS) – medium-sized and large businesses.

Important Entities

High-criticality sectors – small or medium-sized businesses

- Other critical sectors – businesses exceeding the medium-sized threshold
- ECN or ECS providers – small businesses

To learn more, you can take the test at: https://monespacenis2.cyber.gouv.fr

High-criticality sectors:

Energy, Digital infrastructures, Transport, Space, Health, Public administration, Drinking water, Banking, Wastewater

Other critical sectors:

Financial market infrastructures, Manufacturing, production, and distribution of chemicals, Manufacturing industry, Research, ICT services, Postal and courier services, Waste management (B2B), Production, processing, and distribution of food products, Digital service providers

See the scope and definition of concerned entities (Articles 1 to 7).

QORUM Secur'Num

Chimere is a partner of Qorum Secur'Num, a one-stop shop for cybersecurity and digital compliance. With over 450 cybersecurity experts across more than 50 sites in France, Qorum Secur'Num can support you in all areas of your compliance efforts with the NIS 2 directive.

Directive (UE) 2022/2555 on EUR-Lex

NIS 2 Directive | ANSSI

What Does the Directive Contain?

Cybersecurity Risk Management (Article 18)

This article requires the concerned entities to implement integrated cybersecurity risk management that encompasses prevention, detection, and response to security incidents. The directive emphasizes a proactive approach, recommending regular security risk assessments to adapt rotective measures.

Cybersecurity Governance Policies (Article 20)

This article requires entities to establish appropriate governance policies, including continuity and recovery plans to ensure resilience in the event of a cyber incident. It also mandates cybersecurity training for staff and the development of a security culture within the organization.

Specific Cybersecurity Measures (Article 21)

Among the most important, this article lists mandatory technical measures such as access control, securing communications and authentication, vulnerability management, and securing networks and information systems.

The article is divided into 10 sub-points:

- 21.2.a Policies related to risk analysis and information system security
- 21.2.b Incident management
- 21.2.c Business continuity, including backup management, recovery, and crisis management
- 21.2.d Supply chain security, including security aspects related to the relationships between each entity and its suppliers or direct service providers
- 21.2.e Security of the acquisition, development, and maintenance of networks and information systems, including the handling and disclosure of vulnerabilities
- 21.2.f Policies and procedures for assessing the effectiveness of cybersecurity risk management measures
- 21.2.g Basic practices in cyber hygiene and cybersecurity training
- 21.2.h Policies and procedures regarding the use of cryptography and, where applicable, encryption
- 21.2.i Security of human resources, access control policies, and asset management
- 21.2.j The use of multi-factor authentication or continuous authentication solutions, secure voice, video, and text communications, and secure emergency communication systems within the entity, as needed

Incident Monitoring and Detection (Article 22)

This article requires the establishment of mechanisms for detecting and monitoring incidents, including log analysis and the implementation of intrusion detection systems. It notably requires a continuous monitoring system to quickly identify cyber threats.

Incident Notification (Article 23)

Article 23 imposes an obligation for rapid notification of incidents that have a significant impact on the continuity of services, within 24 hours for the initial alert and a final report within 30 days.

Cybersecurity Audits and Compliance Assessment (Article 24)

Finally, entities must undergo regular audits to assess their compliance with security requirements.

Discover how Chimere can make your compliance easier!

https://chimere.eu/en/chimere-nis2/

contact@chimere.eu

About Chimere.

Chimere is a French and European Zero-Trust Network Access solution. Enter the new era of secure remote access.