REALVNC®

# NETWORK AND INFORMATION SECURITY (NIS2) DIRECTIVE

## Overview:

- Organizations are now seeking solutions that not only enhance security and resilience but also align with new regulatory demands, particularly around secure remote access and critical infrastructure visibility.
- RealVNC® offers solutions that improve operational efficiency while supporting NIS2 compliance obligations.
- It is crucial to have robust solutions in place to reduce the risk of increased sanctions for non-compliance.

The NIS2 Directive took effect on January 16, 2023, and became law on October 17, 2024, across the EU, with each member state responsible for adopting it into national law.

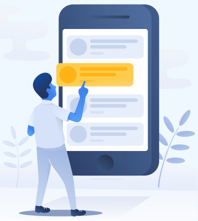
NIS2 represents a significant step toward improving the security of network and information systems in critical sectors. It is holistic, covering both IT and OT (Operational Technology), and aims to enhance the resilience and security of critical infrastructure, as well as the organizations supporting it.

### Sanctions for Non-Compliance

To strengthen overall compliance with NIS2, sanctions have been raised to reflect the importance of protecting critical infrastructure and ensuring secure supply chains.

**Important entities –**
up to 7 million euros or 1.4% of the total annual turnover

**Essential entities –**
up to 10 million euros or 2% of the total annual turnover



### NIS2 applies to two main groups:

NIS2 applies to two main groups. Organizations must consider location, size, and industry when determining their classification.

Importantly, organizations do not need to be based in the EU, NIS2 applies to all companies providing services or activities within the EU.

## Key NIS2 obligations

There are four key areas that NIS2 has introduced which outline the main requirements and obligations organisations must follow.

### Risk Management

- Organizations must take measures to minimize their cybersecurity risks. This includes, but is not limited to, high-level risk assessments, efficient incident management, a secure supply chain, and enhanced network security protocols.

### Improved Incident Reporting and Response

- NIS2 requires senior management to oversee and approve the organization’s cybersecurity measures, as well as receive sufficient training. This ensures a top-down approach, with cybersecurity prioritized at the highest levels.

### Reporting Obligations

- Entities classified as “essential” and “important” must follow strict reporting guidelines. Specific deadlines are in place alongside required documentation to demonstrate incidents are being handled correctly.

### Business Continuity

- Organizations must have sufficient plans to ensure a high level of business continuity in the event of a cyber incident. This includes system recovery plans, emergency procedures, and adequate resources.

### Important Entities 🟩

Other organizations that are not ‘essential’ but provide services to or within the EU, have more than 50 employees or 10 million euros in revenue, and operate within 15 specified critical industries

CHEMICALS · RESEARCH · FOOD · POSTAL SERVICES

WASTE · MANUFACTURING · DIGITAL PROVIDERS

### Essential Entities 🟥

Companies that have more than 250 employees or 50 million euros in revenue and work within eight specified critical industries

ENERGY · TRANSPORT · FINANCE · PUBLIC ADMIN

HEALTH · SPACE · WATER · DIGITAL

## REALVNC: SUPPORTING NIS2 COMPLIANCE

| | |
|---|---|
| **Business continuity solutions** | Ensure uninterrupted operations and quick recovery in the event of a cyber incident. |
| **Compliance-focused approach** | Designed with regulatory frameworks like NIS2 in mind. |
| **Secure supply chain** | Protect sensitive data and ensure third-party risk is minimized. |
| **Clear reporting framework** | Understand and meet reporting obligations confidently. |
| **Proven secure solutions** | Remote access tools designed to safeguard information and infrastructure. |

## HOW REALVNC CONNECT HELPS

| | |
|---|---|
| **Secure remote access** | Safeguard data and enable instant, reliable access without increasing risk. |
| **Regulatory alignment** | Built to comply with industry and government standards, including NIS2. |
| **Incident management** | Supports reporting and incident handling requirements with robust technical measures. |
| **Risk management confidence** | Designed to enhance, not expand, your security risk landscape. |
| **24/7 monitoring** | Our technical team proactively mitigates vulnerabilities, ensuring continuous protection. |
| **Support for reporting obligations** | Dedicated SLAs and session logging/auditing make compliance simpler. |

### Is your organization ready for NIS2?

- Have you conducted a high-level gap analysis to determine if your technology solutions are NIS2 compliant?
- Do you have the right infrastructure in place to ensure compliance?
- Have your current solutions improved work processes and resilience?
- Could RealVNC Connect provide a more effective approach to NIS2 compliance while also supporting other security frameworks?

REALVNC
www.realvnc.com

**Interested in having a conversation about RealVNC and NIS2?**

**Get in touch →**