The NIS2 Directive

NIS2 is the successor of the European 2016 NIS1 Directive. All EU Member States must incorporate it in their national legislation before October 2024. The main goal is to make entities based in the EU more cyber resilant.

What's new

- **Size cap:** > 50 employees OR > € 10 million annual turnover FOR applicable industries & sectors
- NIS2 mandates implementation of **10 Minimum Measures**
- **Supply chain security:** suppliers of 'entities covered by NIS2 scope' must have Basic Cyber Hygiene Practices
- Strict process for **Reporting of security incidents**
- **Fines** up to € 10 million or 2% of global turnover
- **Corporate accountability:** including liability and a potential temporary ban from management roles.

10 Minimum Measures

NIS2 mandates the implementation of 10 Minimum Measures:

- **Risk analysis** and information systems security policies
- **Incident handling**
- **Business continuity**, such as backup management and disaster recovery, and crisis management;
- **Supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers security in network and information systems including vulnerability handling and disclosure;
- **Policies and procedures** to assess the effectiveness of cybersecurity risk-**management** measures;
- **Basic Cyber Hygiene** Practices (baseline security)
- **Cybersecurity training;**
- **Policies and procedures** regarding the use of cryptography and, where appropriate, encryption;
- **Human resources security**, access control policies and asset management;
- The use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
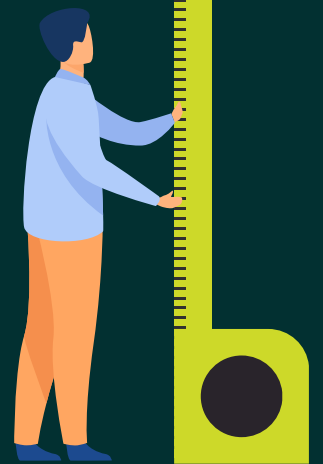
From NIS to NIS2

NIS - Vital suppliers

- Healthcare
- Energy
- Bank and financial market infrastructure
- Water supplies
- Transport
- Digital service providers
- Digital infrastructure

NIS2 - Added industries

- Food
- Space
- Public administration
- Postal and courier services
- Providers of public electronic communications networks or services
- Waste water and waste management
- Digital services such as social networking services platforms and data centrer services
- Manufacturing of certain critical products

TD SYNNEX

Better Together with TD SYNNEX
Road to NIS2

Call to action

- Determine for each of your customers whether they fall under the NIS2's scope
- If the answer is yes, enable these customers to implement the 10 Minimum Measures
- Being a supplier of your customer, you must have your Basic Cyber Hygiene Practices in place

Customer's 10 Minimum Measures & Your Basic Cyber Hygiene Practices

To help you put NIS2 into practice for your customers and for yourselves,
TD SYNNEX has developed a 3-step Route to NIS2.

- **Step A. Risk Analysis, Policies & Procedures** – TD SYNNEX will help you to analyse the current situation and to identify which actions need to be taken. This will result in Policies and Procedures.

- **Step B. Basic Cyber Hygiene Practices** – After completing Step A, TD SYNNEX will support you covering all of the identified gaps with a solution that suits your needs. See image 'Step B' as an example.

- **Step C. - Incident Reporting Obligation** – Incident handling has got very strict requirements under NIS2. TD SYNNEX will help you to clear out the requirements and to implement them in your Incident Response Plan.

Recover · Identify · Project · Detect · Respond — NIS2

Please reach out to us for support on your Route to NIS2:

NL: tdsecurity@tdsynnex.com
BE: tdas_security.be@tdsynnex.com
TD SYNNEX Academy: training.bnl@tdsynnex.com

Step B Basic Cyber Hygiene Practices

Multifactor authentication · Encryption · Backup & Recovery · Security awareness training · Admin rights/ acces control · Install updates · Antivirus · Network security