



FOR SMALL AND MEDIUM-SIZED BUSINESSES IN DENMARK

NIS2 Readiness Checklist

30 yes/no questions to see where your business stands –
in about 15 minutes.

- ✓ The 10 security measures NIS2 requires, in plain language
- ✓ 3 quick questions per measure
- ✓ A simple score and what to do next

polarit.dk

+45 31 67 10 87 • Support@PolarIT.dk

JUMPCLOUD MSP PARTNER

MAKE WORK HAPPEN 2026

PolarIT ApS
CVR 46412249

Does NIS2 apply to you?

NIS2 is the EU's updated cybersecurity directive. In Denmark it applies through the national NIS2 law, in force since 1 July 2025. It covers medium and large organisations in 18 critical sectors – and many of their suppliers feel it too.

1 Do you operate in a covered sector?

For example energy, transport, health, digital infrastructure, ICT service management, manufacturing, food, waste, chemicals, postal services or public administration.

2 Are you a medium or large business?

Generally 50 or more employees, or annual turnover above €10 million. Some organisations are covered regardless of size.

3 Do you supply a covered organisation?

Even if you're not covered directly, your customers must manage supply-chain risk – and will increasingly ask you to show good security.

If you answered yes to any of these, NIS2 is relevant to you. The checklist is a useful health check either way.

Three things every manager should know

01

Management is responsible

Management must approve the security measures, oversee them and take part in training – and can be held accountable.

02

Incidents must be reported fast

Significant incidents: early warning within 24 hours, notification within 72 hours and a final report within one month.

03

Fines are significant

Up to €10 million or 2% of global turnover for essential entities, and up to €7 million or 1.4% for important entities.



How to use this checklist

Answer each question honestly with yes or no. 'Partly' counts as no. Tick the box for every yes, then count your ticks on the last page.

The 10 security measures (NIS2 Article 21)

21(a) Risk analysis & security policies

Know your risks and have security policies to manage them.

We have a written overview of our key systems and data, and the main risks to them. Yes ☐

We have an information security policy approved by management. Yes ☐

We review our risks and policy at least once a year. Yes ☐

21(b) Incident handling

Detect, handle and report security incidents in time.

Staff know exactly who to contact if they suspect a security incident. Yes ☐

We have a written incident plan, including who reports to the authorities within 24 hours. Yes ☐

Logs from our key systems are collected and kept, so we can see what happened. Yes ☐

21(c) Business continuity & backup

Keep the business running during and after an incident.

Critical data is backed up, with at least one copy offline or protected from deletion. Yes ☐

We have tested restoring from backup within the last 12 months. Yes ☐

We have a plan for working if email, cloud services or the office are unavailable. Yes ☐

21(d) Supply chain security

Manage the risk from suppliers and service providers.

We have a list of suppliers that have access to our systems or data. Yes ☐

Our supplier contracts include security requirements. Yes ☐

Supplier access is limited to what's needed and removed when no longer needed. Yes ☐

21(e) Secure acquisition & maintenance

Keep systems secure when buying, developing and maintaining them.

Operating systems and software are updated automatically on all devices. Yes ☐

Vulnerabilities on internet-facing systems are fixed promptly. Yes ☐

Security requirements are considered before we buy or build new systems. Yes ☐

21(f) Measuring effectiveness

Check that your security measures actually work.

We regularly check that our security measures work (reviews, tests or audits). Yes ☐

We can produce evidence – reports or logs – that our controls are in place. Yes ☐

Findings are followed up with an owner and a deadline. Yes ☐

21(g) Cyber hygiene & training

Basic security habits and awareness training for everyone.

All staff have had security awareness training within the last 12 months. Yes ☐

Strong, unique passwords are enforced – for example with a password manager. Yes ☐

Administrator rights are limited to the people who really need them. Yes ☐

21(h) Cryptography & encryption

Protect data with encryption where it matters.

All laptops and mobile devices have full-disk encryption switched on. Yes ☐

Data is encrypted in transit – websites use HTTPS and email uses TLS. Yes ☐

We have a simple policy for encryption and for handling encryption keys. Yes ☐

21(i) HR security, access & assets

Control who has access to what – from first day to last.

We have an up-to-date inventory of devices and user accounts. Yes ☐

Access follows least privilege and is reviewed regularly. Yes ☐

All access is removed on the same day someone leaves. Yes ☐

21(j) Multi-factor authentication

Use MFA and secure communication.

MFA is required for email and cloud apps for every user. Yes ☐

MFA is required for remote access and all administrator accounts. Yes ☐

We have a secure way to communicate in an emergency, even if email is down. Yes ☐

Your score

/ 30

Count your ticks out of 30.

● 25–30

Good shape

You have most of the basics in place. Focus on evidence and documentation – that's what auditors and customers will ask for.

● 15–24

Clear gaps

The foundation is there, but important controls are missing. Prioritise MFA, access control, backup and incident handling first.

● 0–14

Significant work needed

Start with the quick wins that reduce the most risk: MFA everywhere, automatic updates, tested backups and same-day offboarding.

Quick wins that close several gaps at once

→ Turn on MFA for every user and every admin account

→ Manage all devices centrally: updates, encryption and screen lock enforced by policy

→ One identity for every app (single sign-on), so access is removed in one place

→ Test a restore from backup – and write down how you did it

Want a second pair of eyes?

PolarIT helps Danish businesses get NIS2-ready with one managed platform for identity, devices, MFA and access – plus the documentation to prove it.

Book a free NIS2 readiness chatpolarit.dk/nis2.html**Get a free external security check**polarit.dk/security-check.htmlJoseph Cunningham · Founder, PolarIT · +45 31 67 10 87 · Support@PolarIT.dk

This checklist is general guidance to help you assess your readiness. It is not legal advice and does not replace an assessment of your specific obligations under the Danish NIS2 law.