securenok®

WHITE PAPER

Cybersecurity for the drinking water supply in Norway

PREPARED BY:
SECURENOK® AS

See more. Fear less.

Cybersecurity challenges facing Norway's drinking water supply

Digitalization and increased automation have made water treatment and distribution systems more efficient, but also more vulnerable. As IT and OT converge, new risks emerge: production outages, contamination threats, regulatory penalties, and a loss of public trust.

As critical infrastructure, drinking water supply is subject to concrete requirements under the new Digital Security Act, which comes into force on 1 October 2025. This means cybersecurity can no longer be treated as an afterthought. It has to be built into day-to-day operations.

This document provides insight into the current threat landscape and shows how SNOK® can help water treatment facilities across Norwegian municipalities and inter-municipal companies (IKS) run more securely and reliably.

Tor Ommund Ljosland
Chief Sales Officer

Epost:
tol@securenok.com

Tlf:
+47 41 40 67 70

securenok®

Poor cybersecurity can have serious consequences

Even minor incidents in the water sector can have major consequences, affecting public health, safety, and trust alike:

Supply disruption

A brief interruption in water production can quickly affect tens of thousands of residents and critical services like hospitals, schools, and the fire brigade.

Contamination

Unauthorized access to control systems can lead to incorrect chemical dosing or tampering with treatment processes, posing a serious risk to public health.

Reputational damage

Public trust in the water supply is everything. An incident that puts water quality at risk can have lasting consequences for both the municipality and its residents.

Regulatory consequences

The new Digital Security Act requires water utilities to have reporting obligations, risk management procedures, and incident response plans in place. Failure to comply can result in sanctions and formal orders.

Why is the water sector being targeted?

Security not built in
Many control systems in water utilities were never designed with modern security features in mind. Things like updates, antivirus protection, and encryption often can't be applied without disrupting operations.

IT and security teams lack OT expertise
Most have a background in traditional IT security, but not the specialized knowledge and tools needed to protect industrial OT environments.

Limited visibility and monitoring
PLCs, SCADA systems, pumps, and sensors are often left out of conventional security setups, creating blind spots.

Weak network segmentation
Without a clear separation between IT and OT, an attack can spread rapidly across systems.

Geographic spread
Water treatment plants and pumping stations are often spread out and unmanned, making continuous monitoring and effective incident response a real challenge.

NRK

A real-world example from Norway: the Bremanger sabotage

In April 2025, hackers took control of the control system at a dam near Risevatnet in Bremanger, an infrastructure with many parallels to water treatment facilities. The valves were left open for nearly four hours, releasing up to 500 litres of water per second, before the attack was detected and stopped.

(NRK 13. august 2025).

securenok®

A legally required security system

Cybersecurity in the water sector is no longer optional. It is a legal requirement. As part of critical national infrastructure, water utilities are now covered by the Digital Security Act, which comes into force on 1 October 2025. The act is based on the EU's NIS1 directive and sets out clear requirements for how water treatment facilities and distribution systems must be protected.

The Digital Security Act: new obligations for water utilities

The new Digital Security Act introduces requirements that mean municipalities and inter-municipal companies must treat cybersecurity on the same level as physical security and emergency preparedness. Serious incidents must be reported to the authorities within 24 hours, and management is responsible for ensuring that a system is in place to identify and handle the risk of cyberattacks across their facilities.

The act also requires all organizations to have a continuity plan in place, including the ability to detect and respond to attacks, as well as recover if an attack succeeds. This means security work must be anchored at the executive level and cannot be left to ad hoc solutions.

IEC 62443: the industry standard for OT security

While the law sets the overall framework, IEC 62443 provides concrete guidance on how OT environments can be secured. The standard emphasizes robust network architecture and segmentation, strict access controls and authentication, continuous monitoring and logging, and procedures for updates and lifecycle management.
For water utilities, this means building a comprehensive and well-documented security architecture, not just implementing isolated measures.

ISO 27001: bridging IT and OT

Many municipalities already use security management frameworks like ISO 27001 to protect their IT systems and processes. The biggest challenge going forward is extending this framework to cover OT systems as well, so that the security of pumps, valves, and control systems in water treatment becomes a fully integrated part of the overall management system.

What this means for Norwegian water utilities

Municipalities and inter-municipal companies need to establish a structured, documented, and ongoing approach to cybersecurity. The Digital Security Act is based on NIS1, but the water sector also needs to prepare for an expansion to wastewater systems and even stricter requirements when NIS2 is expected to be implemented into Norwegian law in 2026. Without a well-functioning OT monitoring system like SNOK®, it will be difficult to meet legal requirements, maintain the necessary documentation, and respond quickly to unexpected incidents.

With continuous OT monitoring, water utilities gain full visibility, early warnings, and the confidence that both supply reliability and regulatory requirements can be met.


I·V·A·R
securenok

securenok®

Mapping the OT environment, active devices, and potential vulnerabilities at IVAR IKS

I·V·A·R

Customer profile

- Owned by 12 municipalities in Rogaland
- Supplies over 360,000 residents
- 8 water treatment facilities

Challenge

- Compliance with the Digital Security Act, including requirements for monitoring and reporting
- Complex infrastructure: 8 facilities of varying age, spread across a wide geographic area
- No active monitoring or up-to-date overview of the OT network and connected devices

Solution

- Security Status report delivered after 90 days of monitoring with SNOK sensors
- Full visibility into networks, devices, and data communication across production facilities
- Identification of critical security gaps with concrete short- and long-term actions
- A roadmap for continuous monitoring and compliance with IEC 62443 and NIS

"With a health check based on SNOK technology, we got full visibility into what is actually happening in our OT network. It gave us both greater confidence in day-to-day operations and a concrete tool for meeting new regulatory requirements."

I·V·A·R **Svein Roar**
Sikkerhetsrådgiver i IVAR IKS

securenok®

SNOK®: built for demanding OT environments

SNOK® Cybersecurity Monitoring System was developed specifically for industrial control systems, such as water treatment facilities, where traditional IT security solutions often fall short. It delivers continuous insight, early warnings, and real-time confidence in your operations.

SNOK® keeps you fully protected through:

Network sensors

Detects unusual traffic and unauthorized communication within the OT network.

Endpoint sensors

Protects critical devices such as control PCs, HMIs, and servers without disrupting operations.

API integrations

Connects OT monitoring to existing IT security solutions, giving the organization a single, unified security overview across both IT and OT.

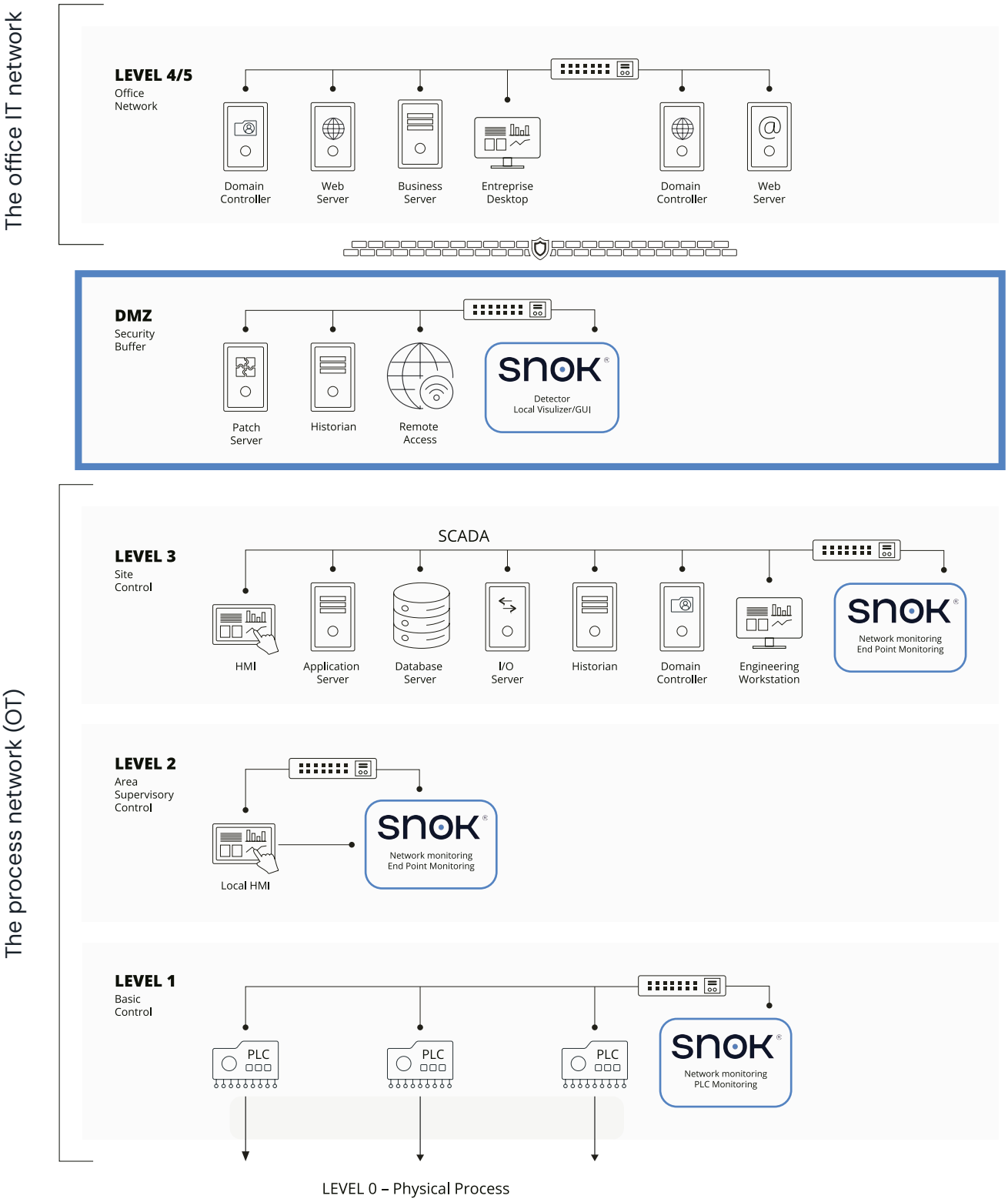
- Actionable security insights
- Compliance with IEC 62443 and NIS2
- Early detection of cyber threats
- Continuity of production

SNOK®

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY

Implementing SNOK®

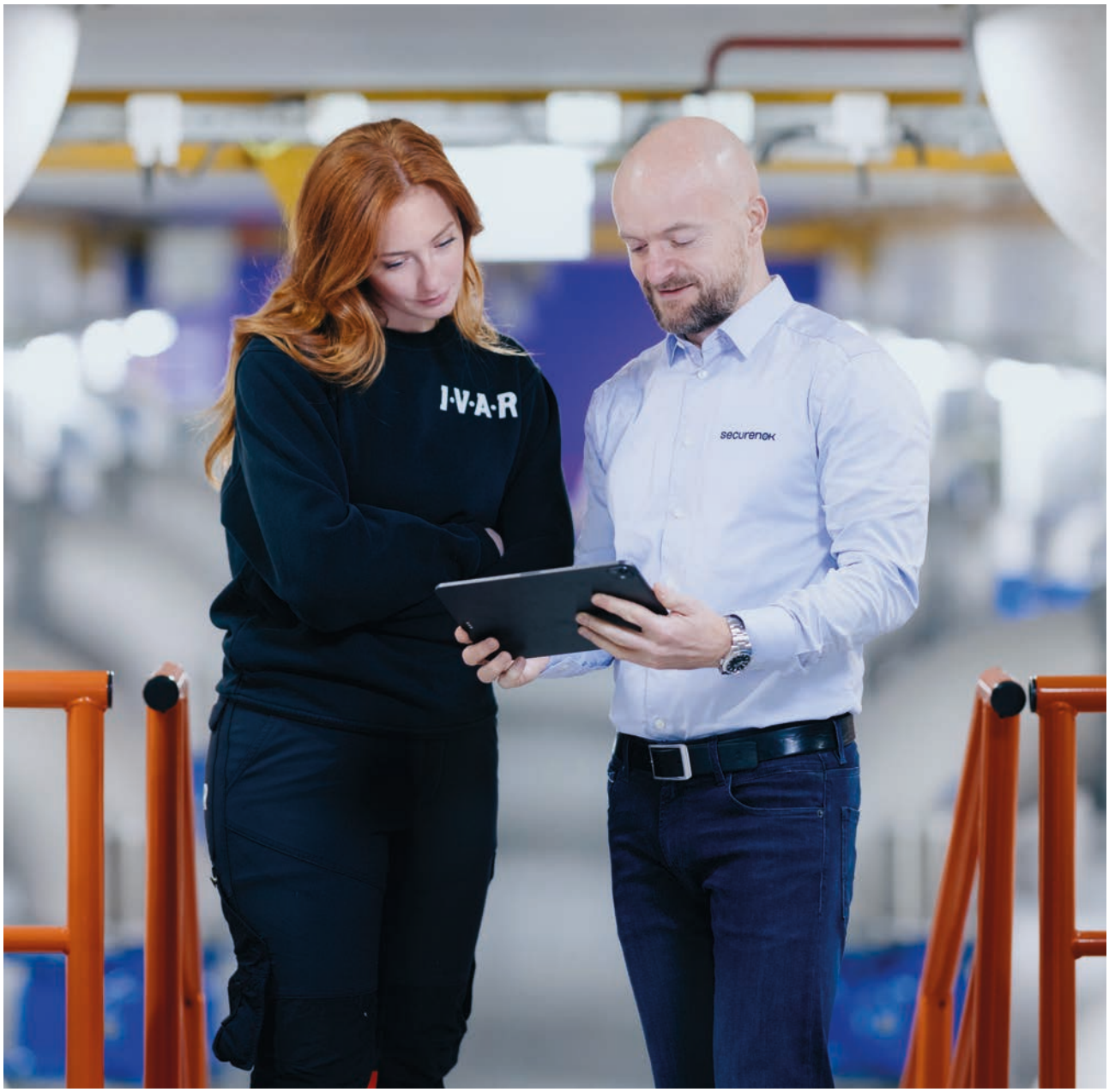


securenok®

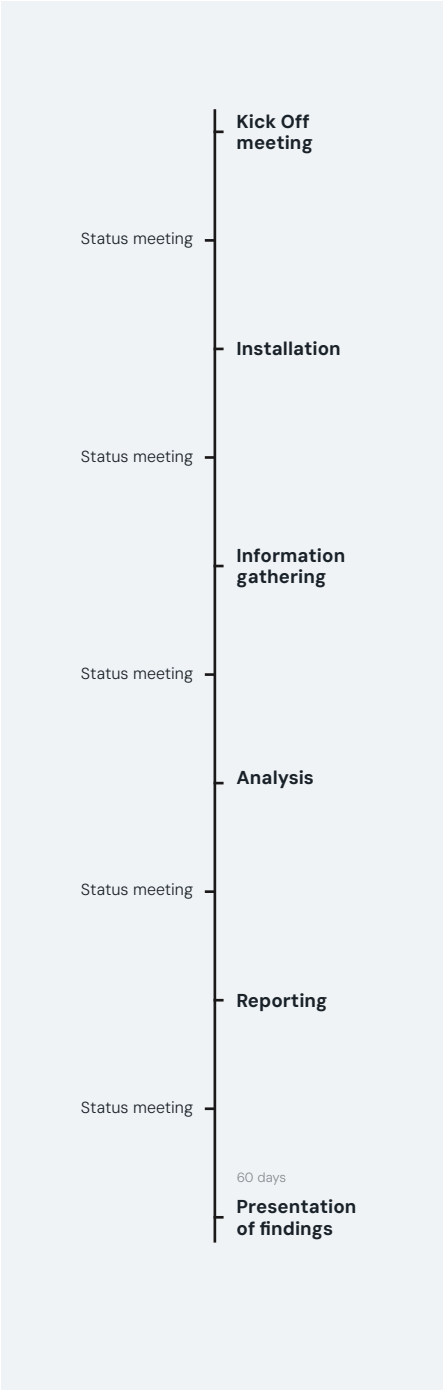
Best practices for a more secure water supply

Security is not just about technology. It requires solid processes and the right organizational setup:

- Real-time monitoring: Deploy sensors across the network and on critical devices.
- Secure endpoints: Remove unnecessary software and limit network access.
- Incident response plan: Develop and regularly test a plan for handling incidents.
- The right expertise: Work with OT specialists who understand the processes specific to the water sector.
- Segmentation: Separate IT and OT networks to contain the spread of an attack..



Implementation and timeline for security status with Securenok



Visibility

Full insight into OT assets and traffic

Risk

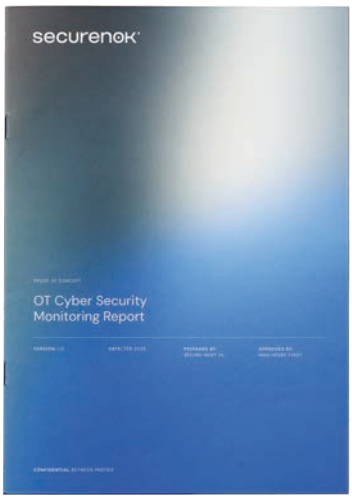
Uncovers weaknesses and unwanted behavior

Actions

Concrete, prioritized recommendations

Fixed price

60-day SNOK license and report included



securenok®

Want to know if your water and wastewater facilities meet today's security requirements?

We offer a security status assessment and practical advice to strengthen your preparedness, tailored to municipalities and inter-municipal companies.

Tor Ommund Ljosland
Chief Sales Officer

Epost:
tol@securenok.com

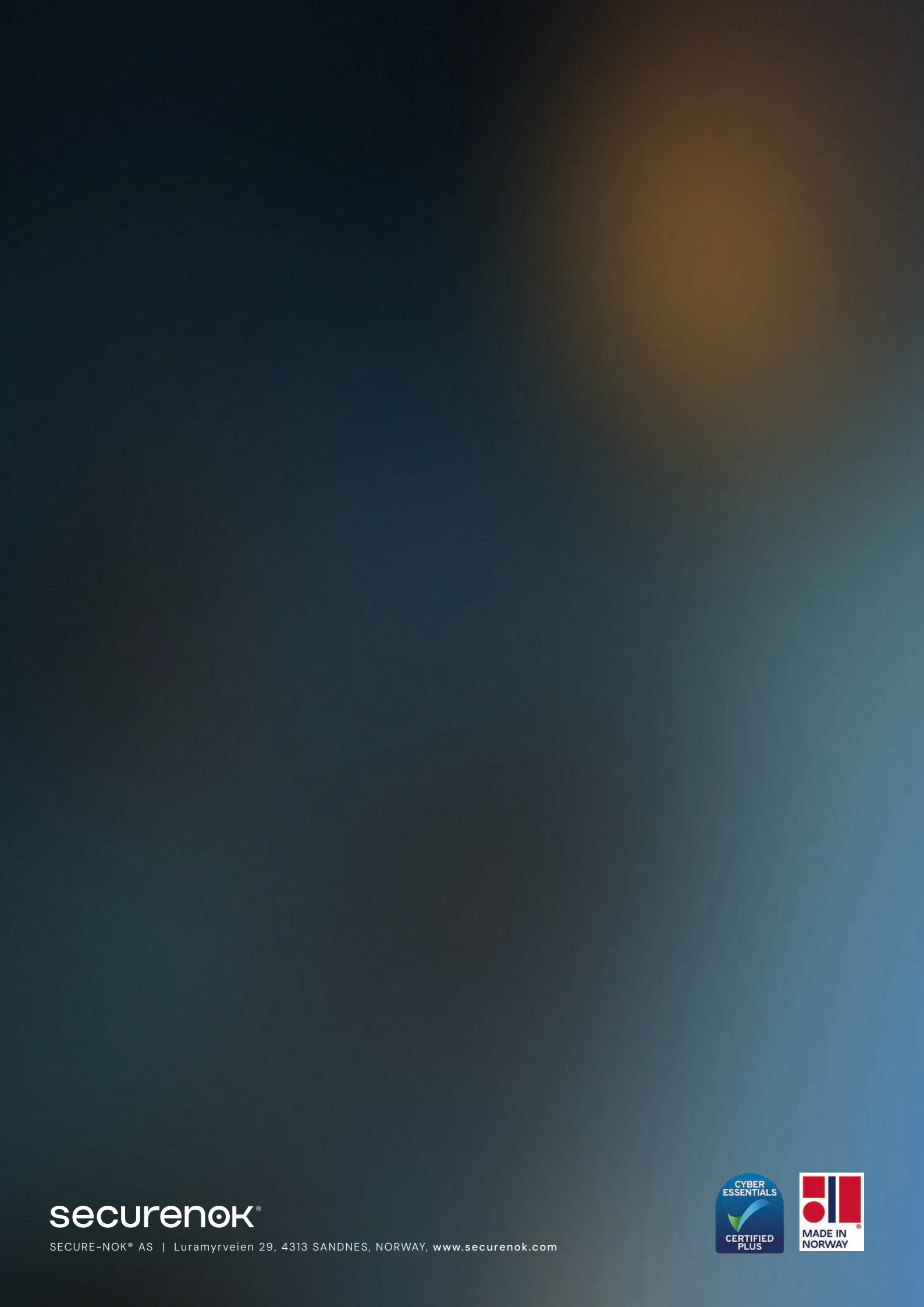
Tlf:
+47 41 40 67 70

Adil Lakrimi
Senior Sales Executive

Epost:
adl@securenok.com

Tlf:
+47 95 23 22 26

See more. Fear less.



securenok®

SECURE-NOK® AS | Luramyrveien 29, 4313 SANDNES, NORWAY, **www.securenok.com**

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY