Antura and NIS2 / the Swedish Cybersecurity Act

Antura works systematically with information security through a management system based on ISO 27001:2022, GDPR and the requirements of NIS2/the Swedish Cybersecurity Act. This work includes risk management, policies and procedures, secure development and operations, access control, encryption, monitoring, incident management, continuity planning, supplier management, training, as well as ongoing follow-up and audits. As a result, Antura has established processes and controls that support customers who need to assess suppliers based on the requirements of NIS2 and the Swedish Cybersecurity Act.

What NIS2 and the Swedish Cybersecurity Act mean

NIS2 is the EU regulation aimed at achieving a high common level of cybersecurity across the Union. In Sweden, the directive has been implemented through the Swedish Cybersecurity Act, which entered into force on 15 January 2026. The regulation applies to operators within designated sectors and requires a systematic and risk-based approach to cybersecurity. For organisations that are covered, the central obligations are to:

1. assess whether the organisation is covered and register in accordance with applicable rules,
2. implement appropriate and proportionate technical, operational and organisational security measures,
3. report significant incidents in accordance with the requirements of the regulation.

Antura's security work in brief

Antura's information security work is an integrated part of how the company governs, develops and delivers its services. The work covers the entire organisation, from the Board of Directors and management to development, operations, support and customer-facing functions.

Governance and management

Information security management system based on ISO 27001:2022, GDPR and the requirements of NIS2/the Swedish Cybersecurity Act. The Board of Directors, CEO and CISO have clearly defined roles.

Risk-based approach

Regular risk assessments based on confidentiality, integrity and availability. Security measures are documented and followed up through the Statement of Applicability.

Secure development and operations

Security by design and security by default throughout the product lifecycle. Separate development and production environments, approved versions, logging, monitoring and encryption.

Access and data protection

The principle of least privilege, support for external authentication and procedures for personal data management, deletion, pseudonymisation, as well as privacy by design/default.

Incident management and continuity

Documented procedures for the classification, handling and reporting of incidents, as well as continuity planning with identified scenarios, exercises and updates.

Follow-up and improvement

KPIs, regular third-party penetration tests, internal audits, external audits and ongoing reporting from the CISO to management.