CYBERSECURITY COMPLIANCE SHEET

NIS2 is here and Johnson Controls can help you be ready

What is NIS2?

The European Network and Information Security Directive (NIS2) outlines cybersecurity requirements for enterprises operating in the European Union (EU). The purpose of NIS2 is to improve the overall cybersecurity posture of the EU by requiring enterprises in key sectors to adopt a broad range of enhanced cybersecurity measures for their organizations. NIS2 builds on the initial NIS Directive from 2016 but includes stricter requirements, an expanded scope of enterprises and sectors that must comply, and increased penalties for noncompliance.

How can you prepare for NIS2?

Preparing for NIS2 compliance involves several key steps to ensure your organization meets NIS2 requirements by the various deadlines. One of the key requirements of NIS2 is the adoption of appropriate vendor and supply chain security measures, including ensuring that suppliers develop products with cybersecurity at the forefront.

How can Johnson Controls Security Products help you comply with NIS2?

Johnson Controls' Security Products can help businesses in the EU comply with the NIS2 Directive by addressing several critical cybersecurity and operational requirements. Here is how:

Enhanced Physical and Cybersecurity integration

Johnson Controls' integrated solutions for intrusion, access control, and video surveillance stand out for their robust security features that cater to both physical and cybersecurity systems. By integrating these tools, businesses can effectively monitor, control, and restrict access to critical infrastructure, helping to satisfy NIS2's risk management and security measures requirements.

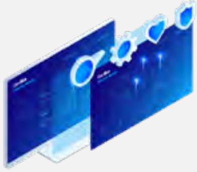
Compliance Reporting and Risk Assessment

NIS2 requires businesses to conduct regular risk assessments and report on their cybersecurity posture. Johnson Controls' platforms can be customized to generate compliance reports, track user activities, and provide auditable logs for regulatory bodies, which simplifies the process of maintaining compliance and demonstrating adherence to NIS2 standards.

About Johnson Controls Trust Center

Johnson Controls promotes a collaborative approach to cybersecurity and data privacy management. Our dedicated internal teams partner with each other to ensure our actions are tightly coordinated. Together, we deliver on the Johnson Controls commitment to security, privacy, and ethics. Our success is led by following security and data privacy practices aimed at addressing security holistically for our customers, products and enterprise. Security is designed into all Johnson Controls products, hardware, hosted services and software. Gain peace of mind with cyber-resilient systems and solutions tailored to your business needs.

Learn more here



Scalable and Modular Solutions for Critical Infrastructure

Johnson Controls offers scalable solutions tailored to various sectors, including healthcare, finance, transportation, and utilities, which are often categorized as critical infrastructure under NIS2. Our security products can be adapted to meet the specific needs of these sectors, facilitating businesses compliance across all verticals.

By leveraging Johnson Controls' integrated security systems, businesses can help protect their networks, prevent unauthorized access, and comply with NIS2 across physical and digital infrastructure.

Some security features may require optional configuration and licensing or maybe limited to specific product configuration.

Johnson Controls Product Cybersecurity Program

Cybersecurity is a high priority for Johnson Controls and is managed by our dedicated Global Information Security (GIS)) organization. We follow security practices that take into account cybersecurity throughout the lifecycle of the solutions we develop, support, and service. Our practices are aimed at addressing security holistically for our customers, products, and enterprises. Johnson Controls' ISASecure certified software security development practices support the NIS2 Directive requirements.

Johnson Controls' Secure Software Development Life-cycle Assurance (SDLA) program is certified to ISA/IEC 62443-4-1 secure development life cycle requirements, including employee training, for all globally developed solutions as policies and standards require.

Secure-by-Design - Products developed with security and privacy requirements in mind (e.g., encryption, Multi-Factor Authentication (MFA), Role Based Access Controls (RBAC), threat modeling and testing through release.

Security testing - Our Secure Development Lifecycle Assurance (SDLA) process requires that solutions undergo security testing before release. Testing is continued throughout the product lifecycle and may include peer code reviews, vulnerability scans, fuzz testing, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and penetration testing.
Security audit and certifications - Risk management audits are conducted for Johnson Controls managed environments and practices, including those resulting in SOC audits reports and ISO 27001 and ISASecure certifications.

Security governance - A dedicated Global Cybersecurity organization provides oversight of Johnson Controls' product security.

Incident handling and reporting - An incident response team follows established plans during an incident and will provide timely notification of incidents to impacted customers.

Supply chain management - Third-party suppliers are assessed for compliance with security requirements. Only suppliers who conform may be used as a source for product in-scope components and services.

CVE Numbering Authority (CNA) - Johnson Controls provides coordinated disclosure, Product Security Advisories (PSAs) and Common Vulnerability and Exposures (CVE) public disclosures as a CNA.

Vulnerability management program - Findings are remediated according to risk level using the Common Vulnerability Scoring Systems (CVSS) for vulnerability assessment.

ISASecure® Security Development Lifecycle Assurance (SDLA) certified All Johnson Controls global development locations comply with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customer commitment to provide cyber-resilient solutions that follow best-in-class industry practices.

ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

Please note that this document is for customer guidance purposes only, is not legal advice and is subject to changes from time to time due to modifications of our solutions. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to deliver smart building solutions.

To learn more, please visit our website at **www.johnsoncontrols.com/**trust-center or contact us at TrustCenter**@jci.com**.

Visit **johnsoncontrols.com** or follow us **@johnsoncontrols**

© 2024 Johnson Controls. All rights reserved.