

# Cybersecurity Requirements for Third Parties

For Suppliers, Partners and Service providers



# Mandatory provisions for all Third Parties

---

## 1. Compliance with Security and Regulatory Standards

The Third Party agrees to comply with applicable regulatory standards and certification, such as NIS2, DORA, PCI DSS or any other relevant regulations. The Third Party commits to provide, upon request, the necessary certifications or audit reports to prove this compliance.

## 2. Security Awareness and Training

The Third Party shall provide regular and up to date information security training to its employees and ensure that only personnel informed of and compliant with security-related policies and procedures required by Nexans are assigned.

## 3. Data Protection and Confidentiality Measures

The Third Party agrees to comply with applicable data protection laws and regulations (such as GDPR), implementing technical and organizational measures to ensure the confidentiality and security of personal data, including encryption of communications and databases.

The Third Party must implement measures to protect Nexans's information notably sensitive data or confidential information, including access rights management to this information and technical protections to prevent unauthorized use or disclosure of confidential information, including encryption of communications and databases.

## 4. Threat Detection and Incident Management

The Third Party must deploy systems to detect internal and external threats, and to protect systems against cyberattacks.

In the event of a security incident that may impact Nexans assets, the Third Party must notify Nexans within 24 hours of the discovery and provide all necessary cooperation to manage the incident, including detailed information on the incident and the actions taken to resolve it.

## 5. Supply Chain Risk Management

The Third Party must ensure that all third parties, subcontractors, and partners involved in providing services meet the appropriate security requirements, implementing controls to manage risks associated with the supply chain.

## 6. Provision of Evidence

The Third Party shall provide any necessary evidence demonstrating compliance with contractual, security, and regulatory requirements upon Nexans's request, within a reasonable timeframe.

## 7. Non-compliance and Cybersecurity Breach liability

Failure to comply with the Nexans's cybersecurity obligations constitutes a material breach of this Agreement. In such cases, the Nexans reserves the right to: (a) terminate the contract immediately without penalty, (b) seek full financial compensation for all damages, including legal and regulatory costs and enforce remedial actions, such as enhanced security controls, audits, or access restrictions.

All corrective measures shall be at the Third Party's sole expense.

The Third Party shall be fully liable for any security breach affecting Nexans' data, systems, or services, including penalties and compensation for damages.

# Mandatory provisions for Indirect Third Party with access to Nexans IS, Direct Third Party, IT / OT Third Party

---

## 8. Information Security Management and Cybersecurity Governance

The Third Party shall have an implemented and maintained Information Security Management System (ISMS) aligned with international standards such as ISO 27001 & 27002, IEC 62443 and NIST cybersecurity framework when applicable).

The Third Party must define clear cybersecurity governance, including the designation of a security officer, risk management processes, and the implementation of control mechanisms to ensure that security objectives are met and maintained.

## 9. Security Risk Assessment

The Third Party must conduct regular cybersecurity risk assessments for their systems, solutions or services, and implement mitigation plans for identified risks to protect physical and logical processes against potential threats.

## 10. Business Continuity and Disaster Recovery Plan (Service Availability)

The Third Party must establish a business continuity (BCP) and disaster recovery plan (DRP) to ensure the availability of critical services in the event of a major incident, with regular tests to validate the effectiveness of these plans.

## 11. Audit, Compliance and Contract Termination

Nexans reserves the right to conduct scheduled audits of the Third Party's security and compliance practices to ensure adherence to contractual obligations and applicable security standards. The Third Party agrees to provide reasonable access to

its systems, processes, and documents related to data management and security and fully cooperate during any audit. In case of non-compliance, the Third Party will take necessary measures to remedy the discrepancies within a reasonable timeframe.

Upon the contract's termination, the Third Party must guarantee service reversibility, including the secure return of data, irreversible destruction (if applicable), and the ability to recover or to transfer services to Nexans or another Third Party without compromising security or confidentiality.

# Definitions

---

<b>IT/OT Third Parties</b>	Means notably manufacturers, system Integrators, software and hardware vendors (even upstream libraries or firmware), cloud providers (SaaS, PaaS, IaaS, NaaS...) / hosting, OT vendors (like SCADA systems), remote service providers or third-party Managed Service Providers (MSP), code repositories / CI/CD pipelines (e.g. GitHub, Jenkins).
<b>Direct Third Party</b>	Means suppliers, that are not considered as IT/OT Third Parties, that don't provide digital services or tech BUT they are part of the operational resilience of the NIS2-regulated entity (or simply critical for the entity) and notably critical raw material supplier (notably a disruption can highly affect ability to deliver critical infrastructure), critical Chemical suppliers (notably affects cable safety, durability, and compliance), energy suppliers (notably outage stops production)
<b>Indirect Third Party having access to Nexans IS</b>	Means supplier that are not considered as IT/OT Third Parties BUT have access to NIS2 Entity IS and or critical facilities (ie: insider threat risk) and notably non-digital service suppliers but having physical access to critical facilities, non-digital service suppliers but having physical access to HQ and office and non IT 3rd party (Consulting firm, partners...) having access to Nexans IS (independently if it remotely or not).
<b>Third Party</b>	Means IT/OT Third Parties, Direct Third Party, Indirect Third Party having access to Nexans IS and non digital or physical supply chains - unless these suppliers have a direct impact on network and information systems and notably office supplies, catering services, non critical raw materials, standard logistics etc...