# NIS-2 Compliance Checklistfor Kautschuk Group Suppliers and Partners

This supplier checklist is designed to evaluate and document the cybersecurity posture of Kautschuk Group supply chain partners, ensuring alignment with NIS‑2 obligations. It aids in identifying whether our partners have established robust cybersecurity policies, risk management processes, and technical controls, as required by our organization's compliance framework.

| **Checklist Item** | **Question/Requirement** | **Response**  | **Comments/Notes** |
| --- | --- | --- | --- |
| **Security Governance & Leadership** | Does your organization have a documented cybersecurity policy, appointed CISO (or equivalent), and board-level oversight of cybersecurity? | ☐ yes☐ no |  |
| **Cybersecurity Management System (ISMS)** | Do you maintain an ISMS (e.g., ISO 27001 certified or equivalent) and conduct regular risk assessments covering IT and, if applicable, OT systems? | ☐ yes☐ no |  |
| **Risk Management Process** | Do you have a formalized risk assessment process that identifies, documents, and mitigates cybersecurity risks (including supply chain risks)? | ☐ yes☐ no |  |
| **Incident Response Plan (IRP)** | Is there a documented Incident Response Plan that includes roles, responsibilities, and procedures for prompt incident detection, containment, and reporting? | ☐ yes☐ no |  |
| **Network Segmentation & Access Controls** | Do you implement network segmentation (e.g., separate IT from OT environments) and enforce strict access controls (including least privilege and MFA)? | ☐ yes☐ no |  |
| **Vulnerability Management & Patching** | Are systems regularly scanned for vulnerabilities and patched/upgraded promptly, with documented processes in place? | ☐ yes☐ no |  |
| **Encryption & Data Protection** | Is sensitive data encrypted both in transit and at rest, with secure key management practices in place? | ☐ yes☐ no |  |
| **Secure Configuration & Hardening** | Do you use documented, secure baseline configurations for hardware, software, and network devices (including hardening of operating systems and applications)? | ☐ yes☐ no |  |
| **Employee Training & Awareness** | Are employees trained regularly on cybersecurity best practices, including phishing awareness and secure data handling? | ☐ yes☐ no |  |
| **Third-Party/Subcontractor Management** | Are there contractual provisions and verification measures in place to ensure that any subcontractors or downstream suppliers meet equivalent cybersecurity standards? | ☐ yes☐ no |  |
| **Compliance & Audit Readiness** | Can you provide evidence of regulatory compliance (e.g., audit reports, certifications) and do you routinely review and update your cybersecurity measures? | ☐ yes☐ no |  |

Thank you for taking the time to complete our cybersecurity supplier checklist. Your prompt and thoughtful responses play a vital role in maintaining a resilient and secure supply chain, ensuring that we all meet the necessary regulatory and security standards. We appreciate your cooperation and commitment to upholding high cybersecurity practices.

For questions, comments, and further support, please contact the Kautschuk Group *CISO* at it@kautschuk.com.