Supplier Security Principles

First publication	: August 2022
Current publication	: November 2025
Version	: V3.0
Document type	: Policy
Scope	: Suppliers and their ecosystem
Confidentiality Status	: Public

Life Is On Schneider Electric

Our Vision



"Cybersecurity is not an option - these Supplier Security Principles outline the fundamental actions and collaboration needed to deliver strong cybersecurity throughout the supplier ecosystem to protect our mutual interests and our customers."

Ard Verboon

Chief Procurement Officer



“While extended supplier relationships have introduced new cyber risks that threaten supply chain stability, Schneider Electric is committed to being as collaborative as possible with its suppliers to raise the bar on cyber defense.”

Christophe Blassiau

SVP Global Chief Information security Officer and Chief Product Security Officer

Why are Supplier Security Principles needed?

Schneider Electric is focused on digitalizing its core processes, customer solutions, and supporting technologies. This transformation is expanding our digital footprint and cybersecurity risk. Similarly, our suppliers' digital transformations are increasing their attack surface and cybersecurity risk.

We are dedicated to transparent collaboration with our suppliers to safeguard our digital ecosystem and the industry as a whole. Our Trust Charter drives our interactions with stakeholders, customers, shareholders, employees, and communities in a meaningful and inclusive manner. This applies to everyone at Schneider Electric and our subsidiaries, including our suppliers.

Our direct procurement suppliers provide electrical products, components, electronic manufacturing services, brand labeling, and solutions, while our indirect suppliers offer IT, telecommunications, and professional services. Our goal is to collaborate with all suppliers to mitigate threats that could harm customers, disrupt business continuity, breach private and sensitive information compliance, or result in intellectual property theft.

What is Schneider's Security Management policy for Suppliers?

Schneider Electric's Supplier Security Management policy encompasses a structured approach to Cybersecurity, AI and Data Protection throughout procurement processes and lifecycle management based on four fundamental principles:

1) Implement Cybersecurity and Data Privacy/Protection measures throughout procurement processes and lifecycle management

2) Adopt a risk-based approach in supplier relationships

3) Ensure compliance adherence

4) Integrate Trustworthy Artificial Intelligence (AI) practices to promote responsible and secure use of AI

We collaborate closely with all our suppliers to ensure they adhere to these principles, recognize any security gaps, and exhibit an elevated level of cyber resilience to Schneider Electric, as well as their other customers and stakeholders.

Our Core Principles for the Supplier Ecosystem

Working with Schneider Electric to adopt and meet the high standards established in our core principles is mutually beneficial.

1. Apply Cybersecurity, Data Protection and Trustworthy AI Measures to the Procurement Process and Lifecycle Management

As part of the Supplier Security Management Policy, we apply mature, consistent, repeatable, and effective security measures for cybersecurity and data privacy to all our procurement processes and lifecycle management.

This ensures Cybersecurity Data Privacy, and trustworthy AI principles are constantly considered and addressed as essential elements in every phase of procurement. We achieve this by assuring that:

- Cybersecurity, Data Protection and trustworthy AI are built-in requirements of the procurement processes.
- All procurement contracts shall stipulate and contain clear and precise clauses that enforce continual compliance with Cybersecurity, Data Protection/Privacy and AI governance requirements.

Cybersecurity, Data Protection and AI obligations shall be continuously reviewed and optimized to keep up with the evolving threats.

2. Embrace a Risk-Based Approach to Supplier Engagements

Schneider Electric takes a risk-based approach that helps us assess the security posture of our suppliers. This approach delivers a more enriching, collaborative, and valuable outcome for Schneider Electric, our suppliers, and our customers.

In assessing our suppliers' security posture, we classify them according to the level of criticality of their risks. These rankings help us efficiently and accurately mitigate the cybersecurity threats that suppliers may pose to us and all our stakeholders, including our customers.

Based on the rankings as seen below in Figure 1, we collaboratively tailor mitigation plans that are coupled with the monitoring of supplier performance through rating tools and the review of the legal requirements assigned to each supplier category. This approach aims to –provide our customers trustworthy, secure, privacy-protective, and resilient products, systems, and services.

Cybersecurity, Data Protection and AI Risk Profile and Mitigation Activities		
Risk Profile	**Type of Supplier**	**Mitigation Plans and Legal Requirements**
Critical	Partners and co-innovation suppliers who provide worldwide services	• Cybersecurity partnerships • Real-time monitoring • Cybersecurity and Data Privacy audits • Cybersecurity Terms & Conditions , Data Privacy (DPA)and Artificial Intelligence Addendums that provide additional terms about security provided by the supplier
High	Suppliers with high business impact who have access to confidential and restricted data	• Real-time monitoring • Cybersecurity, AI and Data Privacy audits as applicable • Cybersecurity Terms & Conditions ,Data Privacy and Artificial Intelligence Addendums that provide additional terms about security provided by the supplier
Moderate	Suppliers with regulatory impact or who conduct important business	• Cybersecurity, AI and Data Privacy audits as applicable • Cybersecurity Minimum Requirements Terms & Conditions with specific requirements if needed
Low	Suppliers with low-risk purchases	• Cybersecurity Minimum Requirements Terms &Conditions

Figure 1: Risk Profile Identification and Mitigation Activities for Suppliers

This process also helps our suppliers better understand gaps in their own security posture and, ultimately, demonstrate their cybersecurity maturity to their many other customers and stakeholders.

3. Ensure Adherence to Compliance

Schneider Electric is committed to upholding compliance with all applicable laws, executive orders, regulations, directives, and standards at global, regional, and local levels. Consequently, we expect our suppliers to adhere to these standards in all their interactions with us. Our business success relies on the continuous trust our customers and stakeholders have in the security and reliability of our products, systems, and services, as well as our commitment to protecting data privacy.

Schneider Electric maintains this confidence by regularly assessing our suppliers' compliance. These assessments occur throughout our relationship, from early sourcing stages to security due diligence, and continue periodically throughout our collaboration.

As part of our ongoing commitment to securing the digital ecosystem, our Supplier Security Management Policy mandates that all procurement contracts with suppliers classified as critical or high risk must include the right for Schneider Electric to audit them and verify the effectiveness and coverage of their cybersecurity and data privacy controls. We urge all our suppliers to ensure their compliance with these requirements and to be prepared for regular audits to demonstrate their commitment to cybersecurity and data privacy. Together, we can build a strong partnership that enhances our collective security posture while aligning to business objectives.