Third-Party Security Principles

First publication : September 2022
Current publication : September 2022
Version : V1
Document type : Policy
Scope : Suppliers and ecosystem
Confidentiality Status : Public

Life Is On Schneider Electric

Our Vision

"A Schneider Electric partner is a cybersecure partner."

Daniel W. Bartel

Chief Procurement Officer

"While extended third-party 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 Cybersecurity & Global CISO

Global cybersecurity risks are always evolving, and as Schneider Electric digitizes our core business processes, customer solutions, and supporting technologies, our digital landscape and risk exposure grows and evolves as well. Our third-party suppliers are also digitalizing, leading to an even larger attack surface, and thus, to more cyber vulnerabilities.

Schneider Electric's Trust Charter is driven by a trust that powers all our interactions with stakeholders and our relationships with customers, shareholders, employees, and the communities we serve in a meaningful, inclusive, and positive way. The Trust Charter applies to everyone working at Schneider Electric or any of our subsidiaries and includes our third-party suppliers.

We are committed to collaborating with our suppliers in an open, close, and transparent manner, which we believe is a critical step towards safeguarding our digital ecosystem as well as the industry at large. Our direct procurement suppliers interact with us to provide electronic and electrical products and components as well as electronic manufacturing services, brand labelling, and solutions. Indirect third parties supply us with IT, telecommunications, and professional services. Our aim is to collaborate with all of them to reduce any threats that may cause damage our customers, interrupt business continuity, violate compliance of private and sensitive information, or lead to theft of our intellectual property.

To achieve this goal, Schneider Electric has established a Third-Party Security Management Policy, which is built upon three core principles:

1. Apply cybersecurity and privacy measures to procurement processes and lifecycle management.
2. Embrace a risk-based approach in third-party relationships.
3. Ensure adherence to compliance.

We work closely with all our suppliers to assure they embrace these principles, identify gaps in their own security posture, and demonstrate a new level of cyber resilience to Schneider Electric, as well as to their other customers and stakeholders.

Our Core Principles for the Supplier Ecosystem

We are confident that by working with us to adopt and meet the highest standards established in our core principles, our third-party suppliers can realize countless business benefits and become more secure organizations.

1. Apply Cybersecurity and Privacy Measures to the Procurement Process and Lifecycle Management

As part of the Third-Party Security Management Policy, we apply mature, consistent, repeatable, and effective security measures for cybersecurity and privacy to all of our procurement processes and lifecycle management. This ensures cybersecurity and privacy are constantly considered and addressed as essential elements in every phase of procurement. We achieve this by assuring that:

- Cybersecurity and privacy 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 and privacy requirements.
- Security and privacy obligations shall be continuously reviewed and optimized to keep up with the evolving threats.

2. Embrace a Risk-Based Approach to Third-Party 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 third parties, 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 third parties 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 assures that we are providing our customers trustworthy, secure, privacy-protective, and resilient products, systems, and services.

Cybersecurity Risk Classification and Mitigation Activities		
Risk Level	**Type of Third-Party Supplier**	**Mitigation Plans and Legal Requirements**
Critical	Partners and co-innovation suppliers who provide worldwide services	• Cybersecurity partnerships • Real-time monitoring • Cyber assessments • Cyber Terms & Conditions that provide additional terms in regard to security provided by the supplier
High	Suppliers with high business impact who have access to confidential and restricted data	• Real-time monitoring • Cyber assessments • Cyber Terms & Conditions that provide additional terms in regard to security provided by the supplier
Moderate	Suppliers with regulatory impact or who conduct important business	General Terms & Conditions with specific requirements if needed
Low	Suppliers with low-risk purchases	General Terms & Conditions

Figure 1: Risk Classification and Mitigation Activities for Third-Party Suppliers

This process also helps our third parties 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 supports and champions compliance with applicable laws, executive orders, regulations, directives, and standards on a global, regional, and local level. Therefore, as a basic principle, we expect our third-party suppliers similarly in all interactions with us.

Our business success is tied directly to the consistent and ongoing confidence our customers and other stakeholders have in the security and trustworthiness of our products, systems, and services, as well our ability to protect data privacy.

Schneider Electric is only able to maintain this confidence by regularly assessing the compliance of our third parties. Such assessments take place throughout our relationship with them, from early sourcing stages to security due diligence, and periodically throughout the duration of our collaboration.

As a part of our ongoing commitment to securing the digital ecosystem, our Third-Party Security Management Policy requires all procurement contracts for suppliers with a classification of critical or high risk to reserve the right for Schneider Electric to audit them and attest to the effectiveness and coverage of their security and privacy controls.

Conclusion

Schneider Electric is committed to continual collaboration with our suppliers as we safeguard our relationships with our customers, stakeholders, and other third parties. These core principles embody our vision for how we protect and secure all of our interactions and we appreciate the ongoing commitment from our suppliers.