Third-Party Security Principles

First publication : August 2020
Current publication : August 2020
Version : V.1
Document type : External communication
Scope : Suppliers and ecosystem

Life Is On Schneider Electric

Our Vision

"A Schneider partner is a cybersecure partner."

Daniel W. Bartel,
Chief Procurement Office

"Securing our perimeter, our offerings and our services relies on securing our sourcing ecosystem."

Christophe Blassiau,
Chief Information Security

The ongoing trend towards digital transformation continues to make our world a much smaller place. Because almost everything and everyone is connected, we have all effectively become part of a global digital ecosystem, where the choices we make both affect and are influenced by the choices of others.

This digital ecosystem ensures we can live our lives when, where, how and with whom we want. More importantly, however, it is the lifeblood of the global digital supply chain and the heartbeat of the global digital economy. But it is only as effective, useful and rewarding as the trust its members have in it.

At Schneider Electric, forging and ensuring trust in the digital ecosystem is not just a technology issue: It is an urgent strategic imperative for all our stakeholders, as well as industry at large. This is especially true for the essential businesses our world leaders rely on to safeguard global supply.

Schneider Electric takes this responsibility seriously. Our commitment to Life is On begins with our commitment to ensuring trust in the digital ecosystem. That is why cybersecurity it is at the core of our Principles of Responsibilities and built into everything we do. As the global leader in energy management, we believe access to energy and digital is a basic human right. By reducing the risks that threaten the global supply chain, we are leading the fight to protect and strengthen the digital economy so we can all have trust in, contribute to and benefit from the digital ecosystem.

To achieve our vision, we frequently rely on trusted third parties to help us secure and protect the digital ecosystem. Through them, we are able to reach our strategic objectives and realize better business performance. But these relationships also introduce new business risks, including critical cybersecurity risks.

To mitigate these risks, Schneider Electric strives to collaborate with suppliers who share our values and vision. As essential members of our digital community, we hold them to the highest possible standard when it comes to ensuring the security of our supply chain. This is consistent with our Principles of Responsibility, which resolve us to provide our customers with the secure products, systems and services they need, while protecting the privacy of their and all our stakeholders' data.

Therefore we have established a Third-Party Security Management Policy, built on three Core Principles. Our goal is to collaborate with our suppliers, both to ensure their compliance with this policy and to cascade our guidelines to their own vendors and service providers. Not only will this enable them to better navigate our stringent procurement and quality assurance processes, it will help them better understand gaps in their own security posture and, ultimately, demonstrate their cyber resilience to their many other customers and stakeholders.

We are confident that by working with us to adopt and meet the high standards established within our Policy, our trusted third-party suppliers will realize countless business benefits. But more importantly, by building on the Core Principles established within it, together we can collectively reduce and even eliminate the cyber risks that threaten the global digital ecosystem.

Our Core Principles

1. Security and Privacy are Essential to the Procurement Process and Lifecycle

Schneider Electric's Third-Party Security Management Policy applies mature, consistent, repeatable and effective measures, built on sound precepts, to ensure cybersecurity and privacy are constantly considered and addressed as essential elements in every phase of the relationship's lifecycle. These precepts include:

- 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. Risk-Based Approach

Schneider Electric takes a risk-based approach that guides our third-party acceptance/rejection decision-making process and helps efficiently and accurately mitigate cybersecurity threats third parties pose to us and all our stakeholders, especially our customers.

A Core Principle of our Third-Party Security Management Policy, this risk-based approach improves how we assess the security posture of our third parties. By applying risk-measurement and ratings tools and other known, trusted methodologies, we are better able to identify and rank our third-party relationships by risk criticality.

The approach ensures an accurate appreciation of risk, helps establish the measures third parties and third-party candidates must take to mitigate their risks before entering an agreement with Schneider Electric and establishes regular performance monitoring.

Overall, it delivers a more enriching, collaborative and valuable outcome for Schneider Electric, our third parties and our customers. It allows us to tailor mitigation plans and scale efforts and resources that ensure we are providing our customers trustworthy, secure, privacy-protective and resilient products, systems and services. But it 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. Compliance

Schneider Electric supports and champions compliance with applicable laws, executive orders, regulations, directives and standards. Therefore, as a basic principle, we expect our third parties' continuous compliance as well.

A key element of our historical success is the assurance our customers and other stakeholders consistently have in the security and trustworthiness of our products, systems and services, as well as their confidence in our ability and commitment to protecting the privacy of their data.

Schneider Electric is only able to maintain stakeholder confidence by regularly assessing the compliance of our third parties. Such assessments take place throughout the third-party relationship, from early sourcing stages, to security due-diligence and periodically throughout the duration of a collaborative relationship.

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