Cyber Badge Principles

First publication : November 2020
Current publication : April 2022
Version : V.2
Document type : External communication
Scope : Customers & eco-system

Life Is On Schneider Electric

Our Vision

"Cybersecurity is a top business priority for Schneider Electric. This is especially true of our customer-facing representatives, who must always be extra vigilant against cyber risks."

Christophe Campagne
Senior VP Project Execution

"Deploying the Cyber Badge is an important step to strengthening customer trust, especially within the industrial manufacturing sector, where OT security has become crucial to global supply."

Nathalie Marcotte
Senior VP Process Automation

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 Trust Charter, Schneider Electric's Code of Conduct 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 our customers' people, assets and operations, 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 deploy highly skilled experts to help us secure and protect our customers' people, assets—including their data—and operations. We refer to these experts as Customer Facing Populations (CFP's), and through them, we are better able to reach our strategic objectives and help our customers realize better business performance. But these relationships also introduce new business risks, including critical cybersecurity risks.

Customer Facing Populations include Field Services Representative and Technicians, Project Managers for systems and solutions, remote and on-site support teams, solution commissioning teams, software integration teams, and the like. The Cyber Badge initiative was launched in 2019 and currently involves over 20 000 Customer Facing employees. Most of our CFP's work at customer sites; others interact with customers or access customer data and installations via secured remote connections.

To ensure our Customer Facing Populations are able to meet customer demands and expectations, as well as to work in diverse IT and OT environments, they must be protected through consistent cybersecurity measures. This includes a robust mix of technology, training and controls. The objectives are twofold. First, we must always ensure Schneider Electric CFP's and the devices they use across multiple customer organizations will not become the vector of a cybersecurity incident or attack. Second, all cybersecurity incidents are detected and reported in accordance with Schneider Electric's strict standards, policies and procedures.

To help meet these objectives, Schneider Electric has instituted and continually enforces its Cyber Badge Policy. Built on three Core Principles, the policy provides guidance and helps secure, control and standardize how our thousands of Customer Facing People interact with and serve our global customers each and every day.

Our goal is to work closely with our CFP's, first to ensure they are easily able to comply with the Cyber Badge policy and, second, to help them understand what steps they need to take if they are identified as being non-compliant. The policy not only enables them to better serve our customers and to meet their own professional goals, it helps them better understand gaps in their own security posture and, ultimately, demonstrate Schneider Electric's cybersecurity stance to our customers and other stakeholders.

We are confident that by working with us to adopt and meet the high standards established within our Cyber Badge Policy, and by building on the Core Principles established within it, our CFP's will collectively reduce the cyber risks that threaten the global digital ecosystem.

Our Core Principles

"The Cyber Badge attests that each of our 20,000 CFP's has the expertise, demeanor and tools they need to ensure the safest interaction with our customers."

Christophe Blassiau,
Senior VP Cybersecurity
Global CISO

1. The Cyber Badge is the Cornerstone of Customer Trust

When it comes to cybersecurity, Schneider Electric has a long-standing commitment to transparency and open collaboration. In that spirit of transparency and collaboration, we encourage our customers to have Schneider Electric Customer Facing Populations demonstrate their compliance with our Cyber Badge.

2. Cyber Badge Compliance and Enforcement

Schneider Electric supports and champions compliance with applicable laws, executive orders, regulations, directives and standards. Therefore, as a basic principle, we expect all our employees and representatives to continuously comply 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 trust by regularly assessing whether all our Customer Facing Populations are compliant with our Cyber Badge Policy. These audits, which track cybersecurity training and endpoint security, are performed daily on all endpoints, and collected on a monthly basis for analysis and communication to non-compliant Customer Facing Populations.

As a critical part of our ongoing commitment to securing the digital ecosystem, our Cyber Badge Policy dictates that all non-compliant Customer Facing Populations are prevented from interacting with customers in any way, locally or remotely, and their direct and functional managers are informed to ensure this restriction is enforced.

Additionally, if the CFP remains in breach of our Cyber Badge principles, he or she will be "locked out" from his or her Schneider Electric asset or endpoint so that it cannot be used within Schneider Electric systems and networks and so it cannot connect to any customer's IT or OT systems and infrastructure.

Access to the CFP's end point is restored and the Badge regained only after the CFP is proven to be back into compliance with the Cyber Badge Policy.

3. An Initiative Endorsed Across Schneider Electric

As a testament to our commitment to our Principles of Responsibility, top management from multiple Schneider Electric business units and functions has endorsed the Cyber Badge. This includes leaders from Field Services, Energy Management, Process Automation, Equipment and Transformers, Building Services, Project Execution and Customer Support.

In addition, Schneider Electric has built an extensive community of senior-level Cyber Badge managers, who are responsible for ensuring that all CFP's remain compliant with our Cyber Badge Policy.

These Cyber Badge managers, as well as representatives of Schneider Electric's Governance organization, ensure mandatory cybersecurity training classes focus on topics and threats specific to CFP's, including training on behavioral best practices, safe use of removable devices, anti-malware checks, mobile devices health, incident detection and reporting, and other pertinent subjects.

These managers also ensure all the Schneider Electric assets and endpoints used by our CFP's comply with the company's cybersecurity policies, are always up-to-date and always adequately protected. When a CFP is found to be non-compliant, his or her manager is informed. Measures are then taken, both to understand the root cause of the non-compliance and to ensure the CFP is able to regain compliance as quickly and easily as possible.

All Customer Facing Populations interacting with customers must comply with Schneider Electric's Cyber Badge Policy. We encourage our customers to enquire about the Cyber Badge status of every Schneider Electric representative they encounter.