Source Code Security Principles

First publication : September 2022
Current publication : June 2025
Version : V2
Document type : Policy
Scope : Public
Confidentiality Status : External use

Life Is On Schneider Electric

Our Vision

"Our EcoStruxure architecture and offerings are built on the foundation of our software source code, which we consider valuable intellectual property. We leverage the legal and technical measures at our disposal to protect it."

Helen Lamprell
Chief Business Legal Counsel

"Protecting source code — the seed of the Digital Transformation in many industries — is a vital component of our security posture and underpins the trust our customers and other stakeholders have in us."

Christophe Blassiau
SVP Cybersecurity & Global CISO

Overview

Global cybersecurity risks are constantly evolving. As Schneider Electric digitizes its core business processes, customer solutions, and supporting technologies, our digital landscape and risk exposure expand accordingly. Additionally, as our partners, suppliers, and customers embrace digitization, the attack surface increases, leading to a heightened number of cyber vulnerabilities.

At Schneider Electric, we collaborate with every entity in our ecosystem—including our customers, suppliers, partners, shareholders, employees, and the communities we serve—to build and maintain trust. This commitment extends beyond cybersecurity; it is a prioritized strategic imperative, as our business fundamentally relies on trust.

Schneider Electric's Trust Charter embodies the principles that guide all our interactions in a meaningful, inclusive, and positive manner. This Code of Conduct applies to everyone working at Schneider Electric and our subsidiaries, emphasizing our responsibility to protect our source code against cybersecurity risks such as leakage, theft, or tampering.

Schneider Electric, in collaboration with trusted third parties, develops source code that forms our proprietary intellectual property (IP) and is integral to our software, including firmware. This source code is the driving force behind our offerings, solutions, and infrastructures. To safeguard this valuable asset, we have established an internal *Source Code Protection and Usage Policy* ("Policy") that complements the Secure Development Lifecycle principles we have already adopted.

The Policy is designed to safeguard our source code throughout its entire lifecycle. By aligning with the latest standards and regulations, we ensure the appropriate level of protection. The Policy aims to:

- Reduce the risk of source code leakage and tampering.
- Secure and control access to critical data and IP associated with the source code.
- Enhance traceability of all third-party code.
- Provide guidance on improving the security posture of our research and development (R&D) partners.
- Ensure compliance with applicable regulations.

Several core principles ("Core Principles") underpin this strategy, helping us achieve our vision. These Core Principles provide a framework for collaboration with all our stakeholders, including our customers and the broader third-party software development community. They also ensure compliance with the *Source Code Protection and Usage Policy*, enabling us to collectively deliver secure products and solutions that foster trust.

By Partnering with us to adopt and meet the high standards outlined in these Core Principles, our stakeholders can unlock numerous business benefits. More importantly, by mitigating risks associated with the development, management, and distribution of software, we can collectively work to protect and strengthen the digital economy. This collaborative effort fosters trust, enabling all of us to contribute to and benefit from the digital ecosystem.

Our Core Principles

1. Responsible Parties and Governing Practices

The *Source Code Protection and Usage Policy* applies to all Schneider Electric employees, contractors, and representatives, requiring them to comply with license obligations associated with any source code. The Policy covers all source code developed on behalf of Schneider Electric, whether used internally or in delivering products and solutions to our customers.

Under the Policy, Schneider Electric is responsible for ensuring that all source code remains untampered and for reducing the risk of exfiltration. It mandates that any third-party source code must have the appropriate license—or licenses, depending on the nature of the source code—that is compatible with the company's other policies. If the source code contains components developed under different licenses, each must comply with our policies and be compatible with one another.

The Policy also addresses supply chain attacks by dependencies, ensuring the trustworthiness of the source, its internal storage, and its verification. When third-party code is used as part of a Schneider Electric software solution, we are responsible for its configuration management as part of our secure development process.

Additionally, the Policy mandates that Schneider Electric's R&D teams may only use software engineering tools with a direct or indirect access to the source code that have been validated through a certification process. The R&D teams must ensure that source code storage is securely managed, and its accesses respect the Least Privilege principles.

As part of the Policy, we classify and identify our source code based on its sensitivity and the environments in which it is expected to operate:

- **Sensitive**: Source code that is critical to our customers or to Schneider Electric.
- **Restricted**: Code that is not sensitive but requires certain restrictions and controls.
- **Open source**: Code that can be used in accordance with open-source licenses.

This classification, and identification determines the level of protections we implement to control access to the respective source code.

2. Code Storage and Transmission

The Policy governs all aspects of how we store and transmit our source code and IP. This includes, but is not limited, authorization and access, residency, protection at rest, and protection in transit. By ensuring compliance with our clearly defined and enforced controls, we reduce the risk of source code leakage or tampering, enhance secure access to the code, and enable effective tracing of any third-party code.

3. Third-Party Licensed Source Code and Access to Schneider Electric Code

Schneider Electric frequently relies on trusted third parties to support its offerings with source code they develop. These vendors are required to adhere to these principles, as well as our Supplier Security Principles, to help secure and protect the digital ecosystem while better serving our customers.

We recognize that code developed by third-party can introduce new cybersecurity risks into Schneider Electric products and services. To address this, the Policy effectively manages and

governs the software development lifecycle, engaging a broader community of stakeholders, including third-party developers.

To ensure compliance, we regularly check source code for hard-coded credentials, backdoors, and other features that could expose us to cybersecurity threats. This includes ensuring that passwords, tokens, and other forms of credentials are not embedded within the source code itself. Additionally, as part of our Secure Development Lifecycle, we document every use of third-party code, monitor it for vulnerabilities and security patches, and rapidly deploy necessary updates. Security and privacy considerations are integrated into the design phase of source code development.

Beyond third-party developers, the Policy also applies to any entity that requires access to proprietary Schneider Electric source code, including customers, researchers, and regulatory authorities. Schneider Electric actively collaborates with these stakeholders, particularly customers in highly regulated segments, to ensure compliance with the Policy. This may include geo-locking to control where the source code resides and how it is transmitted.

4. Source Code Guidance from the NIST Framework

The Core Principles outlined here guide how we protect and control our source code throughout its lifecycle. These principles are based on the globally recognized NIST Framework, which is widely utilized to identify and address high-priority business risks. The NIST Framework encompasses prevailing standards, guidelines, and practices for better managing and reducing cybersecurity risks.

By applying the NIST Framework to our source code lifecycle, we enhance our ability to ensure resilient and reliable access to essential IP. This includes securely managing software updates, remediating code vulnerabilities, and protecting it from degradation.

5. **Policy Execution**

Our *Source Code Protection and Usage Policy*, along with its Core Principles, forms the foundation for managing and controlling our source code. These Core Principles are validated by our internal cybersecurity organizations, which are responsible for developing actionable core controls to automate the execution of the Policy as much as possible.

Conclusion

Source code security is key elements of the cybersecurity supply chain for software, and Schneider Electric is committed to its continuously improvement. We rigorously apply our Core Principles while ensuring we adapt to evolving technologies and changing business needs.