Source Code Security Principles

First publication	: September 2022
Current publication	: September 2022
Version	: V1
Document type	: Policy
Scope	: Public
Confidentiality Status	: External use

Life Is On | Schneider Electric

Our Vision

"Our software source code, which is the backbone of our EcoStruxure architecture and offers, is precious intellectual property. We protect it using all our legal and technical means."

Peter Wexler
Chief 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

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 partners, suppliers, and customers are also digitalizing, leading to an even larger attack surface, and thus, to more cyber vulnerabilities.

Schneider Electric works with every entity in our family and ecosystem of customers, shareholders, employees, and the communities we serve to forge and ensure trust. This is not only as a cybersecurity issue, but also an urgent strategic imperative, as our business runs on trust Schneider Electric's Trust Charter is driven by a trust that powers all our interactions in a meaningful, inclusive, and positive way. This Code of Conduct applies to everyone working at Schneider Electric or any of our subsidiaries — and it applies to how we protect our source code from cyber security risks such as leakage, theft, or tampering.

Schneider Electric and trusted third parties develop source code that is the intellectual property (IP) used in our software, which includes firmware, and it is the driving force behind our offers, solutions, and infrastructures. To protect this source code, we have established an internal Source Code Security Policy that complements the Secure Development Lifecycle principles we have already adopted.

The Source Code Security Policy helps protect our source code throughout its entire lifecycle and we align with the latest standards and regulations to guarantee the right level of protection. The intention of the policy is to:

- Reduce the risk of source code leakage and tampering.
- Secure and control access to critical data and IP associated with the source code.

- Improve and enable traceability of all third-party code.
- Provide guidance on how to improve the security posture of our research and development (R&D) partners.
- Ensure compliance

There are several core principles behind this strategy which help us achieve our vision. These principles provide the framework for how we collaborate with all our stakeholders, including our customers and the broader third-party software development community. The principles also help ensure compliance with the Source Code Security Policy so we can collectively bring to market secure products and solutions that engender trust.

We are confident that by working with us to adopt and meet the high standards established within these principles, our stakeholders can realize countless business benefits. But more importantly, by reducing the risks around the development, management, and distribution of software and its source code, we can jointly help protect and strengthen the digital economy so we can all have trust in, contribute to, and benefit from the digital ecosystem.

Our Core Principles

1. Responsible Parties and Governing Practices

The Source Code Security Policy applies to all Schneider Electric employees, contractors, and representatives who are required to comply with license obligations attached to any source code. It also applies to all source code written on behalf of Schneider Electric, including the source code the company uses internally or in the provision of products and solutions to our customers.

Under the Policy, Schneider Electric is responsible for ensuring all source code is untampered with and we are responsible for reducing the risk of exfiltration. The Policy also requires that any source code contain the appropriate license — or licenses, depending on the nature of the source code — that is compatible with the company’s other policies. Some source code may contain source code developed under different licenses. Each of these licenses must comply with our policies and be compatible to each other whenever allowable and applicable.

The Policy also prevents dependency confusion, which ensures that source code is not dynamically linked to source repositories hosted by third parties. 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.

The Policy also states that Schneider Electric’s R&D teams can only use software engineering tools for the development and storage of source code that have been validated by a certification process. The R&D teams must ensure source code repositories are securely managed and operated properly, and the teams must determine which best practices should be applied for the protection of the code.

2. Source Code Classification and Access

As part of the Policy, we classify our source code depending upon its sensitivity and the environments within which it is expected to operate using three tiers:

- **Sensitive**: Source code that is critical to our customers or intellectual property of 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.

These classifications determine the level of protections we install to control access to the respective source code.

3. Code Storage and Transmission

The Policy also controls and governs all aspects of how we store and transmit our source code and IP, including but not limited to authorization and access, residency, protection at rest, and protection in transit.

Ensuring compliance, as well as our clearly defined set of enforced controls, helps reduce the threat of source code leakage or tampering, improves secure access to the code, and enables us to trace any third-party code.

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

Schneider Electric frequently relies on trusted third parties to support our offers with source code they develop. These vendors must follow these principles, as well as our Third-Party Principles, to help us secure and protect the digital ecosystem while better serving our customers.

However, we recognize that third-party developed code could introduce new cybersecurity risks into Schneider Electric products and offers. Therefore, through our Policy, we securely manage and govern the software development lifecycle across a broader community of stakeholders that includes third-party developers.

To ensure compliance, source code is regularly checked for hard-coded credentials, backdoors, and other features that make the code vulnerable to cybersecurity threats. This includes ensuring that passwords, tokens, and other forms of credentials are not stored within the source code itself. In addition, as part of our Secure Development Lifecycle, we record every use of third-party code, monitor the code for vulnerabilities and security patches, and rapidly deploy patches. Source code development must include security and privacy in the design phase as well.

Beyond third-party developers, the Policy also governs any entity who needs access to proprietary Schneider Electric source code, including customers, researchers, and authorities. Schneider Electric actively works with these stakeholders, including customers in highly regulated segments, to help them comply with this Policy. This can extend to geo-locking where the source code resides and how it is transmitted.

5. Source Code Guidance from the NIST Framework

The Core Principles here, which essentially direct how we protect and control our source code across its lifecycle, are based on the globally recognized NIST Framework. The NIST Framework is widely used to help determine and address high-priority business risks. It includes prevailing standards, guidelines, and practices for better managing and reducing cybersecurity risks.

By applying the NIST Framework across our source code lifecycle, we are better able to assure resilient, reliable access to essential IP, including how we securely manage software updates, remediate code vulnerabilities, and otherwise protect it from degradation.

6. Policy Execution

Our Source Code Security Policy and its Core Principles are the foundation of how we manage and control our source code. They are verified by our internal cybersecurity organizations who are responsible for developing actionable core controls that automate as much of the execution of the Policy as possible.

Conclusion

Source code security is one of elements in the cybersecurity supply chain for software that Schneider Electric is committed to continuously improve. We strictly and diligently apply our Core Principles while ensuring we adapt to evolving technologies and changing business needs.