SIEMENS energy

Cybersecurity at Siemens Energy

siemens-energy.com/cybersecurity
cybersecurity@siemens-energy.com

Bringing the highest value to our customers

Our commitment to cybersecurity

As digitalization continues to transform our energy systems, the advancements in technology and efficiency also give rise to heightened vulnerability to cyberattacks. At Siemens Energy, we help our customers effectively and efficiently overcome this challenge by providing products, solutions, and services with best-in-class security as well as dedicated cybersecurity support to our customers along the full value chain.

Ensuring Industrial Cybersecurity

Critical infrastructure has become a prime target for cyberattacks. To be a trusted partner for our customers, our portfolio must be cybersecure to protect against cyber threats.

Our efforts in Industrial Cybersecurity ensure cybersecurity resilience by holistically and systematically addressing security in all phases of the portfolio lifecycle, through processes, guidance, competence, and state-of-the-art security technology. Siemens Energy uses established and proven mechanisms to ensure the integrity of Siemens Energy portfolio by leveraging secure-by-design and defense-in-depth concepts.

Cybersecurity is our daily responsibility. With our diverse team of experts, we strive to be the most cybersecure energy technology company and bring the highest value to our customers.



Dr. Judith Wunschik
Chief Cybersecurity Officer of Siemens Energy

Focus areas

The scope of our cyberdefense includes information (IT) security and Industrial Cybersecurity (ICS).

→ **All**
customer-facing products and solution

~110,000
IT assets

>100
factories

~30,000
suppliers

Our objectives

- **We secure our energy assets**
- **We create business of tomorrow**
- **We shape the cybersecurity ecosystem**

Complying with industry standards

For Siemens Energy, protecting our data and information assets and offering secure products and solutions to our customers are the most relevant challenges we face. We meet this challenge through a continuous improvement process that includes technical, organizational and personnel measures.

We identify the required measures using established security standards:

- ISO 27001 for information security
- NIST Cybersecurity Framework (CSF) for our organization
- IEC 62443 for industrial cybersecurity, such as production facilities and customer-facing products and solutions

The quality of these measures is controlled by key performance indicators that are based on testing, audits, Red Team/Blue Team exercises, penetration tests, security scanning, and other methods.

Actively managing cyber risks

Cyber risk management is key for handling risks to information technology, operational technology, and the products and solutions that Siemens Energy offers its customers.

Our cyber risk management relies on an appropriate organizational structure where roles and responsibilities are well-defined and that is enhanced by automated workflows.

Siemens Energy's approach to an active cyber risk management includes the continuous and transparent improvement of processes and tools and the simplification and standardization of risk treatment plans for critical assets as well as managing risks to suppliers, providers, and vendors.

Detecting & responding to cyber incidents

Just as important as minimizing risks for cyber attacks is responding quickly and decisively when incidents occur. Siemens Energy maintains a Security Operation Center (SOC) to enable rapid action in any situation and to brace ourselves for potential attacks. This is made possible by:

- Threat intelligence and threat hunting capabilities to assess our threat situation and adapt our defense in a preventive manner
- Vulnerability management to proactively identify efficiencies in our IT landscape
- Incident and crisis response to react to cyber emergencies



We are here for you with more than 1,000 years of experience of all ages (22–60 years) and more than 15 nationalities in a global team on four continents.

Driving a cybersecurity culture

As recent attacks have shown, employees are the weakest link in the cybersecurity chain, and hackers can use them to gain access. Employees need to be aware of the consequences of their behavior when they're working with corporate data and information assets and systems.

With our own awareness program, which is based on the latest scientific approaches, our security awareness concepts and methods are continuously modernized and developed to anchor cybersecurity in the DNA of Siemens Energy.

The result is an internal cybersecurity culture that emphasizes cybersecurity as a daily responsibility in the minds of our employees.

Website

To get an overview on Cybersecurity at Siemens Energy, visit **https://www.siemens-energy.com/cybersecurity**

Contacts

If you want to report a potential security issue involving Siemens Energy portfolio or infrastructure, send an email to **cert@siemens-energy.com**

If you have questions or comments on the content of this document, send an email to **cybersecurity@siemens-energy.com**

Published by

Siemens Energy Global GmbH & Co. KG
Otto-Hahn-Ring 6
81739 München
Germany

For the U.S. published by
Siemens Energy, Inc.
4400 N Alafaya Trail
Orlando, FL 32826
USA

For more information, please contact us by e-mail:
cybersecurity@siemens-energy.com

Unrestricted © Siemens Energy, 2024

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract. All product designations may be trademarks or product names of Siemens Energy Global GmbH & Co. KG or other companies whose use by third parties for their own purposes could violate the rights of the owners.

Siemens Energy is a trademark licensed by Siemens AG.