Siemens Cybersecurity FAQs

1) *Do you have a Cybersecurity Organization?*

Siemens has established dedicated roles for to ensure Cybersecurity resilience and sustainable implementation of Cybersecurity Strategy. They are supported by different boards with respective representation that ensure an effective collaboration. The Cybersecurity organization covers all of Siemens, from business, product development, and administrative activities.

2) *How does Siemens safeguard critical infrastructure, protect sensitive information, and assure business continuity?*

Established central Cybersecurity Governance for Siemens to adequately protect Siemens' information assets, IT/OT infrastructure, Product and Services providing a common and implemented information security approach followed by all employees, based on international standards and good practices. Siemens has an Information Security Management System (ISMS) consisting of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.

3) *Does Siemens have any certifications?*

ISO 27001 is the international standard that describes best practices for an ISMS. Achieving an accredited certification to ISO 27001 demonstrates that your organization is following information security best practice and provides an independent expert verification that information security is managed in line with international best practice and business objectives.

Cybersecurity Governance for Siemens' is ISO 27001 certified since October 2017

4) *Do you have an Incident Response process?*

Incidents are undesired events that have or will have a detrimental effect on Siemens and therefore require measures to prevent further harm or damage. Major incidents or incidents that are not handled properly can cause company crises. Siemens has developed and implemented a global Incident Response Process that ensures central reporting channels and the involvement of relevant stakeholders.

5) *How does Siemens protect the company's tangible and intangible assets exposed to security risks?*

Depending on their importance to our business, their loss or impairment may seriously harm the company or individual company units. To avoid this possibility, Siemens has implemented an Enterprise Risk Management System to uniformly and systematically identify critical assets and ensure the development and implementation of adequate protection concepts.

The following security risks are considered:

- loss of confidentiality (for example, theft of sensitive information)
- loss of integrity (for example, tampering with software) and
- loss of availability (for example, the non-availability of buildings or key personnel).

6) *What is the Charter of Trust?*

Founded in 2018 at the Munich Security Conference, the Charter of Trust was initiated by Siemens because of increasing daily life exposure to malicious cyber-attacks. Today, its members have transformed it into a unique initiative of leading global companies and organizations working together to make the digital world of tomorrow safer.

https://www.charteroftrust.com