Charter
of Trust

Charter of Trust

on Cybersecurity

charter-of-trust.com | #Charter of Trust

Digitalization creates opportunities and risks

Charter of Trust

And it‘s common truth

We can’t expect people to actively support the digital transformation if we cannot **TRUST** in the security of data and networked systems.

Charter of Trust

That’s why together with strong partners we have signed a “Charter of Trust” – aiming at three important objectives

1. **Protect the data** of individuals and companies

2. **Prevent damage** to people, companies and infrastructures

3. **Create a reliable foundation** on which confidence in a networked, digital world can take root and grow

Founding and Contributing Partners

AES, AIRBUS, Allianz, Atos, Cisco, Daimler, Dell Technologies, IBM, MSC, NXP, SGS, Siemens, Telekom, Total, TÜV SÜD, Mitsubishi Heavy Industries, Ltd.

Associated Partner Forum

Bundesamt für Sicherheit in der Informationstechnik, TU Graz, CCN Centro Criptológico Nacional

Charter of Trust

And we came up with ten key principles

01 **Ownership of cyber and IT security**

02 **Responsibility throughout the digital supply chain**

03 **Security by default**

04 **User-centricity**

05 **Innovation and co-creation**

06 **Education**

07 **Certification for critical infrastructure and solutions**

08 **Transparency and response**

09 **Regulatory framework**

10 **Joint initiatives**

Charter of Trust

For a secure digital world

Charter of Trust

A critical factor for the success of the digital economy

Key Principles

Charter of Trust for a secure digital world

charter-of-trust.com

01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "it is everyone's task".

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protections across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as

- **Identity and access management:** Connected devices must have secure identities and safe-guarding measures that only grant access to authorized users and devices
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate
- **Continuous protection:** Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism

03 Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models

04 User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks

05 Innovation and co-creation

Combine domain know-how and deepen a joint under-standing between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage contractual Public Private Partnerships, among other things

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future

07 Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions

08 Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice, which focuses on critical infrastructure

09 Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)

10 Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay

Charter of Trust

And we bring them to life as

Principle 1 — Ownership of cyber and IT security

Our Siemens approach for a new **Cybersecurity organization**

Our Vision

For our society, customers and Siemens, we are
the trusted partner in the digital world
by providing industry leading cybersecurity
Together we make cybersecurity real – because it matters

Our Holistic approach

Protection of our **IT and OT Infrastructure**

Protection of our **products, solutions and services**

Enable cyber **solutions for our business**

Concrete implementation steps at Siemens

In January 2018 we established a **new Cybersecurity unit** headed by Natalia Oropeza, our new **Chief Cybersecurity Officer** (CCSO). In this function, she reports directly to the Managing Board of Siemens AG. With this new position we're fulfilling one of our requirements in the Charter of Trust.

"Cybersecurity is more than a challenge. It's a huge opportunity. By setting standards with a dedicated and global team to make the digital world more secure, we are investing in the world's most valuable resource: TRUST.

Our concrete answers to today's upcoming Cybersecurity issues and our proposals for more advanced Cybersecurity rules and standards are invaluable to our partners, stakeholders and societies around the world. That is what we call "ingenuity at work."

Natalia Oropeza,
Chief Cybersecurity Officer, Siemens AG

Charter of Trust

And we bring them to life as

Principle 2 — Responsibility throughout the digital supply chain

The Siemens security concept
defense-in-depth

Concrete implementation steps at Siemens

Siemens provides a **multi-layer concept** that gives plants both **all-round and in-depth protection**

- Know-how and copy protection
- Authentication and user management
- Firewall and VPN (Virtual Privat Network)
- System hardening and continuous monitoring

Concrete implementation steps with the CoT partners

With our partners, we are defining a **list of minimum security requirements** for **all players in the supply chain**, and effective **mechanisms** that can **support their implementation**

Charter of Trust

An aligned CoT view on 17 Baseline Cybersecurity Supply Chain Requirements[1)] along the digital supply chain

Category	Baseline Cybersecurity Supply Chain Requirements [1)]
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data
	Data shall be protected from unauthorized access throughout the data lifecycle
	The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/ segmentation, operational security, physical security, vendor management)
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services.
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer, & Separation	Encryption and key management mechanisms shall be available, when appropriate, to protect data
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable
	A process shall be in place to ensure that products and services are authentic and identifiable
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

1) For next generation products and solutions

Source: Charter of Trust – Task force "Baseline Cybersecurity Supply Chain Requirements[1)]" May 2019

Charter of Trust

Principle 6

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future.

What does that mean and why is it so important?

A significant number of cybersecurity incidents are attributed to human error or negligence. Raising everyone's awareness of cyber risks and protection measures is the first line of defense.

To continue developing IT security at the technological level, people need to be able to acquire the skills and qualifications that are needed for the digital transformation. Only in this way can people adapt to the new job profiles.

That's why corresponding supportive programs for schools, universities and companies should be continued and expanded.

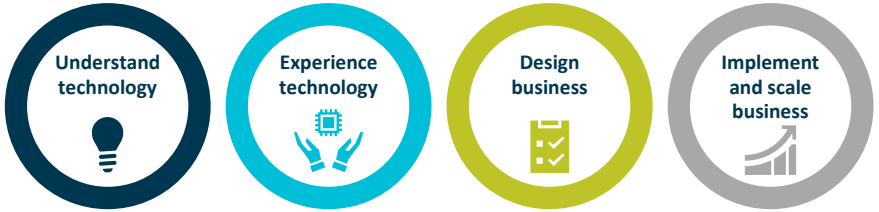
Concrete implementation steps

Siemens example

By carrying out regular cybersecurity awareness training sessions worldwide, Siemens ensures all employees have a high level of security awareness. We invest in building dedicated security expertise for products, solutions and services with a role-specific curriculum.

InfoSec Cards, for example, give practical hints categorized in different topics to support our employees in implementing Siemens-specific InfoSec rules and regulations. With annually renewed Trend Cards, we provide an overview of the most important current technical and non-technical trends in the broader field of cybersecurity that may possibly influence the Siemens portfolio.

And our "Applying Digitalization to your Business" training session, featuring cybersecurity as key element, has been rolled out throughout the company and consists of four important pillars:



Applying digitalization to our business

A hands-on training to accompany digital transformation

Charter of Trust

As Charter of Trust, we jointly want to address key challenges in Cybersecurity education and propose 13 recommendations – internal and external

Joint objectives

Build a security culture
91% of cyber attacks take advantage of the human vulnerability – looking to exploit our curiosity, sense of urgency, and fear.

Drive for more diversity in Cybersecurity workforce
Millennials and Gen Y only comprise 35% of the field. Women represent 24% of the cybersecurity workforce overall.

Expand Cybersecurity competencies and activities
According to a recent ICS2 study, the shortage of cybersecurity professionals is almost 3 million today – with APAC having the greatest shortage – around 2.15 million[1]

Recognize that Cybersecurity is a challenge
The digital transformation has left people unaware of the risks and threats associated with technologies that are greatly improving their way of life and work.[2]

Internal deployment

1. Make the risks inherent in Cyberattacks transparent and visible – and highlight the opportunities of Cybersecurity
2. Ensure that all employees throughout the entire organization receive Cybersecurity education to build capacity
3. Position Cybersecurity with Top Management
4. Increase know how along industry-accepted standards/certifications
5. Implement a curriculum to embed "security by default" design in development of services and products
6. Encourage Cybersecurity community building throughout the entire organization

External ecosystem

7. Establish basic level of Cybersecurity hygiene understanding – from the earliest levels of education through to post-retirement
8. Promote Cybersecurity as a career path in its own right – spanning across different disciplines
9. Align the capacity and the skills that the education system produces with the current demand
10. Ensure education along common standards and certification
11. Create and encourage additional pathways to jobs (in addition to traditional degrees) and include Cybersecurity proficiency
12. Increase collaboration between private and public sector
13. Make internal education paths and education programs of companies accessible externally

Source: Charter of Trust project team 1) In the US the shortages is about 497K, EMEA has the smallest gap around 142K (Source: IC²) 2) ENISA report https://www.enisa.europa.eu/

Charter of Trust

FEBRUARY 16, 2018

Launch at Munich Security Conference

MARCH 8, 2018

New partners joined at CERAWeek 2019

APRIL 23, 2018

First Roadshow at Hannover Messe

MAY 17, 2018

New partners joined at U.S. Infrastructure Week

OCTOBER 16, 2018

Second Roadshow at the Digital Industry Summit in Paris

JUNE 26/27, 2018

First Partner Work-shop in Geneva

OCTOBER 18, 2018

Baseline requirements approved by Board of Directors

NOVEMBER 12, 2018

Third Roadshow in Washington D.C.

MARCH 20/21, 2019

Second Partner Workshop in Montpellier

FEBRUARY 15, 2019

First anniversary at Munich Security Conference 2019

NOVEMBER 15, 2018

French President Emmanuel Macron presents Paris Peace Call

APRIL 1, 2019

Roadshow at Hannover Messe

APRIL 2, 2019

Roadshow in Brussels

APRIL 23, 2019

Roadshow in Tokyo – MHI joins CoT

Charter of Trust

Charter of Trust

charter-of-trust.com

Together we strongly believe

- Effective cybersecurity is a precondition for an open, fair and successful digital future
- By adhering to and promoting our principles, we are creating a foundation of trust for all

As a credible and reliable voice, we collaborate with key stakeholders to achieve trust in cybersecurity for global citizens.

Be part of a **network** that does **not only sign**, but **collaborates** on **Cybersecurity!**

Let us be your **trusted partners** for **cybersecurity** and **digitalization**

Together we will **improve** our **technology, people** and **processes**

Join us by **following our principles** and making the digital world more secure

Charter of Trust