Charter of Trust

For a secure digital world

Jim Jacobson ◆ Chief Product & Solution Security Officer ◆ Siemens Healthineers

Creating trust in a secure digital world

Charter of Trust

People and organizations need to trust that their digital technologies are safe and secure; otherwise they won’t embrace the digital transformation.

Digitalization and cybersecurity must evolve hand in hand.

3 Goals

Charter of Trust

1. We wish to protect the data and assets of individuals and businesses.
2. We wish to prevent damage to people, businesses, and infrastructures.
3. Together we wish to build a reliable basis for trust in a connected and digital world.

Goal 1

Charter of Trust

We wish to protect the data and assets of individuals and businesses.

The digital world changes everything. Artificial intelligence and big data analytics are revolutionizing our decision making; billions of devices are being connected by the Internet of Things and interacting on an entirely new level and scale.

Goal 2

Charter of Trust

We wish to prevent damage to people, businesses, and infrastructures.

As much as these advancements are improving our lives and economies, the risk of exposure to malicious cyber attacks is also growing dramatically. Failure to protect the systems that control our homes, hospitals, factories, grids, and virtually all of our infrastructures could have devastating consequences. Democratic and economic values need to be protected against cyber and hybrid threats.

Goal 3

Charter of Trust

Together we wish to build a reliable basis for trust in a connected and digital world.

But no entity can take on this topic alone – regardless of how well set up we may be. The powers of politics, business and society must be pooled together – because cybersecurity concerns us all. To discuss the matter, we are using important worldwide forums. Together we will light the way and sign the Charter of Trust, showing how we can make the digital world more secure.

10 Key principles

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Certification for critical infrastructure and solutions
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Principle 1

Charter of Trust

Ownership for 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”.

Principle 2

Charter of Trust

Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection 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 safeguarding measures that only allow authorized users and devices to use them.

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.

Principle 3

Security by default

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

Principle 4

Charter of Trust

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.

Principle 5

Charter of Trust

Innovation and co-creation

Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships.

Principle 6

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.

Principle 7

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.

Principle 8

Charter of Trust

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 is focusing on critical infrastucture.

Principle 9

Charter of Trust

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).

Principle 10

Charter of Trust

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.

Together we will shape Cybersecurity

www.charter-of-trust.com

Charter of Trust

SIEMENS	AES	AIRBUS	Allianz
Atos	DAIMLER	enel	IBM
msc	NXP	SGS	·T··