Charter
of Trust

Charter of Trust

on Cybersecurity

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

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**

Charter of Trust

For a secure digital world

06 **Education**

07 **Certification for critical infrastructure and solutions**

08 **Transparency and response**

09 **Regulatory framework**

10 **Joint initiatives**

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

We are also coming up with baseline requirements for our suppliers along the supply chain

Category	Baseline requirements
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 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
	Robust business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption
	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)

Charter of Trust

Nevertheless

"We can't do it alone. It's high time we act – together with strong partners who are leaders in their markets."

Joe Kaeser
Initiator of the Charter of Trust

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

Where it all started: Munich Security Conference 2018

Thank you for your attention.

Charter of Trust