Charter of Trust

For a secure digital world

Charter
of Trust

Charter of Trust

For a secure digital world

The digital world is changing 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.

As much as these advances 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 infrastructure could have devastating consequences. **Democratic and economic values need to be protected from cyber and hybrid threats**.

Cybersecurity is and has to be more than a seatbelt or an airbag here; it's a factor that's crucial to the success of the digital economy. 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**.

In order to keep pace with continuous advances in the market as well as threats from the criminal world, **companies and governments must join forces and take decisive action. This means making every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses, and infrastructures; and build a reliable basis for trust in a connected and digital world**.

Hedging the all-encompassing impact of digitalization and cybersecurity and creating a holistic basis of trust can't be achieved by a single company or entity; it must be the result of close collaborations on all levels. **In this charter, the signing partners outline the key principles we consider essential for establishing a new charter of trust between society, politics, business partners, and customers**.

AIRBUS

IBM

SIEMENS

Allianz

Munich Security Conference MSC Münchner Sicherheitskonferenz

SGS

DAIMLER

NXP

T

Our principles

1 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."

2 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.

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.

4 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.

5 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.

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.

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.

8 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 infrastructure.

9 Regulatory framework | Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of the 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.


AIRBUS
Allianz
DAIMLER
IBM
Munich Security Conference msc
Münchner Sicherheitskonferenz
NXP
SGS
SIEMENS
T