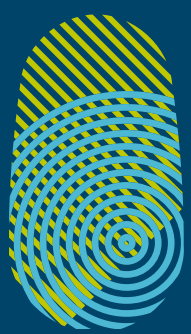
Cybersecurity

Creating security in a networked 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 while 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 cyberattacks 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.**

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 both individuals and businesses, prevent damage to people, businesses, and infrastructures and build a reliable basis for trust in a connected and digital world.**

In other words, it's a matter of building trust in cybersecurity, advancing it on all its various levels and thereby paving the way for digitalization. And that's not something that any company can do all by itself. **It has to be approached through a close collaboration of all the parties involved. In this document, the undersigned outline the key principles for a secure digital world – principles that they're actively pursuing in collaboration with civil society, government, business partners and customers.**

AES · cisco · IBM · SIEMENS

AIRBUS · DAIMLER · msc · T

Allianz · DELL Technologies · NXP · TOTAL

Atos · enel · SGS · TÜV SÜD

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's 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 policy-makers 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.

charter-of-trust.com

Cybersecurity is critical for everyone

5 tips for better security

1 Keep your hardware and antivirus software up to date. Be cautious when dealing with unknown apps.

- Internet-capable equipment should always be up to date.
- Install updates as soon as they become available.
- Don't install unknown apps.

2 Use different passwords and two-factor authentication for your accounts.

- Long, cryptic passwords incorporating numbers, symbols and both capital and small letters are more secure.
- Avoid simple sequences of numbers or characters, names in normal text, and complete words.
- Don't let others know your passwords, and don't write them down in places like note pads.
- Use two-factor authentication with additional identification, such as an SMS code.

3 Be able to recognize spam (fake email) and be cautious when dealing with attachments and links.

- Be mistrustful of emails with unrequested information or attachments, or messages from a known name accompanied by an unknown email address.
- Don't click on links embedded in emails from unfamiliar sources. You can use your mouse pointer to compare the pop-up text with the link without clicking it.
- Don't open executable files (.exe, .scr, .cpl, zip files) or Office documents that contain macros.
- Delete emails from services you don't use or that you don't normally receive email from, such as delivery services, banks, telephone providers and hotels.
- Ignore requests to install software from an unknown source.

4 Don't accept every "friend" request on social media.

- Check to see if you know the person and whether the request is really from that person.
- If you're in doubt, ignore the request.

5 Provide access only to certain limited data and information.

- Don't release your personal data carelessly.