Delivering on our commitments

Building a secure digital world by defining baseline requirements

At the signing ceremony at the Munich Security Conference (MSC), the Charter of Trust partners committed to “make the digital world more secure,” and those words have been met with decisive action. During the first Partner Meeting in Geneva, the 16-strong group agreed to work together to expand on the principles of the Charter.

The 10 binding principles act as the backbone of the Charter. They are necessary in order to protect data, prevent harm to people, companies, and infrastructures, and build security, growth, and trust in a digital world. To get started, the partners agreed to tackle Principle 2: responsibility throughout the digital supply chain.

What does this mean in practice?

As a first step, Charter of Trust partners set up baseline requirements for our suppliers along the digital supply chain. We will be able to make our products and services more secure by committing to these 17 baseline requirements. Coupled with effective mechanisms, this will support the successful implementation of Principle 2.

Charter of Trust companies have agreed to define specific requirements for their suppliers based on principles like a heightened level of data protection, including security policies that increase the level of supply chain security.

For example, there is an expectation that CoT partners and our suppliers will design products and services in such a way that they guarantee the confidentiality, authenticity, integrity, and availability of data. Equally, CoT partners expect security checks, tests, and corrections to be conducted on products, services, and the underlying infrastructure on a regular basis. Partners pledge that they will not consent to “back doors” in their products and services even if required to do so by a government. These are just some of baseline requirements that we are pledging our company and our supplies to meet.
**Our next steps in the coming months**

We plan to agree on a risk categorization approach that differentiates between different levels of criticality. For example, is the data in question highly sensitive or confidential? Is it stored on internal infrastructure, or is it in the public cloud? These factors will determine whether higher levels of security are required for the specific use case, and whether this requirement can be fulfilled by a self-declaration or it needs to be verified by an existing international certification system or standard.

The final phase of defining Principle 2 will be to map the requirements of the selected certification systems and standards so that suppliers can determine whether they already comply with Charter of Trust requirements or additional measures are necessary.

In parallel with these steps, Charter of Trust partners are developing implementation plans for their next-generation products and services. Where there are early examples, they will be able to demonstrate how these principles are already being implemented with their suppliers and partners.

**What are the benefits?**

A common set of principles drives greater consistency in the supply chain and improves transparency. Rather than having to negotiate requirements in individual contracts, procurers can apply a pre-defined, unified set. For the supplier, this means fulfilling a higher degree of transparency and predictability.

The overall goal is to raise the bar in cybersecurity, where the supply chain is viewed as increasingly important.

**More information**

[chartier-of-trust.com](http://chartier-of-trust.com)