



**Charter  
of Trust**

# Driving security in an insecure world

**The Charter of Trust**

Cybersecurity is  
becoming more and more  
urgent.

## Key global trends are driving it



Growing  
cyber risk to  
businesses



Fundamental  
technological  
changes



Workforce  
gap is  
widening



Increasing  
professional  
hacking



More laws and  
regulations  
worldwide



Challenging  
local vs. global  
regulation

---

**That's why:**    There is a strong need to act!

---

That's why together with strong partners  
we have signed the Charter of Trust:

aes

Allianz 

Atos

 **BOSCH**

**DELL**  
Technologies

**IBM**

 **Infineon**

 **msc**

 **Microsoft**

 **MITSUBISHI**  
HEAVY INDUSTRIES

  
TotalEnergies

**SIEMENS**

**NXP**



Together, we shape cybersecurity worldwide  
aiming at three important objectives:



Protect the data of  
individuals and  
companies



Prevent damage to  
people, companies  
and infrastructures



Create a reliable foundation  
on which confidence in a  
networked, digital world  
can take root and grow



## And we defined ten 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
- 06 Education
- 07 Cyber-resilience through conformity and certification
- 08 Transparency and response
- 09 Regulatory framework
- 10 Joint initiatives

A trusted network supporting our mission, the **Associated Partner Forum** brings together regulators, think tanks, and academic research institutions with CoT's industry partners.



Bundesamt  
für Sicherheit in der  
Informationstechnik

CANADIAN CENTRE FOR  
CYBER SECURITY



CYBER READINESS  
INSTITUTE

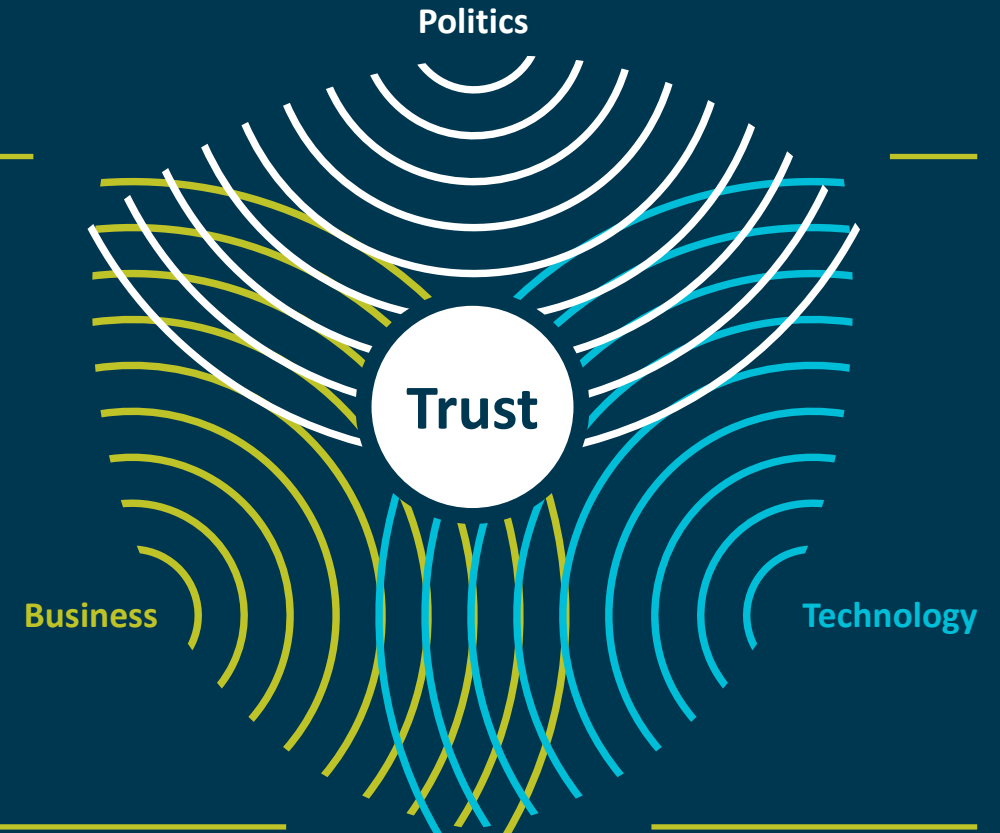


## And we are driving this by

... offering proven approaches to secure the digital world – by **establishing, piloting and adopting global baseline requirements and concepts.**

... striving for a global approach to the regulatory framework for Cybersecurity – by **shaping the political debate** worldwide by foresight and reason.

... embedding Cybersecurity in the digital transition of the industry – by successfully putting **security at the core of digital business models.**





## The Charter of Trust is being recognized ...

His Excellency Jose Angel Gurria  
(Secretary-General of OECD)

“The Paris Peace Call and the **Charter of Trust** launched at Munich Security Conference in 2018 are **excellent new forms of stakeholders working together** for more Cybersecurity by joining forces.”



# Five years of collaboration are showing results



# Five years of collaboration are showing results – details

---



## Together we scale **Supply Chain Security.**

We deliver a common risk-based approach aligned with international norms and are now developing practical guidance for wider adoption.



## **Security by Default** will be a must-have across all our businesses.

That's why we came up with a joint definition and develop a first roll-out plan for use-cases, applications and industries.



## We drive **Cybersecurity education.**

We believe people can be an organization's best firewall. So, we commit to driving education in our organizations. We've also launched activities for selected target groups – from students, via SMEs, to education providers.



## We shape the harmonization of **regulation and standardization**

Thanks to our collective efforts, we are shaping global political regulations on the national, European and global level.



## We turn **Cybersecurity** into a real business opportunity.

Cybersecurity is not only a cost factor but offers many important business opportunities. That is what we see time and again, and that is what we demonstrate to the societies we live in as well as to our suppliers and customers.

## Concrete objectives were defined per prioritized Taskforces – Paying directly into achieving our promises as made in messages

Messages		Principles	Objectives (as defined in Taskforce Integration Team)
		<b>P1</b> Ownership for IT and OT cybersecurity	N/a
Together we scale Supply Chain Security	➔	<b>P2</b> Responsibility throughout the digital supply chain	<ul style="list-style-type: none"> <li>Define <b>baseline requirements</b> to secure products and services along our supply chain <sup>1)</sup></li> <li>Establish <b>risk-based methodology</b> and <b>verification</b> for implementing baseline requirements in our own supply chains</li> </ul>
We are convinced: Security by Default will be a must-have across all our businesses	➔	<b>P3</b> Security by default	<ul style="list-style-type: none"> <li>Define <b>critical Cybersecurity requirements</b> needed to deliver secure products, processes, services and business models.</li> <li>Establish <b>verification methodology</b> in order to provide assurance of the requirements being adequately met</li> </ul>
		<b>P4</b> User-centricity	N/a
		<b>P5</b> Innovation and co-creation	N/a
We drive Cybersecurity education	➔	<b>P6</b> Education	<ul style="list-style-type: none"> <li>Define <b>internal requirements</b> and <b>external recommendations</b> on cybersecurity education</li> <li>Develop <b>roll-out concepts</b> (e.g., campaigns)</li> </ul>
We shape the harmonization of regulation and standardization globally	➔	<b>P7</b> Certification	<ul style="list-style-type: none"> <li>Develop guidance on how to earn and sustain trust through international standards and certification</li> </ul>
		<b>P8</b> Transparency and response	<ul style="list-style-type: none"> <li>Explore / establish information sharing policies relevant for CoT Partners</li> <li>Create human network, supported by TI sharing solution</li> </ul>
	➔	<b>P9</b> Regulatory framework	N/a ( <b>Communicate</b> and <b>advocate</b> content developed by other Taskforces e.g., via new website)
We turn Cybersecurity into a real business opportunity	➔	<b>P10</b> Joint initiative	N/a ( <b>Operationally steer</b> overall CoT work)

➔ Deep Dive (next page)

➔ Deep Dive (next page)


1) For next generation products & solutions

■ Active Taskforce

■ Aspiration covered in other Taskforces


# Principle 2 – Common risk-based approach for the Digital Supply Chain

## External communication package released



### Common risk-based approach for the Digital Supply Chain

Charter of Trust – Principle 2  
Unrestricted | Version 1.0 | 11/02/2020



Charter of Trust  
Principle 2  
Common Risk-based Approach for the Digital Supply Chain

Category	Baseline Cybersecurity Supply Chain Requirements
Data Protection	<ul style="list-style-type: none"><li>Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data</li><li>Data shall be protected from unauthorized access throughout the data life cycle</li><li>The design of products and services shall incorporate security as well as privacy where applicable</li></ul>
Security Policies	<ul style="list-style-type: none"><li>Security policies consistent with industry best practices (such as ISO27001, ISO20445, SOC2, IEC62443) shall be in effect (including access control, security education, employment verification, encryption, network isolation/segmentation, operational security, physical security, vendor management)</li><li>Guidelines on secure configuration, operation and usage of products or services shall be available to customers</li><li>Policies and procedures shall be implemented so as not to consent to include back doors, malware and malicious code in products and services</li></ul>
Incident Response	<ul style="list-style-type: none"><li>For confirmed incidents, timely security incident response for products and services shall be provided to customers</li></ul>
Site Security	<ul style="list-style-type: none"><li>Measures to prevent unauthorized physical access throughout sites shall be in place</li></ul>
Access, Intervention, Transfer and Separation	<ul style="list-style-type: none"><li>Encryption and key management mechanisms shall be available, when appropriate, to protect data</li><li>Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced</li></ul>
Integrity and Availability	<ul style="list-style-type: none"><li>Regular security scanning, testing and remediation of products, services and underlying infrastructure shall be performed</li><li>Asset management, vulnerability management and change management policies shall be implemented that are capable of mitigating risks to service environments</li><li>Business continuity and disaster-recovery procedures shall be in place and shall incorporate security during disruption, where applicable</li><li>A process shall be in place to ensure that products and services are authentic and identifiable</li></ul>
Support	<ul style="list-style-type: none"><li>The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available</li><li>Based on risk and during the time frame of support, processes shall be in place for:<ol style="list-style-type: none"><li>1. Contacting Support</li><li>2. Security Advisories</li><li>3. Vulnerability Management</li><li>4. Cybersecurity-related Patch Delivery and Support</li></ol></li></ul>
Training	<ul style="list-style-type: none"><li>A minimum level of security education and training for employees shall be regularly deployed (e.g. through training, certifications, awareness)</li></ul>

Unrestricted | CoT P2 – Report 1 | Version 1.0 | 11/02/2020

Page 4



Charter of Trust  
Principle 2  
Common Risk-based Approach for the Digital Supply Chain

### 2.3 Verification

A standard verification process shall be used to ensure that digital suppliers are adhere to the baseline requirements. The process allows for three verification elements, which will be used according to the criticality of the digital supplier. Therefore, the verification element to be employed is aligned to the criticality level of the supplier being assessed.

Verification Element	Verification Element description	Supplier criticality
DP Document proof	Supplier shall provide evidence that it complies with the baseline requirements	High
SA Self-Assessment	Supplier shall demonstrate compliance to the baseline requirements by completing a self-assessment questionnaire	Medium
SD Self-Declaration	Supplier shall declare its compliance with the baseline requirements, e.g. through accepting T&Cs	Low

The verification process is designed to have minimum impact on existing procurement processes. It has been specifically designed to be "light" while at the same time raising awareness and compliance with foundational cybersecurity requirements and best practices that should be adopted by all digital suppliers.

### 3 Context and further resources

The Charter of Trust believes that cybersecurity is a foundational element of trust in the digital economy for all. For creating this foundation, Charter of Trust partners aim to lead by example driving applicable Charter of Trust requirements through their companies and connected ecosystems (e.g. suppliers, partners and others). Furthermore, the partners aim at demonstrating the effectiveness of collaborative private enterprise efforts to regulators and policymakers.

The members of the Charter of Trust are continuously working on advancing the ten principles, defining clear baseline requirements and best practices where applicable. These are widely shared with a broad network of stakeholders to ensure a far-reaching level of trust.

To learn about the work of the Charter of Trust and find the latest releases, please refer to our website [www.charter-of-trust.com](http://www.charter-of-trust.com)

Unrestricted | CoT P2 – Report 1 | Version 1.0 | 11/02/2020

Page 6

Available on the CoT Website

[www.charteroftrust.com](http://www.charteroftrust.com)



## Content deep dive

# Principle 6 – Brochure and newly launched website help small and medium sized enterprises in their efforts towards more Cybersecurity

- Target group: Small and Medium-sized Enterprises
- Content: Concrete step-wise approach towards a stronger setup for Cybersecurity
- Statistical data with “relevance” for German based SME’s
- Language: Available in German (and English translation)

Available on the CoT Website

[www.charteroftrust.com](http://www.charteroftrust.com)





Let's take it  
to the next level.  
Ready?

# 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

[www.charteroftrust.com](http://www.charteroftrust.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.

If you have questions about our  
Charter of Trust initiative on Cybersecurity

To learn more, visit the CoT website  
[www.charteroftrust.com](http://www.charteroftrust.com)

Follow the Charter of Trust on  
[Twitter](#) and [LinkedIn](#)



## Contact our Secretariat

Reach us by email:  
[secretariat@charteroftrust.info](mailto:secretariat@charteroftrust.info)

## 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 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 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 Cyber-resilience through conformity and certification

Companies and – if necessary – governments ensure cyber-resilient products, systems, services and processes through conformity assessments including e.g., verification by independent parties.

#### 08 Transparency and response

Maintain and expand a network of experts who share new insights and information on incidents to foster collective cybersecurity; engage with regulators and other stakeholders on threat intelligence sharing policy and exchange best practices.

#### 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