Driving security in an insecure world

The Charter of Trust
Cybersecurity is becoming more and more urgent.
There is a strong need to act! That’s why: There is a strong need to act!

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
Together with strong global partners, we have initiated the Charter of Trust.
And we came up with 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 Certification for critical infrastructure and solutions
08 Transparency and response
09 Regulatory framework
10 Joint initiatives
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 two years ago are excellent new forms of stakeholders working together for more Cybersecurity by joining forces.”
Two years of collaboration are showing results

Together we scale Supply Chain Security.

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

We drive Cybersecurity education.

We shape the harmonization of regulation and standardization.

We turn Cybersecurity into a real business opportunity.
Two years of collaboration are showing results – details

Together we scale Supply Chain Security.

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

We drive Cybersecurity education.

We shape the harmonization of regulation and standardization.

We turn Cybersecurity into a real business opportunity.

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

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

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.

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

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

<table>
<thead>
<tr>
<th>Messages</th>
<th>Principles</th>
<th>Objectives (as defined in Taskforce Integration Team)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Together we scale Supply Chain Security</td>
<td>Ownership for IT and OT cybersecurity</td>
<td>N/a</td>
</tr>
<tr>
<td></td>
<td>P1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Responsibility through the digital supply chain</td>
<td>• Define <strong>baseline requirements</strong> to secure products and services along our supply chain 1)</td>
</tr>
<tr>
<td></td>
<td>P2</td>
<td>• Establish <strong>risk-based methodology</strong> and <strong>verification</strong> for implementing baseline requirements in our own supply chains</td>
</tr>
<tr>
<td>We are convinced: Security by Default will be a must-have across all our businesses</td>
<td>Security by default</td>
<td>• Define <strong>critical Cybersecurity requirements</strong> needed to deliver secure products, processes, services and business models.</td>
</tr>
<tr>
<td></td>
<td>P3</td>
<td>• Establish <strong>verification methodology</strong> in order to provide assurance of the requirements being adequately met</td>
</tr>
<tr>
<td>We drive Cybersecurity education</td>
<td>User-centricity</td>
<td>N/a</td>
</tr>
<tr>
<td></td>
<td>P4</td>
<td></td>
</tr>
<tr>
<td>We shape the harmonization of regulation and standardization globally</td>
<td>Innovation and co-creation</td>
<td>N/a</td>
</tr>
<tr>
<td></td>
<td>P5</td>
<td></td>
</tr>
<tr>
<td>We turn Cybersecurity into a real business opportunity</td>
<td>Education</td>
<td>• Define <strong>internal requirements</strong> and <strong>external recommendations</strong> on cybersecurity education</td>
</tr>
<tr>
<td></td>
<td>P6</td>
<td>• Develop <strong>roll-out concepts</strong> (e.g., campaigns)</td>
</tr>
<tr>
<td></td>
<td>Certification</td>
<td>• Develop guidance on how to earn and sustain trust through international standards and certification</td>
</tr>
<tr>
<td></td>
<td>P7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparency and response</td>
<td>• Explore / establish information sharing policies relevant for CoT Partners</td>
</tr>
<tr>
<td></td>
<td>P8</td>
<td>• Create human network, supported by TI sharing solution</td>
</tr>
<tr>
<td></td>
<td>Regulatory framework</td>
<td><strong>N/a (Communicate and advocate)</strong> content developed by other Taskforces e.g., via new website</td>
</tr>
<tr>
<td></td>
<td>P9</td>
<td><strong>N/a (Operationally steer)</strong> overall CoT work</td>
</tr>
<tr>
<td></td>
<td>P10</td>
<td></td>
</tr>
</tbody>
</table>

1) For next generation products & solutions June 2020

Deep Dive (next page)
Principle 2 – Common risk-based approach for the Digital Supply Chain

External communication package released

Available on the CoT Website

www.charteroftrust.com
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)
- Publishing date: MSC 2020

Available on the CoT Website

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.
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

Contact our Secretariat

Reach us by email: cotsecretariat@portland-communications.com

Benoit Roussel
Partner

Paula Iwaniuk
Director

Jefferson Alava Salas
Director

The Charter of Trust Secretariat is provided by:

Portland
A critical factor for the success of the digital economy

**Key Principles**

**Charter of Trust for a secure digital world**

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