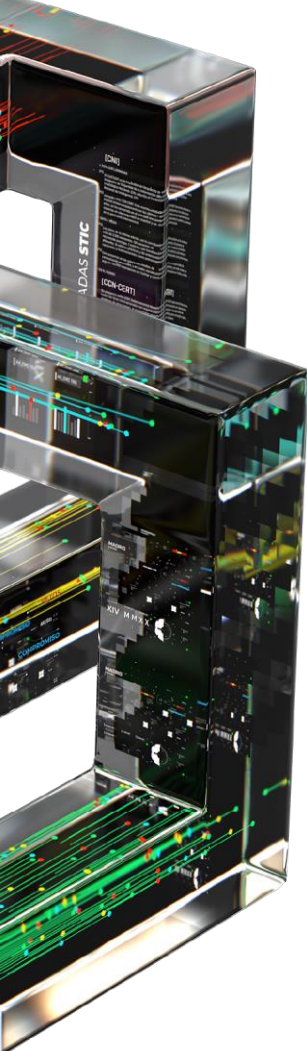
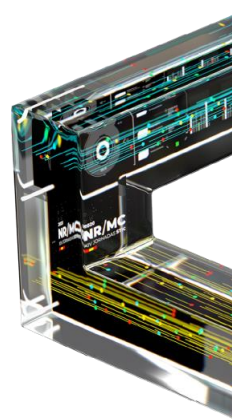




#XIVJORNADASCCNCERT

**Introducción al Charter of Trust,
Estrategia Española de
Ciberseguridad y problemas en la
cadena de suministro**





**Charter
of Trust**

Lucio González Jiménez (SGS)
M^a del Pino Glez. Junco (Siemens)
Arancha Jiménez Martínez (Atos)
Maik Holzhauer (Siemens)
Susana del Pozo Rodríguez (IBM)
Jose Rubio Tora (Siemens)

Charter of Trust

contact@charteroftrust.info



**Charter
of Trust**

Driving security in an insecure world

The Charter of Trust

Cybersecurity is
becoming more and more
urgent.

The Covid-19 pandemic further underpins the need to act

The digital infrastructure has never supported more people than it does today – many of them working from home.

It has become a **crucial factor for business continuity and for society overall.**

When the Covid-19 outbreak scaled to a global pandemic, malicious actors started **increasingly targeting individuals and organizations** with malware and ransomware.

Now more
than ever:

We need individual efforts and more importantly **collaboration** to ensure the **digital security of our lives.**

Together with strong
global partners,
we have initiated the
Charter of Trust.



And we came up with ten principles.



Associated Partner Forum



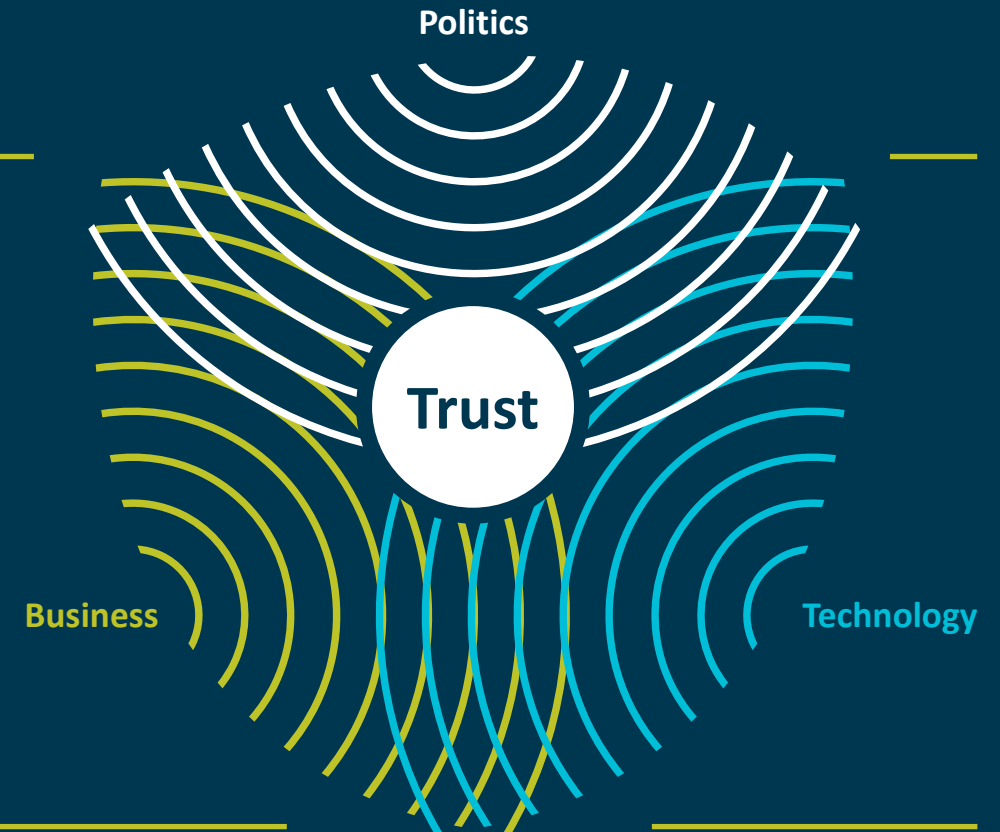
- 01 Ownership of cyber and IT security
- 02 Responsibility throughout the digital supply chain
- 03 Security by default
- 04 User-centricity
- 05 Innovation and co-creation
- 06 Education
- 07 Certification for critical infrastructure and solutions
- 08 Transparency and response
- 09 Regulatory framework
- 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.**



Two 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.

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.”





**Charter
of Trust**

How is Siemens
adopting CoT Principles?



“We want the best companies in each industry to be part of our Charter of Trust and work together on a common set of priorities on what needs to be done.”

Joe Kaeser

Former CEO Siemens AG
Initiator of the Charter of Trust





“Cybersecurity must become part of the DNA of every organization, like it is for quality in outperforming companies.”

Dr. Roland Busch

CEO Siemens AG, Former CTO, CHRO
Former Board of Directors member Siemens AG
of the Charter of Trust

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	- Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data - Data shall be protected from unauthorized access throughout the data life cycle - The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	- Security policies consistent with industry best practices such as ISO27001, ISO20481, SOC2, IEC62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/segmentation, operational security, physical security, vendor management) - Guidelines on secure configuration, operation and usage of products or services shall be available to customers - Policies and procedures shall be implemented so as not to consent to include back doors, malware and malicious code in products and services
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer and Separation	- Encryption and key management mechanisms shall be available, when appropriate, to protect data - Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	- Regular security scanning, testing and remediation of products, services and underlying infrastructure shall be performed - Asset management, vulnerability management and change management policies shall be implemented that are capable of mitigating risks to service environments - Business continuity and disaster-recovery procedures shall be in place and shall incorporate security during disruptions, where applicable - A process shall be in place to ensure that products and services are authentic and identifiable
Support	- The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available - Based on risk and during the time frame of support, processes shall be in place for: - Contacting Support - Security Advisories - Vulnerability Management - Cybersecurity-related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g. through training, certifications, awareness)

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 TSCs	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.charteroftrust.com

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

Page 6

Available via CoT Website

www.charteroftrust.com

And we bring them to life as

Principle 2 — Responsibility throughout the digital supply chain

The Siemens security concept
defense-in-depth



SIEMENS
Ingenuity for life

Concrete implementation steps at Siemens

Siemens provides a **multilayered concept** that gives plants both **all-round and in-depth protection**



Know-how and
copy protection



Authentication and
user management



Firewall and VPN
(Virtual Private Network)



System hardening and
continuous monitoring

Concrete implementation steps with the CoT partners

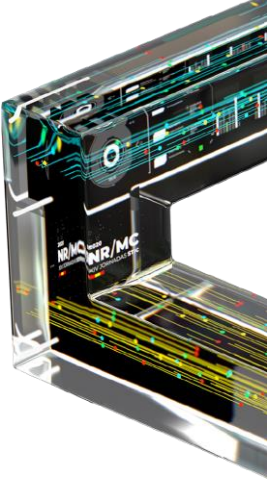
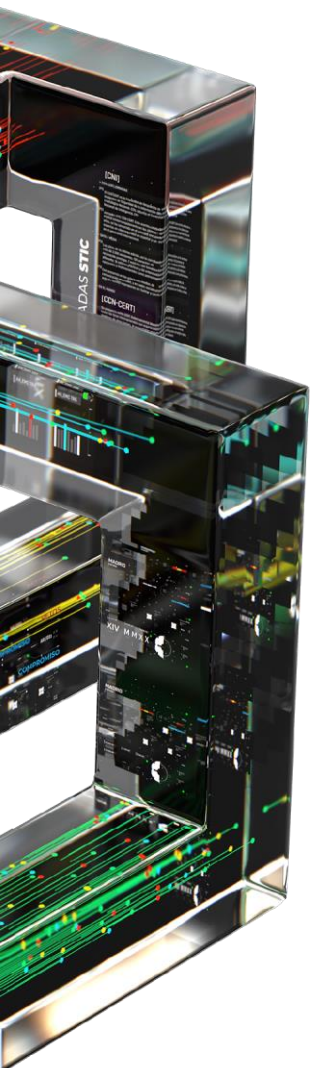
With our partners, we defined a **list of minimum baseline requirements** for all players in the supply chain as well as effective **mechanisms** that can **support their implementation**



**Charter
of Trust**

Thank you for your attention.

Any questions?



MUCHAS GRACIAS

#XIVJORNADASCCNCERT