




**Charter
of Trust**

Charter of Trust Webinar

Task Force P3 - Security by Default



This webinar will be recorded
and made available on the
Charter of Trust website
(www.charteroftrust.com).

Agenda

1. Opening address and introduction to the Charter of Trust

Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) and CEO Business Unit Cybersecurity Services, TÜV SÜD; Task Force Lead, Principle 3 “Security by Default”

2. Introduction of the panellists

Moderator: **Sudhir Ethiraj**, Global Head of Cybersecurity Office (CSO) and CEO Business Unit Cybersecurity Services, TÜV SÜD

Veronica Tan, Director Safer Cyberspace Division, Cyber Security Agency of Singapore (CSA)

S.S. Sarma, Senior Director, Indian Computer Emergency Response Team (CERT-In)

Ashutosh Bahuguna, Scientist, Indian Computer Emergency Response Team (CERT-In)

Amitava Mukherjee, Director Cybersecurity, Siemens Ltd. India

Ki Hyun Park, Senior IT Security Analyst, Mitsubishi Heavy Industries

Didier Ludwig, Cybersecurity Officer, Siemens

3. Panel Discussion on major Cybersecurity Regulations in Asia

4. Q&A with audience



Charter
of Trust

The Charter of Trust has ten principles.



Associated Partners 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



**Charter
of Trust**

Security-by-Default Definition

“Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.”

The three phases of Security by Default at the Charter of Trust

Phase 1

- Products
- Functionalities
- Technologies



Phase 2

- Processes
- Operations
- Architectures



Phase 3

- Sharing of Best Practices for Security by Default adoption

Principle 3 – Previous publications

Requirements for products, functionalities, technologies

Principle 3 - Phase 1 “Products, Functionalities, Technologies” Baseline Requirements

Baseline Requirements	Description
Unique identity	Assets shall be uniquely identifiable.
Secure onboarding	When an asset is being onboarded into an environment the asset shall be able to assert its unique identity.
Secure credentials	Universal default, hardcoded and weak credentials shall not be used.
Login protection	Either the asset or the system will implement account lockout or an authentication back off timer.
Access control	Assets shall include strong authentication mechanisms and have them enabled by default.
Secure storage	Authorization shall be used to ensure legitimate use and mediate attempts to access resources in/from a system.
Secure communications	Storage for security-sensitive data shall be secured.
Minimize attack surface	Sensitive data and system information, including management and control process data shall be protected while in transit.
Secure data deletion	Security features shall be enabled by default and functionalities that are not required or are insecure shall be disabled by default.
Backup feature	Manufacturers shall provide functionality for customers to securely wipe customer data.
Security documentation	Relevant assets shall provide a backup feature for data.
Validate input data	Manufacturers shall provide a comprehensive security guide for the asset which details minimal steps and follows security best practices on usability.
Password changed on first use	All input data shall be validated prior to use by the asset.
Secure updates	Relevant assets shall force a password change during the initial setup.
Telemetry & event monitoring	Assets shall have the ability to securely update and remove / mitigate vulnerabilities and bugs, during their lifecycle, in a timely fashion.
Maintain settings after outage	Assets shall implement logging for telemetry and security related events.
Factory reset	Assets shall maintain settings after power outage.
No backdoors	Assets shall provide a means to return to original factory configuration with all customer data securely removed.
Conceal password characters	No undocumented ways to remotely connect to the asset shall be put in place by the manufacturer.
	Assets shall mask all passwords during input by default.



Explanatory Document for products, functionalities technologies



Achieving Security by Default An Explanatory Document for the Phase 1 “Products, Functionalities, Technologies” Baseline Requirements

Charter of Trust – Principle 3
CoT Public

Requirements for processes, operations and architectures

P3 Phase 2 “Processes, Operations, Architectures” Baseline Requirements

Suggested Baseline Requirements	Description
Security Management Program	A security management program based on best practices shall be established and implemented to continuously improve the security posture.
Risk Management Process	Security risk shall be managed in the organization for critical assets based on risk assessment.
Human Resources Security	Processes shall be established in Human Resources to support security management prior to and during onboarding, as well as offboarding, of personnel.
Training	A minimum level of security education and training on key security issues shall be regularly deployed for employees.
Asset Management	Policies and procedures shall be in place for the management of assets throughout their lifecycle, including onboarding, changes and offboarding.
Identity and Access Management	Access to assets shall be limited to authorized identities only for the time needed, and managed based on risk and the principle of least privilege.
Credentials Management	Organizations shall have a process of enforcing current security best practices to manage credentials and cryptographic material throughout their entire lifecycle.
Physical Security	Physical security shall be in place to protect assets by providing access control and protecting information.
Security Documentation	Process shall be in place to ensure proper and accessible security documentation, including information about capabilities, risks and mitigation strategies.
Continuous Monitoring	Robust monitoring for critical assets shall be put in place for all relevant events and logged information shall be protected.
Vulnerability Management	A Vulnerability Management Process shall be established for the duration of the support lifecycle of assets, including the collection of vulnerability notifications, proactive monitoring, responding to vulnerabilities and related communication. Security updates shall be implemented to address vulnerabilities in a timely, transparent and secure manner throughout the entire asset lifecycle.
Threat Identification and Mitigation	Procedures and policies shall be in place to monitor, identify and monitor threats to assets.
Segmentation	Physical and logical segmentation shall be in place to minimize security risks and to protect critical assets.
Secure Development Lifecycle	Policies and procedures shall be in place for secure development best practices to ensure the integrity of the developed assets and minimize vulnerabilities.
Security Incident Management	Policies and procedures for the management of security incidents shall be established to mitigate risks and minimize damage should an incident occur.
Business Continuity and Disaster Recovery	Policies and procedures shall be in place to identify, maintain and re-establish necessary business operations in a timely manner, including ensuring of proper restoration of data and services in case of disruption.
Security Auditing	Regular and ad hoc internal and external security audits/assessments shall take place to verify for compliance with company security policies and relevant regulations.



Available on the CoT Website

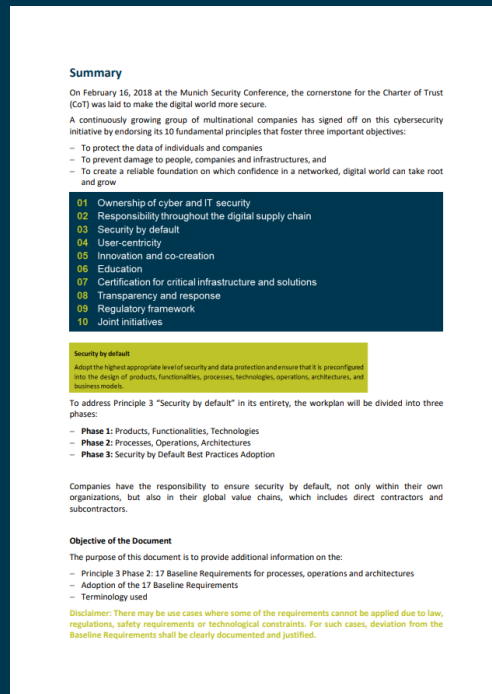
www.charteroftrust.com

June 10, 2025

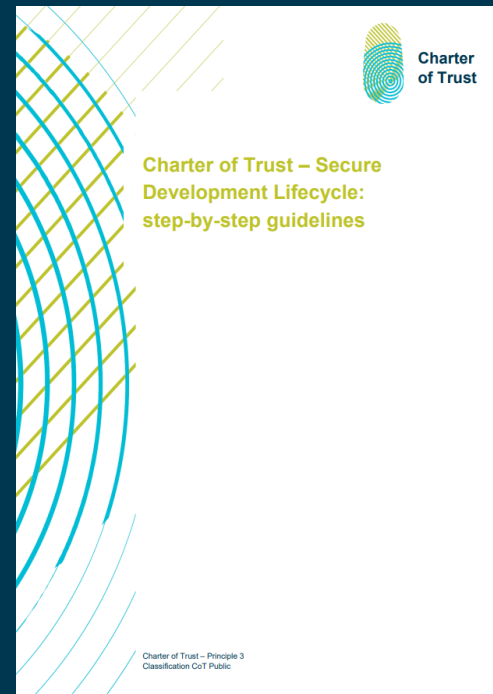


Principle 3 – Previous publications

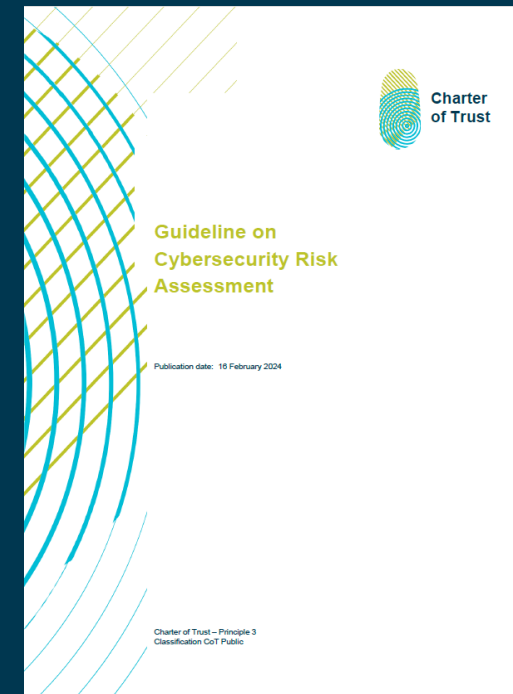
Explanatory Document for processes, operations and architectures



Secure Development Lifecycle: step-by-step guidelines



Guideline on Cybersecurity Risk Assessment



Available on the CoT Website

www.charteroftrust.com

June 10, 2025

Principle 3 – Latest Publication on “Security by Default in view of major Cybersecurity Regulations”



Available on the CoT Website

www.charteroftrust.com

“Security by Default in view of major Cybersecurity Regulations in Asia”

Webinar on June 10th from 13:00 to 14:30 CEST

Our speakers



Sudhir Ethiraj

Global Head of
Cybersecurity Office

TÜV SÜD



Didier Ludwig

Cybersecurity
Officer

Siemens



Ki Hyun Park

Senior IT Security
Analyst

Mitsubishi Heavy
Industries



Veronica Tan

Director Safer
Cyberspace Division

Cyber Security
Agency of Singapore
(CSA)



S.S. Sarma

Senior Director

**Ashutosh
Bahuguna**

Scientist

Indian Computer
Emergency Response
Team (CERT-In)



**Amitava
Mukherjee**

Director
Cybersecurity

Siemens Ltd. India

FOCUS: INDIA, JAPAN & SINGAPORE



**Charter
of Trust**



**Charter
of Trust**

Questions & Answers



**Charter
of Trust**

Thank you for attending!