Charter of Trust

# Achieving Security by Default

## An Explanatory Document for the Phase 1 “Products, Functionalities, Technologies” Baseline Requirements

# 1 Summary

On February 16, 2018 at the Munich Security Conference, the cornerstone for the Charter of Trust (CoT) was laid to make the digital world more secure.

A continuously growing group of multinational companies has signed off on this cybersecurity initiative by endorsing its 10 fundamental principles that foster three important objectives:

- To protect the data of individuals and companies
- To prevent damage to people, companies and infrastructures, and
- To create a reliable foundation on which confidence in a networked, digital world can take root and grow

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

Companies have the responsibility to ensure security by default. This is **the focus of Principle 3.**

**Security by default**

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.

To address Principle 3 “Security by default” in its entirety, the workplan will be divided into three phases:

- **Phase 1:** Products, Functionalities, Technologies
- **Phase 2:** Processes, Operations, Architectures
- **Phase 3:** Business Models

The objective of this Explanatory Document is to define the critical cybersecurity requirements needed to deliver secure products, processes, services and business models. Such requirements must be verifiable in order to provide assurance that the requirements are being met adequately.

Meanwhile, the scope of this document is limited to the Phase 1 Baseline Requirements that cover products, functionalities and technologies. For the subsequent phases, Phase 2 (processes) and Phase 3 (business models), baseline requirements and explanatory documents will be completed at a later stage.

The scope is also limited to cybersecurity (including data protection) for networked assets. While privacy, safety and Artificial Intelligence (AI) / Machine Learning (ML) are all important topics, at this stage, they are not part of Principle 3.

Based on this statement, Charter of Trust members developed a list of 19 Baseline Requirements, based on existing international guidelines[1] to provide companies with guidance on how to embed security into the design of products, functionalities and technologies.

**Disclaimer: There may be use cases where some of the requirements cannot be applied due to law, regulations, safety requirements or technological constraints. For such cases, deviation from the Baseline Requirements shall be clearly documented and justified.**

The purpose of this document is to provide additional information on the:

- Taskforce approach for Principle 3 Phase 1
- Terminology used and
- 19 Baseline Requirements for products, functionalities and technologies.
- The adoption of the 19 Baseline Requirements as a guidance document.

# 2 Explanation on the Phase 1 Approach

## 2.1 Audience

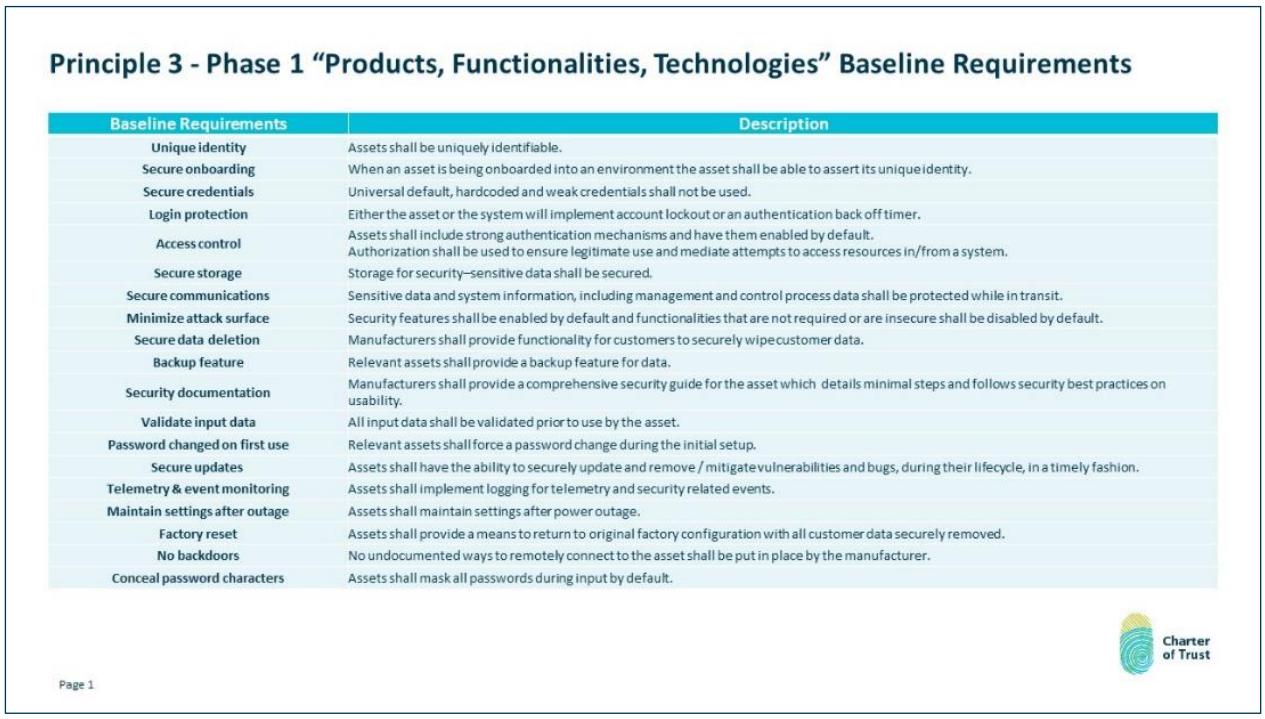
- Current Charter of Trust Members
- Future Members of the Charter of Trust and
- Other stakeholders that will implement the Baseline Requirements.

[1] NIST, ENISA, ETSI, IEC, Japan Terminal Device Certification

## 2.2 Terminology

| | |
|---|---|
| **Asset**: | Anything that is valuable to an organization or consumer that requires protection against cyber threats.<br>**Relevant Asset Categories:**<br>**Examples of assets that are relevant:**<br>– Digital information<br>– Physical device (networked or standalone)<br>– Supporting software and applications<br>**Examples of assets that are irrelevant:**<br>– Paper-based information<br>– Building without technology |
| **Baseline Requirements:** | Mandatory set of requirements to reach an acceptable level of cybersecurity. |
| **Guidance:** | "the act or process of guiding. Direction/Advice/Controlling course." |
| **Guidelines:** | "a line by which one is guided -> an indication or outline of policy or conduct." |
| **Testable:** | "capable to be tested." |
| **Tested:** | "subjected to or qualified through testing." |
| **Verifiable:** | "capable of being verified." |

# 3 Phase 1 "Products, Functionalities and Technologies" Baseline Requirements



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.<br>Authorization shall be used to ensure legitimate use and mediate attempts to access resources in/from a system. |
| Secure storage | Storage for security–sensitive data shall be secured. |
| Secure communications | Sensitive data and system information, including management and control process data shall be protected while in transit. |
| Minimize attack surface | Security features shall be enabled by default and functionalities that are not required or are insecure shall be disabled by default. |
| Secure data deletion | Manufacturers shall provide functionality for customers to securely wipe customer data. |
| Backup feature | Relevant assets shall provide a backup feature for data. |
| Security documentation | Manufacturers shall provide a comprehensive security guide for the asset which details minimal steps and follows security best practices on usability. |
| Validate input data | All input data shall be validated prior to use by the asset. |
| Password changed on first use | Relevant assets shall force a password change during the initial setup. |
| Secure updates | Assets shall have the ability to securely update and remove / mitigate vulnerabilities and bugs, during their lifecycle, in a timely fashion. |
| Telemetry & event monitoring | Assets shall implement logging for telemetry and security related events. |
| Maintain settings after outage | Assets shall maintain settings after power outage. |
| Factory reset | Assets shall provide a means to return to original factory configuration with all customer data securely removed. |
| No backdoors | No undocumented ways to remotely connect to the asset shall be put in place by the manufacturer. |
| Conceal password characters | Assets shall mask all passwords during input by default. |

Charter of Trust

Page 1

Reference: https://www.charteroftrust.com/wp-content/uploads/2020/05/200212-P3-Phase-1-Baseline-Requirements_FINAL.pdf

## 3.1 Categorization by NIST Functions

The **19 Baseline Requirements** are grouped in the following five key domains that reflect NIST Function categories:

1. **Identify**
2. **Protect**
3. **Detect**
4. **Respond**
5. **Recover**

NIST explains[2] each key domain requirement in the following manner:

1. *"The **Identify Function** assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources*

[2] *https://www.nist.gov/cyberframework/online-learning/five-functions*

*that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs."*

2. *"The **Protect Function** outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event."*
3. *"The **Detect Function** defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events."*
4. *"The **Respond Function** includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident."*
5. *"The **Recover Function** identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident."*

# 4 The Baseline Requirements Explained

**Please note that these are Baseline Requirements. However, certain cases will need additional requirements based on the evaluation of benefits and risks.**

## IDENTIFY

**1. Unique Identity: Assets shall be uniquely identifiable.**

- To ensure that an asset inventory can be established and leveraged for visibility and security purposes, (e.g. for incident response capabilities), all assets should be uniquely identifiable digitally.
- This would be important, for example, during forensic analysis. This is also valid for virtual assets, e.g. virtual machines, containers, software and bots.

## PROTECT

**2. Secure Onboarding: When an asset is being onboarded into an environment the asset shall be able to assert its unique identity.**

- To ensure the secure onboarding of assets, they should have the capability to assert their unique identity and to allow them to be inventoried.

**3. Secure Credentials: Universal default, hardcoded and weak credentials shall not be used.**

- Assets should not have universal default credentials. A universal default credential is, for example, the same vendor defined password that is used across assets.
- Assets with default or no credentials should force the user to setup unique credentials before use (e.g. password, fingerprints, voice/face authentication). For BIOS passwords, changing the default credentials should be considered based on the actual use case and risk (e.g. consumer, laptops). Credentials should be managed securely throughout the asset's lifecycle.

- A secure authentication mechanism is recommended. Depending on the risk acceptance level, a specific authentication method might be more appropriate than another. Credentials should be used according to current best practices. Hardcoded credentials should not be used.

4. **Login Protection: Either the asset or the system will implement account lockout or an authentication back-off timer.**
   - The purpose of this requirement is to prevent authentication attacks such as brute force log-in. The assets should implement accounts' back-off timer or lockouts.
   - If login protection is not enforced, such as for safety relevant use cases, occasions or events, compensating security measures should be set-up.
   - It is suggested that locked accounts are not unlocked until a second level authentication is asserted.
5. **Access control: Assets shall include strong authentication mechanisms and have them enabled by default. Authorization shall be used to ensure legitimate use and mediate attempts to access resources in/from a system.**
   - Strong authentication mechanisms based on state-of-the-art technologies and current best practices should be in place.
   - If Multi-Factor Authentication is available, it should be enabled by default.
   - Identification and authentication should be done by different entities different from the asset itself.
   - Access to and by assets should follow an authorization model structured according to current best practices (e.g. role-based access control, attribute/context-based access control, adaptive access control).
   - To ensure legitimate access to assets, authentication and authorization are used. Authentication and authorization are part of secure onboarding and should be supported by the asset.
   - Authentication verifies the identity of the entity requesting access to the assets. Authorization ensures that the level of access to an asset is determined by access rights and should enforce the principle of least privilege.
6. **Secure storage: Storage for security–sensitive data shall be secured.**
   - To protect the confidentiality and integrity of security sensitive information, it should not be stored in plaintext form. Appropriate protection mechanisms should leverage proven cryptographic methods.
7. **Secure Communications: Sensitive data and system information, including management and control process data, shall be protected while in transit.**
   - Sensitive data and system information, namely confidentiality, integrity and non-repudiation, including management and control process data, should be protected while in transit during all network communications. This should follow the current standards and guidance for the protocol(s) implemented, with current cryptographic protocols, according to local legislation.
   - Sensitive data and system information, including management and control process data, should be protected while in transit during all communications as defined by the current standard and guidance for the protocol(s) implemented.
8. **Minimize attack surface: Security features shall be enabled by default and functionalities that are not required or are insecure shall be disabled by default.**

To minimize the attack surface:

- Security features should be enabled by default.
- Functionalities that are not necessary and are deemed insecure should be disabled by default, e.g. disabling network ports, USB ports.
- Software services that are not secure should be removed by default. If necessary, for certain use cases, unsecure services should be disabled by default. Examples may include backwards compatibility and/or support legacy use cases.
- If necessary, certain features may still be enabled, for example, in case of compatibility reasons.

9. **Secure Data Deletion: Manufacturers shall provide functionality for customers to securely wipe customer data.**
   - This functionality will be necessary in case of transferring the ownership of an asset to guarantee the confidentiality of the previous owner's data.
   - The functionality should be provided according to current best practices to securely erase data.
10. **Backup feature: Relevant assets shall provide a backup feature for data.**
    - The goal of this baseline requirement is to ensure availability of asset data.
    - The term "relevant" refers to the risk-based approach as some use cases require higher levels of availability than others.
    - A backup feature should also include restoration capability throughout the asset lifecycle.
    - The risk-based approach will define what data needs to be backed up, e.g. device configurations, and what does not need to be backed up, e.g. operational data being generated by the asset.
    - If the backup contains security-sensitive data, it should be protected according to current best practices.
11. **Security Documentation: Manufacturers shall provide a comprehensive security configuration guide for the asset which details minimal steps and follows security best practices.**
    - The security documentation should support a user to securely set-up, operate and maintain the security of the asset along its lifecycle.
    - The security documentation should reflect current standards and best practices.
12. **Validate Input Data: All input data shall be validated prior to use by the asset.**
    - Assets should validate all input data received via user interfaces, APIs or networks before use.
    - Input validation should follow secure development best practices.
13. **Password changed on first use: Relevant assets shall force a password change during the initial setup.**
    - All password-enabled assets should force a password change during the initial setup. The asset should force a password change to a strong, new password during the first time it is in use, otherwise only functionalities related to the password setup or emergency features should be available.
    - The asset should enforce a strong password policy according to current best practices.
14. **Secure Updates: Assets shall have the ability to securely update and remove / mitigate vulnerabilities and bugs, during their lifecycle, in a timely fashion.**
    - Assets should have the ability to be securely updated.

- It should be possible to remove or mitigate vulnerabilities and bugs during the asset's lifecycle in a timely fashion.
- For assets with no possibility of a software update, the conditions for their replacement period support should be clear.

**15. Maintain settings after outages: Assets shall maintain settings after power outage.**

- Resilience should be built-in to assets, so they do not revert to default settings if power goes out.
- In case of critical services, backup power should be provided to keep the service running for as long as it is reasonably needed.
- Services should recover without discrepancies in case of restoration due to / after a loss of power or network access.

**16. No Backdoors: No undocumented ways to remotely connect to the asset shall be put in place by the manufacturer.**

- The creation of "backdoors" in assets compromises security. Additionally, it impairs customer relationship and trust. No backdoors include local and remote access.
- All ways to connect to the asset should be documented and made available to the customer to ensure transparency.

**17. Conceal password characters: Assets shall mask all passwords during input by default.**

- Every time that typing a password is required, the input box should mask the characters as they are entered. The individual characters of the password should be hidden or replaced by one or more characters such as an asterix "*".
- Under certain circumstances, the asset may provide a feature that permits displaying the characters during input.

## DETECT

**18. Telemetry & Event Monitoring: Assets shall implement logging for telemetry and security related events.**

- Assets should implement logging of information (including security related events, log-in sessions and authentication requests) for forensic capability and telemetry.
- This enables detection of anomalous behaviour and can provide the necessary visibility for incident response.
- Assets with no possibility of logging should support a system to implement logging to the extent possible. An example is the generation of a security related event that is treated in another layer, e.g. SmartCard generates a failed login attempt event, the SmartCardOS sends this event to the Operating System and the event is logged within the Operating Systems Event Logs.

## RECOVER

**19. Factory Reset: Assets shall provide a means to return to original factory configuration with all customer data securely removed.**

- Security sensitive data to be deleted should include personal user data, account data, credentials and configuration data. Assets shall only go back to their default/non-existent credentials after a factory reset that will trigger setup mode.

– A factory reset mechanism must be documented enabling the user to execute the factory reset if needed. The factory reset mechanism could be protected by an authorization step. On the other hand, inadvertent use of the factory reset functionality must be prevented.

# 5 Mapping to international standards and current best practices

**Mapping**

| NIST Function | Suggested Baseline Requirements | NIST 8228 | NIST CyberSec Fram | ENISA Baseline Sec Rec | ETSI TS 103 645 | IEC 62443 | Japan Terminal Device Cert | Principle 2 – Charter of Trust Responsibility throughout the digital Supply Chain |
|---|---|---|---|---|---|---|---|---|
| Identify | Unique Identity | x | x | x | | x | | x |
| Protect | Secure Onboarding | x | x | | | x | | |
| Protect | Secure Credentials | x | x | x | x | x | | |
| Protect | Login Protection | x | x | | | x | | |
| Protect | Access control | x | x | x | | x | x | x |
| Protect | Secure storage | x | x | | x | x | | |
| Protect | Secure Communications | x | x | | x | x | | x |
| Protect | Minimize attack surface | x | x | | x | x | | |
| Protect | Secure Data Deletion | x | x | | x | x | | |
| Protect | Backup feature | x | x | | | x | | |
| Protect | Security Documentation | x | x | | x | x | | x |
| Protect | Validate Input Data | x | | | x | x | | |
| Protect | Password changed on first use | x | x | x | | x | x | |
| Protect | Secure Updates | x | x | | x | x | x | |
| Detect | Telemetry & Event Monitoring | x | x | | x | x | | |
| Protect | Maintain settings after outage | | | | x | x | x | |
| Recover | Factory Reset | | x | | | x | | |
| Protect | No Backdoors | | | | x | x | | x |
| Protect | Conceal Password characters | x | | | | x | | |

# 6 Adoption

Each CoT member will be responsible for driving the adoption of Phase 1 Baseline Requirements for relevant next generation products starting in 2020.