# Achieving Security by Default

An Explanatory Document for the Phase 2
“Processes, Operations, Architectures”
Baseline Requirements

## 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

**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:** Security by Default Best Practices Adoption

Companies have the responsibility to ensure security by default, not only within their own organizations, but also in their global value chains, which includes direct contractors and subcontractors.

**Objective of the Document**

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

- Principle 3 Phase 2: 17 Baseline Requirements for processes, operations and architectures
- Adoption of the 17 Baseline Requirements
- Terminology used

**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.**

# Explanation of the Phase 2 Approach

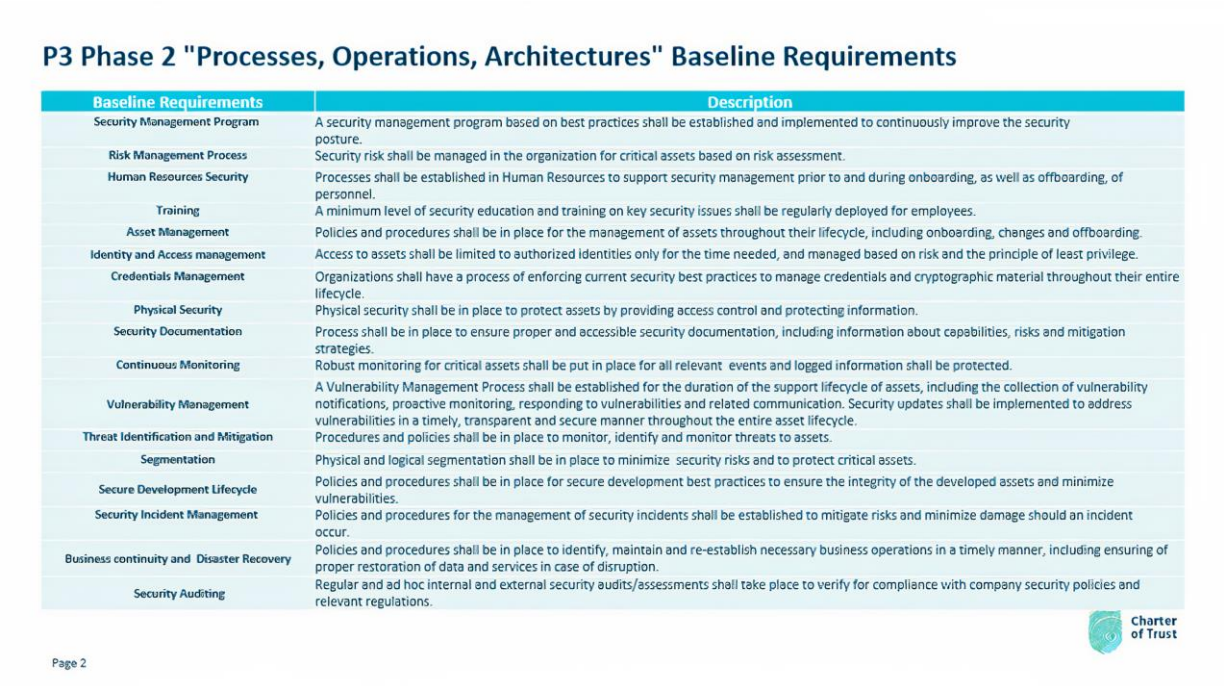
## Audience

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

## 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. |
| **Disaster:** | "Disaster" includes "cybersecurity incidents" |
| **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 of being tested." |
| **Tested:** | "subjected to or qualified through testing." |
| **Verifiable:** | "capable of being verified." |

# Phase 2 “Processes, Operations and Architectures” Baseline Requirements



P3 Phase 2 "Processes, Operations, Architectures" Baseline Requirements

| 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. |

Charter of Trust

Page 2

# 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.**

### *1.* Security Management Program

Requirement: A security management program based on best practices shall be established and implemented to continuously improve the security posture.

The organization shall establish, implement, maintain and continually improve security policies, processes and procedures for the entire lifecycle of assets within the following areas:

- Asset Management
- Risk Management
- Business Continuity and Disaster Recovery
- Human Resources Security including Security Education
- Identity and Access Management
- Credentials Management
- Physical Security
- Operations Security including Continuous Monitoring and Security Updates
- Threat Identification and Mitigation including Segmentation
- Secure Development Lifecycle
- Vulnerability Management
- Security Incident Management
- Security Auditing

- Supplier Management (see requirements defined by the Charter of Trust principle 2 “Responsibility throughout the digital supply chain”)

## 2. Risk Management Process

Requirement: Security risk shall be managed in the organisation for critical assets based on risk assessment.

Explanation:

- The organisation should define and apply an information security risk assessment process.
- It should identify, evaluate and analyse security risks and establish a process for risk treatment.
- Security risk for critical assets shall be identified and a risk treatment plan shall be implemented.
- Supplier risk should be managed according to the requirements defined by the Charter of Trust principle 2 “Responsibility throughout the digital supply chain. ”

## 3. Human Resources Security

Requirement: Processes shall be established in Human Resources to support security management prior to and during onboarding, as well as offboarding, of personnel.

Explanation:

- Pre-employment verification shall be done in accordance with the relevant laws and regulations proportional to the risk associated to the candidate’s role.
- Employee/contractor contract terms and conditions shall comply with an organization’s security policies.
- Confidentiality agreements shall be in place with employees/contractors.
- A segregation of roles/duties shall be considered where relevant to reduce the risk of fraud, employee sabotage or financial loss.
- Employees/contractors shall receive security awareness training according to their role within the organization.
- Processes for job termination shall be established to ensure that assets are returned by employees/contractors and privileges are removed in a timely manner.

## 4. Training

Requirement: A minimum level of security education and training on key security issues shall be regularly deployed for employees.

Explanation:

- The company should regularly provide its employees with appropriate security training in conjunction with the company’s security framework and according to their respective tasks and area(s) of responsibility, at least once per year.
- The company should assure that its employees are familiar with the content and the implementation of applicable security rules and that they can identify and report security incidents in their task area.
- Executives should promote awareness for security by ensuring that security training and awareness measures are carried out and participated in.

- During onboarding process, new employees should pass security training to get a sense of right and wrong, security awareness and security competences according to the requirements of their roles.
- Training in security awareness is a prerequisite for successful implementation of the security framework and to achieve:
    - Compliance with regulations, procedures and policies.
    - Increase employees´ knowledge and competencies concerning threats, risks and security options.
    - Change and maintain employees´ security behaviour and build a more security-aware culture.

## 5. Asset Management

Requirement: Policies and procedures shall be in place for the management of assets throughout their lifecycle, including onboarding, changes, and offboarding.

Explanation:

- The purpose of asset management is to provide necessary and current information about assets, which is a prerequisite for many other requirements.
- Asset management should distinguish at least between “information assets” (the information itself) and “supporting assets” (e.g., the hardware assets where the information manifests, such as a hard disk, a piece of paper, the network wire, etc.).
- The information asset is of value for an organization. This value determines the necessary level of protection. This level of protection needs then be applied for all supporting assets where this information resides.
- The manufacturer/vendor should document the support status of the asset.
- At the end of the supported security lifecycle, the asset owner should assess if the asset has to be phased out and e.g., substituted.

## 6. Identity and Access Management

Requirement: 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.

Explanation:

- Identity and Access Management includes processes, policies, and a supporting technical infrastructure to manage and operate human and non-human access to assets.
- Processes and operations shall be defined and implemented to guarantee that assets can be accessed only by authorized identities.
- This includes identification, authentication and authorization methods for entities accessing the asset corresponding to the risk level assigned to an asset.
- Access to assets shall only be granted with the minimum set of access rights required for the task being performed to fulfil the principle of least privilege.
- Access to assets shall only be granted for a limited period of time, preferably dynamically for the required usage time.

## 7. Credentials Management

Requirement: Organizations shall have a process of enforcing current security best practices to manage credentials and cryptographic material throughout their entire lifecycle.

Explanation:

- Credentials, such as passwords, pins, biometric templates, tokens or certificates, should be managed securely throughout their lifecycle.
- Credentials shall be secure: universal default, hardcoded and weak/no credentials shall not be used.
- The process shall always force users to setup unique credentials before use.
- Cryptographic material, such as encryption keys, shall be managed throughout their lifecycle using best security practices.

## 8. Physical Security

Requirement: Physical security shall be in place to protect assets by providing access control and protecting information.

Explanation:

- Policies and procedures for physical security (access control and intrusion detection) should be established, covering all phases of assets' lifetime. Employees should be required to comply with these physical security policies.
- Physical security perimeters should be established to prevent unauthorized access to assets.
- Appropriate controls shall be provided at each entry point or external connection, including protection against tampering.
- Essential equipment, including security measures, should be properly maintained. Equipment providing physical security should be regularly maintained and reviewed.
- Deviation from normal physical or environmental parameters should trigger an alarm and prompt immediate response.

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

## 9. Security Documentation

Requirement: Processes shall be in place to ensure proper and accessible security documentation, including information about capabilities, risks, and mitigation strategies.

Explanation:

- Documentation for the product or service should include information about security capabilities, threats considered and addressed, known residual risks, and mitigation strategies for those risks.
- Any assumptions about the external environment should be explicitly documented.
- Guidelines should be provided for installation including hardening.
- Guidelines for operation, maintenance, monitoring, and administration should be provided.
- Disposal, reuse, and resale procedures should be given, including precautions needed to protect data privacy and confidentiality.
- If default accounts are included (including administrative access), this should be documented.
- External interfaces (networks, ports, APIs, etc.) should be listed and documented.
- Required connectivity or external dependencies should be explained.

- All documentation described here should be maintained throughout the lifetime of the product or service and made available not only to the original purchaser, but also to any subsequent owners.
- Documents could be classified based on the sensitivity of the information they contain.

## 10. Continuous Monitoring

Requirement: Robust monitoring for critical assets shall be put in place for all relevant events and logged information shall be protected.

During the operation of an asset, processes and procedures shall be implemented to ensure effective detection of and reaction to threats by continuously/regularly:

- evaluating if monitoring is operational
- verifying if derived actions are adequate and timely triggered
- checking if logged information is appropriately (i.e., Confidentiality, Integrity, Availability) protected

## 11. Vulnerability Management

Requirement: 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.

Explanation:

- As an asset owner, processes and procedures should be implemented to:
    - Follow the security description of the asset documentation in respect to Vulnerability Management.
    - Subscribe, monitor and/or regularly check for security updates.
    - Assess if updates are relevant and evaluate if mitigations are necessary.
    - Plan patching, updates and/or mitigations.
    - Inform potential affected users.
    - Patch, update and/or implement mitigations.

- As a vendor/manufacturer of an asset, processes and procedures should be implemented to:
    - Ensure up-to-date documentation of how to maintain security of the asset; this includes how security documentation and updates can be securely obtained (i.e., untampered).
    - Proactively monitor for vulnerabilities.
    - Establish an interface for reporting vulnerabilities from 3rd parties to the vendor/manufacturer.
    - Integrate and develop patches, updates, and mitigations in a timely manner to address these vulnerabilities throughout the security lifecycle of the asset.
    - Provide documentation about fixed security vulnerabilities such as documented release notes or security advisories.

- Recursively establish Vulnerability Management for embedded components in the asset and apply the output to the asset.

### 12. Threat Identification and Mitigation

Requirement: Procedures and policies shall be in place to monitor, identify and mitigate threats to assets.

The organization shall establish, implement, maintain and continually improve threat-related policies, processes and procedures for the entire lifecycle of assets, within the following areas:

- Threat monitoring at minimum based on publicly available information, involving continuous analysis and evaluation of security information, to identify and assess external and internal threat sources.
- Threat identification and assessment, consisting of timely discovering of knowledge about threat sources and vulnerabilities and analysing their potential for exploitation. When a relevant threat is identified, it needs to be handled appropriately for mitigation purposes.
- Threat mitigation, aimed to decrease the threat level of a cybersecurity event, by blocking attack opportunities through enhanced security or by reducing the impact of a potential cybersecurity incident.

### 13. Segmentation

Requirement: Physical and logical segmentation shall be in place to minimize security risks and to protect critical assets.

Explanation:

- Segmentation is based on establishing separated zones containing assets with equal protection needs and controllable communication relations to other zones.
- It helps to limit fault propagation and so it supports resilience.
- It supports the application of the need-to-know, separation of duties and least privilege good practices.
- It opens the possibility to establish redundant zones to support availability.
- Segmentation can be implemented physically or logically by separating complex structures either vertically or horizontally.

### 14. Secure Development Lifecycle

Requirement: Policies and procedures shall be in place for secure development best practices to ensure the integrity of the developed assets and minimize vulnerabilities.

Explanation:

A developed asset must implement the functionalities it was designed for with appropriate level of robustness against threats. To achieve this goal, several development best practices should be applied:

- The organization should include secure coding guidelines.
- Threat modelling to ensure that the asset is designed to resist the threats it will be exposed to.
- Vulnerability survey as a way to stay informed of the attackers' capabilities.

- Robust development methodology and tools to ensure that the final implementation corresponds to the design and security requirements.
- Validation process (including testing) to ensure that the asset behaves as specified.
- Clearly defined roles and responsibilities for Design, Development, Validation, and Acceptance.
- Configuration Management (Identity and Access Management, as described under Requirement 7) to ensure the integrity, uniqueness, and reproducibility of the design and implementation.
- Security documentation shall be provided for the asset and maintained throughout the lifecycle, such as guidelines for installation including hardening, operation, maintenance, monitoring, administration, and disposal of the asset.

## 15. Security Incident Management

Requirement: Policies and procedures for the management of security incidents shall be established to mitigate risks and minimize damage should an incident occur.

Explanation:

**Preparation**

- Possible security incidents that may significantly impact[1] business activities must be anticipated and organized.
- Develop and implement the procedure of response to manage incidents (security operation process) that includes the response of the organization, people, components and system to identify the content of response, priority, and scope of response taken after an incident occurs.
- Develop and manage rules regarding publishing information after the occurrence of the security incident.

**Identification**

- Data that is particularly important to the organization's business continuity should be checked for trustworthiness by the entity that has created and processed the data. The organization should check the received data for quality and security (e.g., checking the data for falsification or attack code).

**Containment/Recovery**

- Take appropriate measures on goods (products) where quality may be affected by security incidents, especially regarding production facilities damaged by the security incident.

**Lessons learned**

- Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.

## 16. Business continuity and Disaster Recovery

[1] Deactivation, mistaken output, employee's health and safety, negative impact on the environment etc.

Requirement: 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.

Explanation:

- The organization should assess the risk of a disaster on critical business activities.
- Business continuity plans should be developed to provide protection against loss or unavailability of critical assets and disaster recovery plans should be maintained for them.
- Plans shall be documented and tested for disasters that pose an unacceptable risk to the organization.
- Business continuity plans should be capable of delivering the contracted availability requirements to customers.

### 17. Security Auditing

Requirement: Regular and *ad hoc* internal and external security audits/assessments shall take place to verify compliance with company security policies and relevant regulations.

Explanation:

- Security audits, including internal and external audits, should take place regularly to ensure awareness and mitigation of security risks.
- The audits should include verification for compliance both with the organization's security policies, the relevant global standards such as ISO27001 and IEC62443, and with any relevant regulations as required.
- The result of such a security audit needs to be used for corrective actions and improving the security posture of the organization.

## Mapping to international standards and current best practices

### Mapping

| Suggested Baseline Requirements | NIST CSF | ENISA | IEC 62443 | METI-CPSF | SESIP | IIC | ISO27001 | Principle 2 – Charter of Trust Responsibility throughout the digital Supply Chain |
|---|---|---|---|---|---|---|---|---|
| Security Management Program | X | X | X | X | | X | X | X |
| Risk Management Process | X | X | X | X | X | X | X | |
| Human Resources Security | X | X | X | X | X | | X | |
| Training | X | X | X | X | X | X | X | X |
| Asset Management | X | X | X | X | | X | X | |
| Identity and Access Management | X | X | X | X | X | X | X | X |
| Credentials Management | X | X | X | X | X | | X | X |
| Physical Security | X | X | X | X | X | X | X | X |
| Security Documentation | X | X | X | X | X | | | |
| Continuous Monitoring | X | X | X | X | X | X | X | X |
| Vulnerability Management | X | X | X | X | X | X | X | X |
| Threat Identification and Mitigation | X | X | X | X | X | X | | |
| Segmentation | X | X | X | X | X | | | |
| Secure Development Lifecycle | X | X | X | X | X | X | X | |
| Security Incident Management | X | X | X | X | X | X | X | X |
| Business Continuity and Disaster Recovery | X | X | X | X | | X | X | X |
| Security Auditing | X | X | X | X | | | X | |

## Further Resources

Phase 1 Baseline Requirements can be found here.

Phase 1 Explanatory Document can be found here.