# Cyber Security Guide

Revision Date: August 1, 2023

## Table of Content

# 1. INTRODUCTION

This Cyber Security Guide ("CSG") sets out additional requirements regarding cyber security that Supplier shall fulfil when providing Products or Services of any kind to Infineon on the basis of an agreement between Infineon and Supplier ("Agreement"). Because security risks are constantly changing, Infineon will update this CSG from time to time to ensure the protection of Infineon Assets and Confidential Information.

All capitalized terms used herein shall have the meaning as defined in the Appendix – Defined Terms.

# 2. PURPOSE

Infineon Assets shall be protected from risks. Also, Infineon is committed to comply with the requirements of all Applicable Laws and regulations. Accordingly, Infineon requires its Suppliers to exercise utmost care to ensure that Infineon Assets are not compromised in any way due to Supplier's Products or Services. This CSG shall only apply, if and to the extent, the provisions are relevant to Supplier's Products and Services. Such decision shall lie solely with Infineon.

# 3. CYBER SECURITY PROGRAM

Supplier warrants to have established and to maintain a state-of-the-art cyber security program.

The Supplier's cyber security program shall ensure that information and Information Systems are protected against cyber security threats and that Services and Products for Infineon are delivered in accordance with this cyber security program.

Supplier warrants that state-of-the-art technical and organisational cyber security measures are in place and shall be maintained throughout the service provisioning which are based on standards such as the ISO270XX family, NIST CSF, NIST 800-53, CIS or similar, including but not limited to the following control categories:

- **Governance, Roles & Responsibilities**
  A security management program based on best practices shall be established and governed by policies and rules with defined roles and responsibilities.
- **Training and Awareness**
  A minimum level of security education and training on key security issues shall be regularly provided to employees.
- **Asset and Risk Management**
  Assets associated with Data and Information Systems shall be identified and inventoried. Security risks shall be managed for assets based on a risk assessment.
- **Personnel Security**
  Processes shall be established to support security management prior to and during onboarding, as well as offboarding, of personnel.
- **Physical Security**
  Security perimeters shall be defined and used to protect areas that contain either sensitive or critical Data and Data processing Facilities.
- **Access Management (Authentication and Authorization)**
  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.

- **Network Security**
  Networks shall be managed, controlled and secured to protect Data processed or stored on Information Systems.
- **Malware Defences**
  A malware protection concept shall be in place and up-to-date.
- **Cryptography**
  Only defined and approved cryptographic algorithms shall be used, keys are generated securely and key protection is ensured throughout the lifecycle of the protected Data.
- **Security Logging and Monitoring**
  General logging shall be configured including system and application logs and regularly reviewed for potential security relevant events.
- **Information Systems Operations**
  Documented and traceable procedures shall be in place regarding patch management, change management, and backup of Information Systems.
- **Information System Implementation and Development**
  Policies and procedures shall be in place for secure development/implementation of Information Systems to ensure the integrity of Assets and appropriate level of robustness against threats.
- **Incident Management**
  Policies and procedures for the management of security incidents shall be established to mitigate risks and minimize damage should an incident occur.
- **Hardening**
  Documented security configuration and hardening standards shall be maintained for all authorized operating systems and software and its implementation is ensured.
- **Vulnerability Management**
  A documented process on how to manage vulnerabilities for Information Systems shall be implemented.
- **Contingency Planning**
  The organization shall determine its requirements for information security and Information System operation continuity in adverse situations, e.g. during a crisis or disaster.
- **Supplier Management**
  When using external IT service providers and IT services, the responsibilities regarding the implementation of information security measures shall be defined and verifiably documented.
- **Verification & Audit**
  Independent verification or audit of the implemented security controls shall happen regularly.

## 4. Technical Interfaces

Supplier shall implement state-of-the-art technology to warrant a secure way of communication to the Product or Service if not otherwise agreed by Infineon.

## 5. Cyber Security Assessment

Supplier shall conduct an individual cyber security assessment with Infineon to demonstrate compliance with this CSG. The cyber security assessment shall be performed prior to the

conclusion of the Agreement. In case an Agreement has been concluded without a prior cyber security assessment, it shall be performed within 3 months after the conclusion of the agreement upon Infineon's request.

The initial assessment of the Supplier by Infineon may include remote inspections/ interviews or document inspections.

Infineon has the right to perform a cyber security assessment remotely or at the Supplier's premises once a year or in case of a security incident after alignment with the Supplier.

Supplier warrants to participate in conducting the assessment and agrees to provide Infineon reasonable access to Facilities and information.

In case a cyber security certification or attestation exists, the Supplier agrees to provide proof of such certification to Infineon during the assessment or on request.

After previous alignment, Infineon shall have the right to conduct or have conducted by a trusted Third Party a vulnerability or penetration test, alternatively the Supplier shall provide evidence of such tests and follow-up measures to Infineon.

Supplier warrants that for identified cyber security issues a plan of actions and measures (POAM) shall be developed and agreed with Infineon. Supplier ensures that the implementation of agreed measures will take place in the quality and timeframe defined within the POAM at the Supplier's expenses.

Supplier warrants to communicate regularly with Infineon regarding cyber security topics, specifically in case of issues regarding the implementation of the POAM. Supplier shall review the status of the POAM with Infineon at least once a year.

If the cyber security assessment or any subsequent POAM is not performed in due time Infineon may, in its sole discretion, terminate each Transaction Document at any time in whole or in part upon at least 5 (five) days prior notice to Supplier.

## 6. INCIDENT REPORTING & RESPONSE

In case cyber security incidents occur at the Supplier, the Supplier shall report incidents with impact on Infineon to the Infineon Cyber Defense Center within 72 hours (https://www.trusted-introducer.org/directory/teams/infineon-cdc.html, phone: +43 51777 7100, e-mail: cert@infineon.com) and to the Infineon service manager or its designee. Supplier warrants to submit any incident related information as reasonably requested by Infineon and support Infineon within the incident response (e.g. evidence collection, measure implementation).

Supplier warrants to have state-of-the-art cyber incident detection and response processes in place at all times.

Supplier warrants to take all reasonable measures and precautions to prevent damage to or loss of Infineon's Assets and Confidential Information even though not specifically set forth within this agreement.

## 7. SUBCONTRACTORS

Except for subcontracting to Supplier`s Affiliates, Supplier is not entitled to subcontract Services or any part thereof to any Third Party without the prior written consent of Infineon. Denial of subcontracting shall not relieve Supplier of its obligations to fulfil its requirements under the Agreement.

Supplier shall ensure that all Subcontractors comply with all terms and conditions of the Agreement prior to such Subcontractor performing any Services. The Supplier is responsible for compliance and performance of its Subcontractors.

## 8. Working at Infineon Locations

Supplier may be granted access to Infineon Facilities, only with Infineon's prior written consent. Such access shall be used only for the purpose of performing agreed Services. Supplier shall comply with all then current Infineon security and access requirements as made available by Infineon to Supplier. Supplier acknowledges and understands that security provisions may differ for different Infineon Facilities and Supplier will take care to ensure that Supplier employees who have access to an Infineon Facility will be made aware of and comply with all applicable security provisions. For any remote access to Infineon infrastructure, the standard Infineon remote access solutions must be used.

Supplier shall adhere to all Infineon security regulations and use all available security capabilities when accessing Infineon Information Systems (e.g., User IDs, passwords, encryption, access management, reporting of incidents, etc.). Such applicable regulations and related trainings will be made available to Supplier when required. Supplier must ensure that only Supplier's staff that successfully passed the provided training material may work at Infineon locations.

Changing or disabling of security settings or configurations on Infineon Information Systems is forbidden.

Supplier's staff may use Supplier's own computing equipment when providing Services, however, such equipment shall not be connected to Infineon's network, and any Infineon Data shall be protected as provided for in this CSG.

All Infineon Data, which Supplier possesses shall be stored at a storage location as defined or otherwise agreed by Infineon. In particular, Supplier's staff is not entitled to store any Infineon Data on a portable storage or privately owned device unless otherwise agreed.

## 9. Use of Infineon Data

Supplier warrants to not use Infineon data for any advertising, artificial intelligence (AI), statistical, analytical or similar commercial purposes. Infineon retains all right, title and interest in and to Infineon Data if not otherwise agreed by Infineon.

If Supplier processes personal data on behalf of Infineon, such personal data shall solely be used and retained for the purposes related to the performance of the Transaction Document and in accordance with applicable data privacy laws. Separate Data Processing Agreements must be concluded in accordance with applicable data protection legislation.

## 10. Data Retention and Deletion

Supplier shall promptly provide a copy of all Infineon Data upon request by Infineon and/or its Affiliates at any time.

Upon Infineon's and/or an Affiliates written request, Supplier shall delete all Infineon Data in its possession, including any cached or backup copies hereof.

Upon termination of any Transaction Document, or any part thereof, the Supplier shall, either return or Destroy all copies (including the original) of the other Party's Confidential Information

that is in its possession. In the event of a partial termination of a Transaction Document, the foregoing is applicable to any Confidential Information relevant to the terminated portion of the Transaction Document. In the event Confidential Information is Destroyed, the Party Destroying the Confidential Information shall send written confirmation to the other Party that the destruction has been accomplished. Archival media containing any Confidential Information shall be retained as required by Applicable Laws and shall be used solely for such purposes of Applicable Laws and shall be returned or Destroyed upon expiration of the archival requirement.

## 11. SEGREGATION OF INFINEON DATA

Supplier warrants that Infineon Data shall at all times be technically isolated from the data of other customers of Supplier in such manner to (a) prevent access by unauthorized persons, (b) be shielded from potential unintended confiscation by legal authorities who have cause to confiscate the data of any other customer of Supplier.

Additionally, the Supplier agrees to support Infineon in remaining compliant to international regulations and specifically offer the ability to limit access based on the geographic location if required by Applicable Law.

## 12. ILLICIT CODE

Supplier guarantees that unless authorized in writing by Infineon or unless otherwise agreed in the relevant Transaction Document, any software, algorithm, or code associated with software provided to Infineon, regardless of if pre-existing or developed for Infineon:

a) must be properly licensed and cannot contain code of Third Parties without proper license,

b) contain no code and/ or services, catering for unauthorized functionality, e.g., malware, backdoor, unauthorized remote access to or from Infineon’s network,

c) do not replicate, transmit, or activate itself without control of a person operating computing equipment on which it resides,

d) do not alter, damage, or erase any data or computer programs without control of a person operating the computing equipment on which it resides, and

e) contain no key, node lock, time-out, or other function, whether implemented by electronic, mechanical, or other means, that restricts or may restrict use or access to any programs or data developed relative to a Transaction Document, based on residency on a specific hardware configuration, frequency of duration of use, or any other limiting criteria.

## 13. GENERAL TERMS AND MISCELLANEOUS

### 13.1. SECURITY REQUIREMENTS

Infineon and Supplier may agree to additional security requirements in the respective Transaction Document from time to time.

### 13.2. COST OF COMPLIANCE

Unless otherwise agreed in a Transaction Document, Supplier shall be responsible for its own costs associated with compliance with this CSG.

### 13.3. REMEDIES

The performance by Supplier of the responsibilities set forth in this CSG shall not serve to exclude any remedies that Infineon may have pursuant to the terms and conditions of the relevant Transaction Document between Infineon and Supplier.

## APPENDIX - DEFINED TERMS

“Affiliate" shall mean any corporation, company, or other entity, which: (i) is controlled by a Party hereto; or (ii) controls a Party hereto; or (iii) is under common Control with a Party hereto. For this purpose, “Control” means that more than fifty percent (50%) of the controlled entity’s shares or ownership interest representing the right to make decisions for such entity are owned or controlled, directly or indirectly, by the controlling entity.

“Applicable Laws” shall mean all laws, regulations, provisions, legislative enactments, trade and embargo restrictions, and regulatory requirements which need to be observed and complied with in connection with the rendering of the Services.

“Assets” shall mean all physical assets, as well as intellectual property, Data, and Confidential Information, which must be protected from risk of loss or compromise.

“Confidential Information” shall mean any technical and/or commercial information of a Party received by the other Party in any form under or in connection with any Transaction Document, including information relating to the disclosing Party’s respective businesses, facilities, products, services, techniques, and processes, regardless of whether in a form such as (but not limited to) oral disclosure, demonstration, device, apparatus, model, sample of any kind, computer software (including, but not limited to, source code and documentation), magnetic medium, document, specification, circuit diagram, or drawing (including, but not limited to, information of a general nature) and visual observation of the above. Confidential Information as defined above, however, does not include (i) any information in the public domain, unless such information was made public by the other Party’s failure to comply with its obligations under a Transaction Document, (ii) information already known to or in the possession of a Party by lawful means, (iii) information independently developed by either Party or (iv) information which is lawfully obtained by Infineon or Supplier without restriction on disclosure.

“Data” shall mean any digital representation of information, including but not limited to Confidential Information.

“Destroyed” shall mean the destruction of documents and data in a non-retrievable way (e.g. shredding of paper documents or wiping of data from electronic storage media, so that it cannot be reconstructed or otherwise retrieved).

“Facilities” shall mean sites, network or computing facilities.

“Infineon” shall mean Infineon Technologies AG including all its Affiliates.

“Information System” shall mean any discrete set of hard- and software organized for the creation, collection, processing, storage, transfer, or deletion of digital information, including but not limited to applications, servers, clients, and communication equipment.

“Party” shall mean Infineon or Supplier as determined by the context of usage.

“Products” shall mean equipment or software provided by Supplier or its Subcontractors to Infineon.

“Services” shall mean the related task(s) to be performed by Supplier for Infineon pursuant to a Transaction Document. Service may include such things as process design service, programming service, customizing service, analytical service, preventive maintenance service, conversion service, consulting service, software as a service, training, knowledge transfer, support service, system operation service, system roll out service, hardware or

software system maintenance service, patches delivery, system-upgrade service or quality assurance. The preceding list of Services is exemplary and not exhaustive.

“Subcontractor” shall mean any Third Party that is engaged by Supplier to perform all or part of the Services pursuant to a Transaction Document.

“Supplier” shall mean Infineon’s contracting party as identified on the cover page of a Transaction Document.

“Third Party” shall mean any company (e.g., person, corporation, or other entity) other than Infineon, Supplier or Affiliates of Supplier.

“Transaction Document” shall mean a document that defines the specific scope of Services to be performed by Supplier including all requirements and specific terms and conditions agreed by written consent of both Parties, for a specific transaction between the Parties, including the underlying agreement for terms and conditions, if any. Such Transaction Document may be a statement of work or a quotation by Supplier, if such quotation was accepted by Infineon by means of a purchase order.