Supplier IT Security Guide

Revision Date: October 21, 2020

TABLE OF CONTENT

1. INTRODUCTION

This Supplier IT Security Guide (“SISG”) sets forth the basis for requirements that Supplier must fulfil when providing Products or Services of any kind to Infineon.

Because security risks are constantly changing, Infineon will update this SISG from time to time in order to adjust the protection of Infineon Assets and Confidential Information.

2. PURPOSE

Infineon Assets must be protected from risks. Also, Infineon is committed to comply with the requirements of all Applicable Laws and regulations, including those regarding personal data protection, such as but not limited to the European General Data Protection Regulation (“GDPR”). 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 SISG 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. GENERAL REQUIREMENTS

Supplier’s Products or Services must comply with all applicable requirements and guidelines set forth in this SISG. Additionally, Supplier shall take all reasonable measures and precautions to prevent damage to or loss of Infineon’s Assets even though not specifically set forth herein.

For sake of clarity, applicable requirements and measures described herein relate to all of Supplier`s information and communication technology including telecommunications systems.

4. ACCESS REQUIREMENTS

Supplier may be granted access to Infineon Facilities, only with Infineon’s prior written consent. Such access must be used only for the purpose of performing agreed Services. The Supplier shall comply with all then current Infineon security and access requirements. Supplier acknowledges and understands that security provisions may differ for different Infineon Facilities (e.g., due to local technical or regional issues) and Supplier will take care to ensure that any of the Supplier Staff who has 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.

5. SECURITY RULES FOR SUPPLIER WORKPLACES AT AN INFINEON LOCATION

The use of any Infineon Information Systems by Supplier is strictly limited to purposes directly related to Supplier's provision of the Services. Any other use of Infineon Information Systems is strictly prohibited.

Supplier must adhere to all Infineon security rules 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 rules and related trainings will be made available to Supplier when required.

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

Security capabilities and related information must be treated with appropriate care and shall be deemed to be Infineon Confidential Information (e.g., it is prohibited to pass authentication information such as user ID and password to others).

In case of security incidents, such as a suspected infection by malware, or if there are problems with security related software or processes, Supplier shall immediately report the matter to Infineon as provided for in Section 7.5 below.

Incoming e-mail to an Infineon e-mail account shall not be automatically forwarded to external e-mail accounts.

Supplier's Staff may use Supplier's own computing equipment when providing Services, however such equipment may not be connected to Infineon's Network, and any Infineon Data must be protected as provided for in this SISG.

All Infineon Data, which Supplier possesses has to be stored at a storage location as defined or otherwise agreed by Infineon. In particular, Supplier's Staff may not store any Infineon Data on a portable storage device unless otherwise agreed pursuant to Section 13.1.

6. PERSONNEL SECURITY

Supplier must ensure that its Staff is carefully chosen, including background verification checks, as well as properly briefed and constantly trained on information security and data protection issues.

If any member of Supplier's Staff is withdrawn from providing Services for Infineon or if the employment of (or contract with) such Supplier's Staff working for Infineon is terminated, Supplier must inform Infineon without undue delay, if and to the extent, such member of Supplier's Staff has access to Infineon's Facilities, i.e., Infineon account. In case of any such termination, any access to Supplier's systems by that member of Supplier's Staff must be disabled immediately. Infineon Assets, such as computer hardware, must be returned.

7. DATA PROCESSING AT SUPPLIER'S PREMISES

If Supplier's Staff processes Infineon's Data at any Supplier site, the following rules must be adhered to:

7.1. PHYSICAL SECURITY

Supplier shall control access to its data centers and other areas where Infineon Assets are processed or stored at all times. Access may only be granted to such Supplier Staff or sub-/ contractors with a

business need. Each access to a Supplier data center must be logged and logs must be stored at least 30 days. The list containing the Supplier Staff with permanent access to Supplier data centers must be reviewed and updated regularly to ensure only Staff with a clear business need has access.

Supplier's data centers must have fully functional surveillance, intrusion detection, and alarming at all times, detecting and preventing access by unauthorized personnel.

Measures to prevent physical damage, including but not limited to technical defect, elemental damage, outage of infrastructure, human error, signal interception and interference, and unauthorized physical removal of assets, shall be in place.

7.2. Information System Security

7.2.1. Logging

All of Supplier's systems and applications must log and record any relevant information required to monitor and detect any security relevant event, such log files being protected against alteration. Log files shall be reviewed for potential security incidents pursuant to Supplier's own security management system.

If a security incident occurs and it is anticipated that Infineon Data may be compromised, Supplier must immediately notify Infineon pursuant to Section 7.5. In such case any relevant log files must be made available to Infineon.

7.2.2. Access Management

Access to Supplier's systems must be limited to authorized users via a secure authentication process. Each user must have a unique user ID, and the sharing of accounts must not be allowed. System administrators should have a separate admin account to perform any administration tasks.

Access to Supplier's systems must be protected. Such protection must include but not be limited to the secure and state of the art password policy, an automatic session logoff after a certain amount of idle time, lock out in case of multiple failed login attempts, safe and reliable password reset mechanisms, a risk based change process for passwords, and risk based use of two-factor authentication. Passwords shall always be stored and transmitted in a secure way, e.g. by encryption, hashing or discrete channel. Access rights for users must be restricted to those rights which are required to perform their work.

All Supplier's servers containing or processing Infineon Data must be located in a data center, to which access is restricted as set forth in section 7.1. Security patches must be implemented regularly, but in intervals not longer than recommended by the manufacturer or as otherwise required by Infineon.

There shall be no generic, guest, maintenance or default accounts. Any user accounts, including test accounts, which are no longer required, and ports or services which are not required, must be immediately disabled.

The production environment and networks must be separated from the development and test systems.

7.2.3. Endpoint Security

Supplier's Endpoint Equipment must have malware protection, including automatic signature updates. The operating systems as well as software must be updated and patched regularly for security vulnerabilities; the patching intervals must at least meet the recommendations of the software manufacturer. An emergency patch process must be in place.

All Supplier mobile Endpoint Equipment must be secured technically and organizationally, in addition to the general access controls (see Sections 7.1 and 7.2.2), e.g. by using Kensington Locks or lockable cabinets.

7.2.4. Encryption

Supplier shall ensure that confidential Infineon data in possession of Supplier, including backups, are being encrypted both while at rest and in motion, when outside a secure data center.

Any confidential Infineon Data at rest on mobile clients must be encrypted, e.g. via file, container, or volume encryption.

7.3. Network Security

7.3.1. Network Perimeter

All network sections which connect to the Internet must be protected by state of the art network perimeter controls (including e.g. firewalls), which shall include but not be limited to the control of connections and ports and the detection of incidents.

7.3.2. Remote Access

If remote access to Supplier's systems is used, access to the network must be protected by two factor authentication. Any outbound modems (e.g., for the automatic sending of SMS) must have inbound calls disabled.

7.4. Data Life Cycle

If Supplier processes personal data on behalf of Infineon, such personal data will 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 Protection Agreements must be concluded in accordance with applicable data protection legislation.

7.4.1. Data Retention and Disposal

Unless otherwise provided for in a Transaction Document or required by Applicable Laws,

a) Supplier shall implement a backup policy that includes offline availability, to protect e.g. against ransomware,
b) Supplier ensures system and data recovery for at least 30 days backwards, and
c) all Infineon data in Supplier's possession must be backed up pursuant to the backup policy,

d) all Infineon data in Supplier's possession must be unrecoverably destroyed at the latest 30 days after termination of the Transaction Document.

7.4.2. Return or Destruction of Confidential Information upon Termination

Upon termination of any Transaction Document, or any part thereof, each Party shall, as directed by the other Party, either return or Destroy all copies (including the original) of the other Party's Confidential Information that is in their possession. In the event of a partial termination of a Transaction Document, the provisions of this Section 7.4.2 are 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 pursuant to this Section 7.4.2 upon expiration of the archival requirement.

7.5. Incident Detection and Management

Supplier shall have cyber incident detection and response processes at all times and according to best practices in place.

Supplier shall immediately report any cyber incidents with potential impact on Infineon Data to the Infineon Cyber Defense Center (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 his designee. Supplier shall submit any incident related information as reasonably requested by Infineon.

8. Cloud Services and Subcontractors

8.1. Subcontractors

If Infineon has agreed to Supplier's use of Third Party IT services, Supplier shall ensure that such Third Parties

a) shall be contractually committed to comply with the requirements of this SISG by signing an agreement which is at least as strict as the regulations set forth in this SISG, and
b) shall in fact follow necessary procedures and processes in order to ensure such compliance in the performance of all services and production of all products.

8.2. Cloud Services

Supplier may use Third Party Hosting Services, including cloud based services (e.g. Amazon Web Services, Microsoft Azure, Google Cloud Services) and Subcontractors in the provision of Services to Infineon only if approved by Infineon. Once approved, changes to Third Party IT services, e.g. change of provider or hosting location, are only allowed upon prior consent by Infineon. Infineon's approval of any such new or changed Third Party IT services may be subject to an initial and subsequent periodic security reviews by Infineon and such approval may be denied or revoked at any time.

9. Business Continuity and Disaster Recovery

Unless otherwise defined, Supplier is responsible to take reasonable steps to ensure that Products and Services to be provided by Supplier shall not be materially interrupted by any type of disaster (e.g., fire, flood, earthquake, technical malfunction, cyber attacks etc.), by having a disaster recovery and business continuity plan in place. “Reasonable steps” as used herein shall include but not be limited to such things as having regular backup, alternate remote compute facilities for any Supplier operated data center (e.g., a backup hot site); alternative data communication services; maintenance, provision for data recovery, updating and testing (at least annually) of all relevant Supplier disaster recovery plans (including operational interface and integration with all relevant Infineon systems and disaster recovery plans), and the results thereof timely communicated to Infineon.

10. Software Development

10.1. Secure Software Development

Supplier shall follow secure software development practices. This may include but not be limited to

a) establish secure coding practices appropriate to the programming language and development environment being used;
b) apply static application security testing to verify that secure coding practices are being adhered to;
c) create and successfully execute a security testing concept,;
d) perform a penetration test before productive data is hosted on the system or go-live for all systems exposed to the Internet or hosting confidential data;
e) inform Infineon in case a vulnerability has been identified and provides a proper remediation within a reasonable time frame.

If Supplier develops software for Infineon, Supplier must adhere to Infineon’s applicable software development guidelines such as the Infineon Application Security Guidelines or other requirements, which will be made available to Supplier upon request.

10.2. Illicit Code

The 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 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.

10.3. SOFTWARE INTEGRATION

As far as stated in a Transaction Document, Supplier must ensure that any software developed by Supplier for Infineon, regardless if it is pre-existing or developed for Infineon, is fully integrated into any relevant Infineon security requirements, backup, and disaster recovery plan and procedure.

11. REQUIREMENTS FOR EQUIPMENT PROVIDED TO INFINEON BY SUPPLIER

Any software (e.g. operating system, Java, pdf reader, open source software etc.) used as a part of Equipment

a) must be identified by the Supplier's name and revision number;
b) must be current at the date of delivery and it must be warranted that relevant operating system updates and software vulnerability fixes can be implemented continuously, but in intervals no longer than recommended by the manufacturer of the software or equipment, unless otherwise agreed by Infineon, e.g. in case a downtime would be required;
c) must be compatible with Infineon's corporate anti-malware software without impact on the operational use;
d) must support current network security best practices, such as but not limited to network segregation and network access control technologies.

For each software update Supplier will be granted a one-time access to Infineon's network, if necessary.

All Equipment which is planned to be connected to the Infineon network must be compatible with Infineon network settings (e.g. DHCP, DNS, NAC). Equipment must not be used as a network bridge between the Infineon network and other networks.

12. SECURITY AUDIT

Infineon or its designated representative are entitled to conduct Security Audits. All audit activities and results are subject to the confidentiality requirement as set out in the respective Transaction Document.

12.1. AUDIT FORMALITIES

Infineon shall provide reasonable notice to Supplier prior to any Security Audit. Infineon shall try to ensure that such Security Audits are requested no more than twice each business year. Notwithstanding the foregoing, Infineon may conduct an immediate Security Audit in case of a security related incident.

Supplier will provide to auditors access to all information necessary to perform the Security Audit. Upon request of Infineon, Supplier shall participate in conducting Security Audits. Supplier will also assist Infineon staff or auditors in testing relevant services, including installing and running audit software.

12.2. Access to Supplier's Sites and Facilities

Supplier shall provide to Infineon and such auditors and inspectors as Infineon may designate in writing, access to Supplier's and Supplier's Subcontractors' sites or facilities as may be necessary for Infineon or its agents or representatives to perform any Security Audit. Access will be provided at reasonable hours. The access to sites and facilities shall include but shall not be limited to use of Supplier's offices and office infrastructure as Infineon or such auditors and inspectors may reasonably require to perform the Security Audits described in this section. Records and supporting documentation, process descriptions, software and data relating to Supplier's performance hereunder shall be provided by Supplier.

12.3. Vulnerability Scans and Penetration Tests

Supplier shall conduct or have conducted by a trusted Third Party vulnerability and penetration tests of any Supplier hosted software or service which is exposed to the Internet (including but not limited to any Third Party providing the hosted software or service on behalf of Supplier). Supplier shall inform Infineon on the results and remediation activities.

After previous alignment, Infineon shall have the right to conduct or have conducted by a trusted Third Party such vulnerability or penetration tests. Infineon shall share the results of any security audit to Supplier.

12.4. Corrective Actions

Supplier shall take actions to correct the problems found during or to comply with the recommendations of such Security Audit as soon as possible according to a mutually agreed schedule. All such corrective actions are to be completed at Supplier's expense.

13. General Terms and Miscellaneous

13.1. Special Security Requirements

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

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 SISG.

13.3. Remedies

The performance by Supplier of the responsibilities set forth in this SISG 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 A. DEFINITION OF TERMS

"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.

"**Applicable Laws**" shall mean all laws, rules, 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.

"**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.

"**Destroyed**" in the sense of Section 7.4, 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).

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

"**Endpoint**" shall mean any Information System that is connected to and communicates with a network, such as servers, desktop and notebook clients, and mobile devices.

"**Facilities**" shall mean sites, networks or computing facilities.

"**Equipment**" shall mean any piece of technical equipment, including but not limited to manufacturing equipment and Information Systems provided by Supplier to Infineon.

"**Hosting**" shall mean any provision of Services via network resources, including but not limited to web hosting and cloud service provision.

"**Infineon**" shall mean Infineon Technologies AG including all its Subsidiaries.

"**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 servers, clients, and communication equipment.

"**Intellectual Property**" shall mean without limitation any patents and other rights to inventions, copyrights, trademarks, trade names and service marks and any other intangible property rights and all related rights of use or commercialization owned by Infineon.

"**Party**" shall mean Infineon or Supplier as determined by the context of usage.

"**Parties**" shall mean Infineon and Supplier.

"**Products**" shall mean Equipment or software provided by Supplier or its Subcontractors to Infineon.

"**Security Audit**" shall mean an audit of Supplier's compliance with Infineon's security provisions of this SISG and those of any relevant Transaction Document, as well as security risk assessments.

"**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, 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 retained by Supplier to perform all or part of the Services pursuant to a Transaction Document.

"**Subsidiary**" shall mean any company which is directly or indirectly controlled by a Party, whether through ownership of voting securities, by contract or otherwise. By way of clarification and not limitation, any company in which a Party owns greater than fifty percent (50%) interest shall be deemed to be a Subsidiary.

"**Supplier**" shall mean Infineon's contracting party as identified on the cover page of a Transaction Document.

"**Supplier's Staff**" shall mean employees or approved Subcontractors of Supplier who are in any way involved in the provision of services or delivery or products to Infineon.

"**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.

"**Third Party**" shall mean any company (e.g., person, corporation, or other entity) other than Infineon, Supplier or Subsidiaries of Supplier.