Supplier IT Security Guide

Revision Date: November 21, 2017

TABLE OF CONTENT

1. INTRODUCTION

This Supplier IT Security Guide ("SISG") sets forth the basis for requirements that Supplier must fulfil when providing software, Equipment 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 protect Infineon Assets and Confidential Information.

2. PURPOSE

Infineon Asset must be protected from risk of theft or other loss. Also, Infineon is committed to comply with the requirements of all Applicable Laws, including those regarding personal data protection, such as but not limited to the German Data Protection laws. Accordingly, Infineon requires its Suppliers to exercise utmost care to ensure that Infineon Asset is 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 and 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.

Supplier shall ensure that Infineon Data in possession of Supplier are being encrypted at all times, both while in rest and in motion.

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 maintenance services, the standard Infineon remote maintenance solution must be used.

5. SECURITY RULES FOR SUPPLIER WORKPLACES AT AN INFINEON LOCATION

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

Supplier must adhere to all Infineon security rules and use all available security capabilities when accessing Infineon IT Systems (e.g., User IDs, passwords, encryption, authentication mechanisms,

etc.). 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).

Security settings, security related features or precautionary measures against computer viruses for instance, installed on Infineon IT Systems may not be disabled, modified or otherwise circumvented in any way.

In the event of a suspected infection by computer viruses or other 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 email account may not be automatically forwarded to external e-mail boxes.

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 below.

6. PERSONNEL SECURITY

Supplier must ensure that its personnel are carefully chosen, including background verification checks, as well as properly briefed and constantly trained on security 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.

7. DATA PROCESSING AT SUPPLIER'S PREMISES

If and to the extent 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 Asset is stored or kept 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 as required by Applicable Law but not less than 90 days. The list containing the Supplier Staff with permanent access to Supplier data centers must be reviewed and updated at least quarterly to check for the business need of the Supplier Staff or contractor.

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

7.2. Information and Communication Technology System Security

7.2.1. Logging

All of Supplier's systems and applications must log and monitor any security Incident, such log being protected against alteration.

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 below. In such case any log files must be made available to Infineon.

7.2.2. Access Control

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 password protected. Such protection shall 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 process; change of passwords at least every 100 calendar days. Passwords shall always be stored and transmitted in a secure way, e.g. by encryption, hashing or discrete channel.

7.2.3. Server Security

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 7.1 above. 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 or test systems.

7.2.4. Client Security

Supplier's client equipment must have malware and virus protection, including automatic signature updates. The operating systems as well as software must be patched regularly for security vulnerability; however, the patching intervals must at least meet the recommendations of the software manufacturer.

All Supplier client equipment must be secured technically and organizationally, in addition to the general access control (see Section 7.2.2), e.g., by using Kensington Locks, lockable cabinets.

7.3. Network Security

7.3.1. Network Perimeter

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

7.3.2. Remote Access

If remote access to Supplier's systems is used, the access to the network must be protected by strong (at least 2-factor) authentication. Any outbound modems (e.g., for the automatic sending of SMS) must have inbound calls disabled.

7.4. Data Security

This Section 7.4 covers the general protection of Infineon's Data. If and to the extent Supplier processes or has access to or possession of any Infineon personal data, the separate "Infineon Minimum Data Protection Rules" shall apply.

7.4.1. Data Retention and Disposal

Supplier shall implement a backup policy that ensures system and data recovery for at least 30 days backwards.

Unless otherwise provided for in a Transaction Document or otherwise required by Infineon, any Infineon Data in Supplier's possession must be Destroyed if it is not required for the provision of Services anymore or within 30 days if the respective Transaction Document is terminated for any reason.

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 Management

Supplier shall operate state-of-the-art incident detection systems at all times, which allow detection of attacks at least at the network perimeters. Supplier shall operate a process to detect and mitigate Information Security Incidents.

Supplier shall immediately report any Incidents with regard to security to the Infineon Service Manager or his designee, and if not available, then to the Infineon Security Department (phone: +49 89 234 22222. email: Security@infineon.com). Supplier shall submit any Incident related information as reasonably requested by Infineon.

8. Cloud Services and Subcontractors

8.1. Cloud Services

Supplier may use Third Party cloud based IT services (e.g. Amazon Web Services) in the provision of Services to Infineon only if approved in writing by Infineon. By way of clarification, existing Services may not be transferred to a Third Party cloud based IT service without Infineon's prior written approval.

Once approved, changes to the general setup of the Third Party cloud based services, e.g., change of provider, are only allowed upon prior written consent by Infineon.

Infineon's approval of any new or changed Third Party cloud based IT service is subject to an initial and subsequent periodic security reviews by Infineon and such approval may be denied or revoked at any time.

8.2. Subcontractors

If Infineon has agreed to Supplier's use of Subcontractors, Supplier shall ensure that such Subcontractors (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.

9. Business Continuity and Disaster Recovery

Unless otherwise provided for in a Transaction Document, Supplier will be 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, severe weather of any type, severe technical malfunctions, 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 communications 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, etc.

Unless otherwise provided for in a Transaction Document, all Infineon Data in Supplier's possession must be backed up pursuant to the Supplier's disaster recovery plan.

All backup media must be in secured storage and shall be catalogued (e.g. labelled, listed and kept secured), so that missing devices can be identified. However, such media may not be labelled to disclose the data contained or the owner of the data.

10. SECURITY FOR SOFTWARE

10.1. SOFTWARE DEVELOPMENT

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 shall, regardless if pre-existing or developed for Infineon:

a) contain no code and/or services, catering for unauthorized functionality, e.g., malware, backdoor, unauthorized remote access to or from Infineon's Network
b) not replicate, transmit, or activate itself without control of a person operating computing equipment on which it resides,
c) not alter, damage, or erase any data or computer programs without control of a person operating the computing equipment on which it resides; and
d) 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. INTEGRATION

As far as stated in a Transaction Document, Supplier must ensure that all 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 installed and used on Equipment (e.g., operating system, Java, PDF Reader, etc.) provided by Supplier to Infineon must be patched regularly with the latest security patches, 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). Supplier must ensure that such Equipment will be fully operational even after the implementation of such new patch or service pack., Supplier shall further ensure that Infineon`s corporate anti-virus software can be installed and run on the Equipment without impact on the operational use.

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

12. SECURITY AUDIT

Infineon or its designated representative is entitled to conduct Security Audits.

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, such Audits may occur more frequently in the event that a serious security situation requires such a Security Audit). Supplier will provide to such auditors access to all information necessary to perform the Security Audit. Supplier will also assist Infineon staff or auditors in testing Infineon data files and programs, including installing and running audit software.

Notwithstanding the foregoing, Infineon may conduct an immediate Security Audit in case of a security related Incident.

Upon request of Infineon, Supplier shall participate in conducting Security Audits.

12.2. ACCESS TO SUPPLIER'S SITES AND FACILITIES FOR AUDITS

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 office furnishings, telephone and facsimile services, utilities and office-related equipment and duplicating services 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. TOOLS

For Security Audits , Infineon shall have the right to perform or have performed periodic vulnerability tests of any Supplier hosted software or service (including but not limited to any Third Party providing the hosted software or service on behalf of Supplier), subject to the confidentiality requirement as set out in the respective Transaction Document.

For Security Audits, Supplier shall operate and maintain such audit software as Infineon or its agents or representatives may provide to Supplier during the term of and as agreed in any Transaction Document.

12.4. CORRECTIVE ACTION

Infineon shall share the results of any Security Audit to Supplier and Supplier shall promptly take actions to correct the problems found during and/or comply with the recommendations of such Security Audit ; all such corrective actions to be completed as soon as possible according to a mutually agreed schedule 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

"**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 shall include any copies or abstracts made thereof as well as any modules, samples, prototypes or parts thereof.

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).

"**Equipment**" shall mean any piece of technical equipment supplied by Supplier to Infineon.

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

"**Infineon Assets**" shall mean all physical assets, as well as Infineon's Intellectual Property, Infineon Data and Confidential Information, which must be protected from risk of theft or other loss.

"**Infineon Data**" shall mean any data provided by Infineon to Supplier, including but not limited to Confidential Information.

"**Infineon Facilities**" shall mean Infineon's sites, Infineon Networks or computing facilities.

"**Infineon IT Systems**" shall mean any Infineon IT equipment or software, e.g., client workstations such as PC or laptop, servers, communication equipment etc.

"**Infineon Network**" shall mean Infineon's internal computer network.

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

"**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.