SMT TECHNOLOGIES SDN BHD
(A Member of EG Industries Bhd) (199301024828)
Plot 101, 102 & 102A, Bakar Arang Industrial Estate,
08000 Sungai Petani, Kedah, Malaysia.
o : +604 422 9881 f : +604 422 9885 w : www.esmtt.com

Supplier Declaration of Supply Chain Information Security and Cyber-security Compliance

REG.NO:1849-001-PUR/C

SMT TECHNOLOGIES SDN BHD
Plot 102, Bakar Arang Industrial Estate,
08000 Sungai Petani
Kedah Darul Aman, Malaysia.
Email : admin@esmtt.com Web Site : www.esmtt.com

SMT Industries CO., LTD. (SMTI)
196, Moo.10, 304 Industrial Park
Thatoom Sub-district, Srimahaphot Dist
Prachinburi Province, 25140
Thailand.
Tel : +66 (0) 37274 423

TMSMT SDN BHD
Plot 101, Bakar Arang Industrial Estate,
08000 Sungai Petani
Kedah Darul Aman, Malaysia.
Email : admin@esmtt.com Web Site : www.esmtt.com

Overview

EG Industries Berhad and its subsidiaries SMTT/SMTI/TMSMT are committed to supply chain information security and cyber -security compliance to ISO 27001.

1	Supplier must develop and disseminate a security program that addresses customer's supply chain security focus areas and cyber-security requirements.
2	Supplier must review and update their information security program based on internal organizational changes, changes in business relationships (including that with customer) and changes in customer's supply chain security focus areas and cyber-security requirements.
3	Supplier must identify roles and responsibilities within the Supplier's organization to meet customer's supply chain & cyber-security requirements and identify personnel to oversee the implementation of processes and controls to meet customer's the requirements. The identified personnel must be responsible for coordinating activities across the Supplier's organization (as required) to meet customer's supply chain & cyber-security requirements.
4	Supplier must monitor their relevant manufacturing systems (e.g. shop floor systems, warehouse management systems) for variations in standard production time or procedures to minimize potential tampering or material substitution.
5	Supplier must develop and implement measures to minimize opportunities for counterfeit during the manufacturing and repair processes. Supplier must develop and implement processes to detect and handle counterfeit items. Supplier must check for counterfeit items and report such counterfeit items to internal stakeholders and customer site security lead.
6	Supplier must identify and maintain an inventory of: a. all Information Assets (Examples – Servers, IT systems, data storage devices, testing equipment, network devices, encryption keys/ token, software assets et cetera, which should include customer and Supplier Assets.); and b. the location of and device(s) on which customer data resides.
7	All devices that store or process customer IP or Confidential Information must be managed by the Supplier or their authorized service providers
8	Customer IP and/or Confidential Information must not be stored in removable Media unless authorized in writing by customer.

9	Supplier must have the ability to detect if Confidential Information or customer IP is accessed in an unauthorized manner (e.g., ability to identify files accessed improperly as a result of an attack on networks or servers).
10	Supplier must establish a means (e.g., an email address or a 24X7 telephone number or a service desk) for Supplier personnel to internally report suspected Security Incidents.
11	Supplier must develop and implement an incident response plan to detect and handle Security Incidents. The plan must: a. clearly identify the incident response roles and responsibilities; b. define incident types that may impact customer's supply chain security focus areas; c. define incident response procedures for defined incident types; d. define a clear escalation path and procedures to esalate Security Incidents through Supplier's management chain and to customer; and e. be reviewed periodically and updated based on applicable evolving risk and threats.
12	Where Security Incidents involve the loss, disclosure, or duplication of customer IP, Supplier shall make every reasonable effort to retrieve all lost, disclosed or duplicated customer IP. Where Security Incidents involve the loss of tangible goods, Supplier must make every reasonable effort to retrieve all lost tangible goods.
13	Supplier must implement controls to ensure that customer's IP is protected and threats of counterfeit and malicious modifications are mitigated during the periods of disruption.
14	Customer IP and Confidential Information must not be located in or visible from any publicly accessible areas.
15	Supplier must inspect the state of Information Systems or Assets returned after maintenance to detect unauthorized tampering and unauthorized modifications.
16	Supplier must at no time, permit a Vendor to view any customer design, prototype activities, pre-production activities, product manufacturing processes or products except as necessary to perform such vendors authorized services.

17	Supplier must deploy periodic security awareness campaigns to all employees, contractors and third parties involved in services to customer. The following areas must be covered based on the job role or function of the employees, contractors and third parties, as applicable: a. security and information protection practices against social engineering, phishing, malware etc; b. misuse of customer IP; c. Information Systems access; d. Security Incident detection and reporting; e. alerts regarding controlling informal or inadvertent sharing of customer confidential information; f. response to burglary, robbery and in-transit theft; g. visitor access and challenging un-identified persons or vehicles; h. addressing suspicious activities and document fraud; i. management and disposal of scrap; j. detection of counterfeit items and malicious modification; and/or k. shipping processes and procedures.
18	Customer IP and Confidential Information in electronic or tangible format (e.g., work instructions and design documents, specifications, firmware software, pricing information) must be properly secured and controlled in a way that: a. limits its use to its intended purpose; b. limits its access to authorized Supplier personnel; and c. ensures segregation from that of Supplier's other customers (e.g. separate information system customer directories).
19	Supplier must have an information protection policy which includes data classification. All customer IP must be designated and protected at the highest data classification level. Additionally, Supplier must implement for all customer IP a. User Activity Logging: User activity with data (create, read, update, delete) must be logged and stored for at least a year. b. User / Data Monitoring: User Activity or Data Movement must be monitored for violations or anomalies.
20	Supplier must not retain customer IP and other Confidential Information beyond the time that they are required for valid business purposes. If Supplier has to retain customer IP and/or Confidential Information for an extended duration due to legal constraints, they must inform customer immediately.
21	When destruction of customer IP is requested by customer, Supplier must document that such destruction has been implemented in a permanent and irrecoverable manner.

22	Supplier must limit access to customer IP and other Confidential Information to personnel whose job functions require such access. Upon customer's request, Supplier must provide a list of such individuals with such access. The list must identify: a. each individual with access to customer data stored on Supplier's IT systems (e.g. DCC, file server) b. each individual who has access to customer IT systems c. each Supplier IT account created for any customer employee
23	Supplier must use practices that protect their enterprise network on which customer IP and Confidential Information is processed. Practices to protect enterprise networks should include: a. network segmentation/containment deployed as appropriate; b. firewalls configured to deny connections by default; c. intrusion detection/monitoring and prevention systems across the network.
24	Supplier must monitor Information Systems for: a. attacks and indicators of potential attacks; b. unusual transactions that could indicate unauthorized access to customer IP or Confidential Information; c. unexpected changes to system configurations and privileges; and d. unauthorized local, network and remote connections.
25	Customer IP and Confidential Information may only be shared with third parties for whom: a. such IP or Confidential Information is necessary to perform services or provide products to Supplier relating to customer; b. customer has provided authorization prior to such information being shared; and c. Supplier has a valid, active NDA obligating the third party to retain as confidential the intellectual property and confidential information of Supplier's customers
26	After sharing customer IP or Confidential Information , Supplier must immediately remove customer IP and Confidential Information from any device with Internet access used to share such information (e.g., SFTP servers). All other customer data located on any device with internet access should be purged automatically after seven days.
27	Supplier must use anti-virus software to supply chainan for malware, viruses, worms or other maliciously intended software at the following points in real-time: a. network entry/exit points; and b. download of files from external sources (including from emails, external storage devices etc.) Information Systems must have anti-virus software installed. The anti-virus software must contain the latest updates. Anti-virus software must be configured to: a. block the execution of or access to any malware, viruses, worms or other maliciously intended software identified; b. delete any malware, viruses, worms or other maliciously intended software identified; c. quarantine malware, viruses, worms or other maliciously intended software in the event that it cannot be deleted; d. send an alert to appropriate system/network administrators

28	Supplier must ensure that their suppliers and Vendors that have access to customer IP or Proprietary Items are aware and comply with the security requirements provided by customer.
29	When procuring products or services from their supply chain Vendors, other than as mandated by customer, Supplier: a. must establish product security specifications; and/or b. assess the third parties' adherence with the applicable security requirements specified in this document.
30	When there is a supply chain / cyber-security incident involving SMTT's products, supplier must ensure to report containment action within 12 hours , and full cause & countermeasure report within 24 hours.

Reply Details

This Declaration is made by:

.. . . **(the "Supplier"),** for the benefit of EG Industries Berhad and its subsidiaries SMTT/SMTI/TMSMT

The Supplier declares that it has read and understood the above requirements.

By signing this letter, the undersigned Supplier agrees to adhere and comply to the said requirements shall form a substantial condition of the commercial relationship with EG Industries Berhad and its subsidiaries SMTT/SMTI/TMSMT

[LEGAL NAME OF SUPPLIER]
[Original Signature And Company Stamp here]

Date:
Full Address:
Name:
Title:

SMT TECHNOLOGIES SDN BHD
Plot 102, Bakar Arang Industrial Estate,
08000 Sungai Petani
Kedah Darul Aman, Malaysia.
Email : admin@esmtt.com Web Site : www.esmtt.com