 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	2 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

1.0 PURPOSE :

To provide a procedure and guideline for the protection of the Intellectual Property (IP) & Confidential Information (CI) at SFO Technologies Pvt Ltd.

2.0 SCOPE :

This procedure applies to the CI & IP data that is generated in SFO Technologies and, shared with SFO Technologies by the customer.

2.1 DEFINITION

2.1.1 Confidential Information


"Confidential Information" means information, whether or not created by the Recipient, that relates to the business or affairs of the Company, its employees, customers or suppliers and is confidential or proprietary to, about or created by the Company, its employees, customers or suppliers and includes, without limitation, the types of information defined in the data classification and other information of a similar nature defined in the Intellectual Property.

2.1.2 Intellectual Property

Intellectual Property" means:

- i. Patents, inventions, applications for patents and reissues, divisions, continuations, renewals, extensions and continuations-in-part of patents or patent applications;
- ii. Proprietary and non-public business information, including inventions, developments, trade secrets, know-how, methods, processes, designs, technology, technical data, schematics, formulae and client lists, and documentation relating to any of the foregoing;
- iii. Works of authorship, copyrights, copyright registrations and applications for copyright registration;
- iv. designs, design registrations and design registration applications;
- v. Trade names, business names, corporate names, domain names, website names and world wide web addresses, common law trade-marks, trade-mark registrations, trade mark applications, trade dress and logos, and the goodwill associated with any of the foregoing;
- vi. Computer software and programs (both source code and object code form), all proprietary rights in the computer software and programs and all documentation and other materials related to the computer software and programs; and
- vii. Any other intellectual property and industrial property and moral rights, title and interest therein, anywhere in the world and whether registered or unregistered or protected or protectable under intellectual property laws.

This is an Electronically generated document, is the latest revision, and does not require signature.
 All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	3 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

3.0 REFERENCE DOCUMENTS

- 3.1 Procedure for Security Function – 62190002.079
- 3.2 Procedure for Control of Documents – CP001
- 3.3 Procedure for Control of Records – CP002.
- 3.4 Acceptable Use Policy Information Systems - SFO-AUP-POL-001.
- 3.5 Data Protection Policy - SFO-DPP-POL-002.
- 3.6 Information Security Incident Management Policy - SFO-ISMS-POL-003.
- 3.7 IT Security Incident Response Procedure - SFO-ISMS-POL-004.
- 3.8 HR Manual - HRM 1000.

4.0 RESPONSIBILITY :


- 4.1 Head of Security:
To provide physical security to prevent theft and unauthorised entry into the SFO Facility and Authorised Area.
- 4.2 Head of IT
To provide protection of the digital and cyber security for the digital data.
- 4.3 Head of HR
To Ensure SFO’s Policy is communicated to the all the employees and acknowledged by all the employees.
To provide training on the CI and IP to the employees.
- 4.4 Document Control
To ensure the compliance of the Control of Documents and Record procedures and to ensure document distribution is as per the procedure.
- 4.5 Head of SCM
To ensure SFO Policy are communicated to Suppliers and Ensure Compliance to this procedure.
- 4.6 Head of Legal
To ensure SFO Policy are in Compliance to this procedure and meet the necessary compliance requirement.

5.0 PROCEDURE

5.1 SFO Value System

Outsourced design and manufacturing Operations require high level of knowledge sharing between customer organization and vendor. Consequently, IP rights of stakeholders are involved in one form or another. Thus intellectual property management and data protection issues are of prime focus area for SFO. SFO believes in building long lasting relationship with customers and suppliers bound by

This is an Electronically generated document, is the latest revision, and does not require signature.
All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	4 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

organizational ethics and upholding the values of Integrity and Confidentiality. Hence we treat IP Protection of our customers with utmost priority.

This document represents our formal commitment to IP protection. Our policies on how IP is handled by SFO employees and how we audit compliance with these policies are described. We are always open to continuous improvement of this policy based on specific suggestions for improvement from our valued customers.

5.2 Physical Security at SFO

The Security function is administered as per the Procedure for Security Function (62190002.079). The Procedure address the following

- Movement of Employees/Visitors
- Material/ Vehicle Movement
- Movement of Shipment
- Handling of Keys
- Emergency Response
- CCTV

5.3 IT Security at SFO

The IT Security function is followed as per the procedure identified in the reference document. The procedures address the following

- Cyber and Network Security
- Data Security and Backup.
- Authorised Use and Transfer of Data Transferring devices like USB Devices.
- Password Policy.
- Unauthorised reproduction of documents.
- VPN & User Management.


5.4 IP Protection at SFO

SFO is committed to protecting customer Intellectual Property (IP) from inception of the project to completion. This is achieved through four primary areas, each of which is regularly validated through our internal and external audits. The four areas include:

- i. Confidentiality Agreement with customers
- ii. Confidentiality Agreement with suppliers, sub-contractors
- iii. Employee confidentiality agreement
- iv. Document control
- v. Employee awareness and training.

This is an Electronically generated document, is the latest revision, and does not require signature.

All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	5 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

5.4.1 Confidentiality Agreement with Customers

- i. Prior to entering into a formal contract with customers, a non-disclosure agreement is signed with customers which legally binds both parties to protect each other's IP and confidential information.
- ii. SFO's has its own standard format for such Non-disclosure agreement as displayed as Attachment A. However, in case, the customer wishes to
- iii. Follow their own standard format, SFO accepts such format after formal review and mutual discussions.
- iv. Such NDA are normally valid during tenure of contract plus one year after termination. However, in exceptional cases, validity period of NDA is mutually discussed and agreed.
- v. Employees who have handled sensitive assignments are legally bound NOT to disclose any of the knowledge acquired by them to SFO's competitor's for a period of 3 years.

5.4.2 Confidentiality Agreement with Suppliers/sub-contractors


- i. All confidential documents, information received from customers on signing of NDA are normally restricted only for internal use among the employees authorised to work on the project.
- ii. However, in certain cases it becomes necessary to share such confidential information among suppliers and/or sub-contractors who are selected to perform specific tasks relating to customer projects. In such cases, a non-disclosure agreement as per the Attachment is signed with such suppliers/sub-contractors prior to sharing confidential information.

5.4.3 Employee Confidentially Agreement

- i. All employees upon joining SFO, sign a Non Disclosure Agreement (NDA) reflecting the organization's need for the protection of information.
- ii. The same shall be signed by all third party personnel's who access, process, communicate or manage the organizations information processing facilities.
- iii. These agreements affirm that our personnel will comply with SFO IP Protection regulations.
- iv. SFO periodically audits personnel files to verify that all employees have signed the confidentiality contracts.

5.4.4 Document Control

This is an Electronically generated document, is the latest revision, and does not require signature.
 All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.


 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	6 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

- i. SFO has defined very stringent processes for management of hard copies of documents as part of our document control policy.
- ii. All documents are classified based on the origin and content. Based on the classification, appropriate security mechanisms are put in place to ensure that all copies of the documents are regularly accounted for, and are returned and disposed of according to SFO process when usage needs have expired.
- iii. Security classifications are at 3 levels – Confidential, Controlled and Uncontrolled.
 - a. Confidential :
These are documents which are given by the customer or can be accessed only by a limited set of employees of SFO
 - b. Controlled :
These are documents which can be under issue control
 - c. Uncontrolled :
These are documents which are publicly accessible
- iv. For issuing any extra copy of any confidential/ controlled documents to a person who is not in list of authorized recipient, such issues shall be logged and returned back after use.
- v. If return of such documents is not possible, they might be destroyed by the user after taking appropriate authorization from Head of Department. After the destruction, the information is passed to document control for record updation.
- vi. Wherever required access control to confidential documents / Controlled documents shall be restricted by providing access control through Read / write options set at various level in the PC.
- vii. Retention of document and destruction of documents is defined in the procedure for control of records.

5.4.5 Employee Awareness and Training

- i. SFO ensures that all the information security related practices of the organization are disseminated to all employees through mandatory training courses.
- ii. These courses are at various levels starting with induction training for all employees joining the organization to role based training for personnel in critical roles like project leaders etc. Attendance by all employees is tracked and audited regularly.
- iii. To ensure attentiveness, effectiveness, and an opportunity for attendees to have their questions addressed, the training courses are conducted by live instructors in a classroom setting with feedback collected on the effectiveness of training.

This is an Electronically generated document, is the latest revision, and does not require signature.
All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	7 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

5.4.6 Audit and Compliance

- i. In order to secure the highest level of adherence on a consistent basis, SFO implements a comprehensive internal audit program. The internal audit program covers, among various other process compliance, adherence to all the practices related to IP protection.
- ii. For internal audits, auditors selected from cross functional teams so that they audit areas independent to their work.
- iii. They are given special training on auditing practices in order to ensure effectiveness.
- iv. The audit is done based on the audit plan and checklist **QXXXX**
- v. The audit to be conducted once in six months.

6.0 CUSTOMER REQUIREMENTS

NA

7.0 EHS ALERT

NA

8.0 ANNEXURE

Annexure 1: Non-Disclosure Agreement (NDA) Format.

NON-DISCLOSURE AGREEMENT

AGREEMENT made this by and between SFO Technologies Pvt. Ltd having an office address at Plot No.2, Cochin Special Economic Zone, Kakkanad, Kochi, India and ABC Inc, (Customer company) having an office address at

1. Recitals


The parties hereto acknowledge that either party may from time to time disclose to the other party information concerning the Discloser’s business, operation, financials, products, technology, and other information regarding Discloser.

2. Definition

“Confidential Information” shall mean all information designed as Confidential Information (as provided in Paragraph 4) and disclosed by Discloser to Recipient, including any electronic configurations, components specifications, logic diagrams, equipment design, operational hardware and software, and related sales and marketing information and plans, except for information that:


This is an Electronically generated document, is the latest revision, and does not require signature.

All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 Electronics Division II	Document #		Rev #	
	Part Number		Page #	8 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

- (a) Is or becomes part of the public domain; or
 - (b) Is known to the Recipient or any of its subsidiaries prior to the disclosure by the Discloser; or
 - (c) Is subsequently lawfully obtained by the Recipient or may of its subsidiaries form a third party; or
 - (d) Is independently developed by the Recipient or any of its subsidiaries without any breach of this Agreement; or
 - (e) Is approved for public release by the Discloser; or
 - (f) Is required to be disclosed b judicial or government action after all legal remedies to maintain such information is secret have been exhausted.
3. Recipients will receive information in confidence and will not disclose Confidential Information to persons other than its employees and consultants nor will Recipients use Confidential Information for the purposes other than to evaluate a potential investment transaction of discloser, except to the extent that Recipients is entitled to use such Confidential Information for other purposes pursuant to other agreements between Discloser and Recipient
4. Disclosure and Protection of Confidential Information
- As to any information which Discloser regards as “Confidential Information” such disclosures shall be made subject to the following conditions:
- (a) If such information is writing, or in a drawing, or in some other tangible form, such information at the time of disclosure must be clearly marked “Confidential Information’.
 - (b) In the event that such information is orally disclosed, as may happen during meetings of the parties, Discloser shall deliver to Recipient, within ten (10) days of such disclosure; a letter specifically identified any such Confidential Information under this Agreement.
5. Recipient shall use Confidential Information for the purpose of this Agreement only and shall not use Confidential Information for its own benefit, nor disclose Confidential Information or any part thereof to any person, corporation or other organization other than Recipient’s employees and consultants and shall restrict circulation of Confidential Information to the same extent necessary to fulfill the purposes of this Agreement. Confidential Information disclosed under this Agreement shall returned to the Discloser promptly at its written request, together with all copies thereof, except for one copy which may be retained in the files of the patent or law department of the Recipient.
6. Except as may be agreed in writing by the parties in advance neither party shall employ or offer to employ any employee of the other party who has been involved in discussions contemplated by this Agreement or concerning whom information has been disclosed during discussions contemplated by this Agreement.

This is an Electronically generated document, is the latest revision, and does not require signature.
 All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.

 SFO TECHNOLOGIES <small>A NeST Group Company</small> Electronics Division II	Document #		Rev #	
	Part Number		Page #	9 of 9
Title: PROCEDURE FOR INTELLECTUAL PROPERTY PROTECTION POLICY				

7. This agreement shall remain in force and effect for one (1) years form the date first above written.
8. This Agreement is executed and delivered within Republic of India and shall be governed under the jurisdiction of Cochin, Kerala, India.
9. This agreement may be executed via facsimile signatures.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date First above written.

SFO Technologies Pvt. Ltd. ABC Inc (A Customer Company)

By : _____ By: _____

Title: _____ Title: _____

Date: _____

_____ Date: _____

9.0 ABBREVIATIONS

Nil

This is an Electronically generated document, is the latest revision, and does not require signature.
All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp.