1. Intellectual Property.

a. **Injectoplast Private Limited (IPPL) Intellectual Property.** The Parties acknowledge that **IPPL** owns or has license to use all patent, trade secret, trademark, service mark, copyright, mask work, know-how and other intellectual property right, whether registered or unregistered, (collectively, "Intellectual Property Rights") of **IPPL** or **IPPL** customers that **IPPL** makes available to Supplier, or to which Supplier has access to, under the Agreement, and Supplier is permitted to use **IPPL** Intellectual Property Rights strictly and solely in conjunction with Supplier's manufacture, supply and/or repair of any Products for **IPPL** or provision of Services for **IPPL**.

b. **To the extent Supplier performs Services or Designs.** a unique part or a modification of the Product ("Supplier Development Services"), the Parties acknowledge and agree that **IPPL** owns and shall own all right, title and interest in and to technical information, computer or other specifications, documentation, reports, memoranda, works of authorship or other creative works, knowledge, or data, written, oral or otherwise expressed, originated by Supplier or its approved subcontractors as a result of work performed Supplier Development Services ("Work Product"). Supplier and its employees shall assign and transfer and does hereby irrevocably assign and transfer to **IPPL** all right, title and interest to all Work Product without additional consideration. The Parties further agree that all Work Product is and shall be **IPPL** Intellectual Property and Supplier shall have no rights or licenses to disclose, use or exploit it in any way other than for the benefit of **IPPL**.

c. **Supplier's Intellectual Property.** Supplier hereby grants to **IPPL** and its affiliates a perpetual, paid-up, royalty-free, non-exclusive, worldwide, irrevocable license to all Supplier's Intellectual Property Rights subsisting or embodied in or used in connection with the Products and Work Product or Services, with a right to grant sublicenses to others, to make, have made, use, distribute, have distributed, combine with product, have combined with products, offer to sell, sell, repair, reconstruct or rebuild, and have repaired, reconstructed or rebuilt, products including the Products and products similar or identical to the Products.

d. **Software.** If any Product or Service requires Software utilization, then Supplier grants and shall grant to **IPPL** a perpetual, irrevocable, nonexclusive, worldwide, royalty-free, fully-paid, transferable and assignable license to use, repair, modify or sell the Software and all related materials (the "Documentation") in conjunction with Products or Services delivered by Supplier. Supplier is responsible for Software support, maintenance, updates and enhancements at its own costs and for implementing commercially reasonable disaster recovery and business continuity procedures.
Supplier represents, warrants, and covenants that the Software will meet all Product warranties described herein and be free from programming errors. If the Software fails to conform to the foregoing warranty, Supplier shall promptly repair or replace the nonconforming Software at no cost to **IPPL**. Supplier further represents, warrants and covenants that the Software is and will remain virus free and will not include any Trojan horses, trap doors, lockouts, interrupt mechanisms or similar disabling software or code that can damage, disable, corrupt, interfere with or delete any element of the Software or the Product. Supplier further warrants, covenants and represents that it has the right to license the Software to **IPPL**, that it is in compliance with the licenses and notices requirements of all free or open-source software incorporated into the Software and the Software does not incorporate any open source software that requires as a condition of its use, modification, or distribution, that Software or any portion thereof be disclosed or redistributed in source code free of charge. "Software" means any operating system software and any other software installed on, associated with, embedded in or delivered with the Product and/or Service, including but not limited to, any

updates, upgrades, patches, new versions, new releases, bug fixes, derivatives, modifications, technological improvements and enhancements to such Software.

2. Confidentiality and Information Security.

a. **Confidentiality**

i. Each Party agrees that all information provided to the other for the purpose of doing business with each other is confidential and proprietary information ("Confidential Information"). In the case of **IPPL**, Confidential Information includes: (i) **IPPL**, its affiliates and customers' specifications, designs, drawings, documents, correspondence, data and other materials related to the Products including Work Product; (ii) all information concerning the operations, affairs and business of **IPPL**, its affiliates and customers; (iii) **IPPL** Tooling; (iv) the Intellectual Property Rights of **IPPL**; and (v) the terms of the Agreement.

ii. Each Party agrees to hold the other Party's Confidential Information in confidence and restrict access to and disclosure of the Confidential Information of the other Party only to those directors, officers, advisors, employees, agents and contractors of the receiving Party (including, in the case of **IPPL**, its affiliates and customers) who have a need to know the Confidential Information. Neither Party will disclose or transfer the other Party's Confidential Information directly or indirectly, to any other person, firm, corporation or entity without the prior written consent of the other Party.

iii. In the event of any unauthorized use or disclosure of any Confidential Information by the receiving Party, the receiving Party will give prompt notice of the disclosure to the disclosing Party and will remedy any unauthorized use or disclosure of any Confidential Information.

iv. A Party's Confidential Information will not include information that (i) is or becomes generally available to the public within the industry to which such information relates other than from unauthorized disclosures in violation of the Agreement, (ii) is lawfully obtained by the receiving Party from a third party which had no obligation of confidentiality to the disclosing Party with respect there to,(iii) is independently developed by the receiving Party without use of the disclosing Party's Confidential Information, or (iv) is approved by the disclosing Party for disclosure. Additionally, the Parties agree that, subject to Supplier's patent and trademark rights, there are no restrictions on **IPPL** use or disclosure of geometric and functional attributes of the Products.

v. Supplier will deliver at no additional charge the Confidential Information of **IPPL** and all copies thereof to **IPPL** promptly upon the expiration or termination of this Agreement or at any other time upon **IPPL** written request (or, at **IPPL** option, will certify, through its general counsel, that **IPPL** Confidential Information and all copies have been securely destroyed).

vi. Supplier acknowledges and agrees that the actual or threatened breach of this Section would cause irreparable harm to **IPPL**, for which money damages would not be a sufficient remedy or difficult to ascertain, entitling **IPPL**.

vii. **Information Security** "**IPPL** Data" means (i) all data and information generated, provided or submitted by, or caused to be generated, provided or submitted by, **IPPL** in connection with this Agreement; (ii) all data and information regarding **IPPL** business collected, generated or submitted by, or caused to be generated, provided or submitted by, Supplier, its employees, subcontractors or Affiliates; (iii) all such data and information processed or stored, or then provided to or for **IPPL**, as part of this Agreement, including data contained in forms, reports and other similar

documents provided by Supplier, its employees, subcontractors or Affiliates as part of this Agreement.

viii. **Safeguards.** Supplier will establish an information security program with respect to **IPPL** Data which: (i) ensures the security and confidentiality of such **IPPL** Data; (ii) protects against any anticipated threats or hazards to the security or integrity of such **IPPL** Data and Supplier's systems that process or store **IPPL** Data, and (iii) protects against any unauthorized use of or access to such **IPPL** Data and such Supplier systems. All of the foregoing shall comply with applicable Law, shall be no less rigorous than those maintained by Supplier for its own data and information of a similar nature, and in no event shall such safeguards and procedures be less than what is standard in the industry for the applicable Services. At a minimum, and without limiting the generality of the foregoing, Supplier's safeguards for the protection of **IPPL** Data shall include at Supplier's own cost: (1) appropriately securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security, disaster recovery, and business continuity procedures; (3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) encrypting any sensitive **IPPL** Data (as identified by **IPPL**) stored on any mobile media or transmitted over public or wireless networks; (6) physically or logically segregating **IPPL** Data from information of Supplier or its other Third Parties so that it is not commingled with any other types of information; (7) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (8) providing appropriate information security training to Supplier's personnel.

ix. **Access Control.** Access to resources, including **IPPL** Information, must be regulated by using information security access controls and authorization mechanisms commensurate with risk. Supplier will secure its computer networks using multiple layers of access controls to protect against unauthorized access. Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls. Supplier will secure remote access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging and monitoring access events and subsequent audits. Supplier will use only the licenced application for VPN access.

x. **Security Assessment.** Upon request by **IPPL**, Supplier will perform an information security assessment, which must, at a minimum, include a review of Supplier's information security program described above, including: (i) external computer networks, (ii) internal computer networks (including wireless networks), (iii) information security architecture, (iv) physical security, and (v) Internet accessible applications. Supplier shall submit to **IPPL** within 30 days following the completion of each Security Assessment:
(1) a summary of the findings, and (2) a plan to cure promptly (and, in any case, within 30 days) any deficiencies identified in such Security Assessment, which Supplier shall implement in accordance with its terms.

xi. **IT Questionnaires.** Upon request, Supplier shall respond to information technology security questionnaires provided by **IPPL**. Supplier represents and warrants that its responses to such questionnaires shall be complete and correct.

xii. **Information Security Breaches.** Supplier will notify on helpdesk@injectoplast.com of any actual or reasonably suspected (a) unauthorized, accidental or unlawful access to, or acquisition, use, loss, disclosure, modification, corruption or processing of, of any **IPPL** Data, or (b) interference with a process, a function or data on a **IPPL**, its affiliate's or third party's information system that adversely impacts **IPPL** business (a "Security Breach") promptly and, in any event, not later than 24 hours after it becomes aware of such circumstances. Supplier's notice will detail the effect on **IPPL**, if known, of the Security Breach, the nature of the Security Breach, and the corrective actions taken or to be taken by Supplier. Supplier shall promptly take all necessary and advisable corrective actions and shall cooperate fully with **IPPL** in all reasonable and lawful efforts to prevent, mitigate or rectify such Security Breach.