Customer System/Customer Data Security Requirements

THESE POLICY AND PRACTICE TERMS SUPPLEMENT EXISTING AGREEMENTS TO WHICH INFOCHIP AND CUSTOMER HAVE AGREED AND THESE TERMS ARE INCORPORATED WHERE REFERENCED IN SUCH EXISTING, VALID AND ENFORCEABLE AGREEMENTS.

InfoChip shall:

- Immediately inform Customer IT if InfoChip becomes aware of or reasonably suspects any breach of, or unauthorized access to Customer system, any Customer Data or any system on which Customer Data resides.
- Use reasonable efforts to maintain secure network connections and utilize industry standard encryption technology while transferring Sensitive Customer Data (including without limitation Sensitive Customer Data comprised of alphanumeric strings (i.e., payment card numbers, SSN, etc.)) over open pathways or storing such information, including without limitation if behind a firewall or other perimeter protection. "Sensitive Customer Data" includes payment card information, personal information of Customer, Authorized End- Users and End Users, personal information of Customer employees (including by way of example and without limitation Social Security Number, driver's license number, or name associated with data such as job performance, or employment files and health or medical records), financial data, trade secrets, or any data that, if improperly disclosed, could result in damage or liability to Customer or Customer Confidential Information.
- Ensure that all inbound and outbound remote access to and from Customer systems and any systems that process, transmit or store Sensitive Customer Data utilize an end-to-end encryption method of InfoChip's election.
- Maintain a firewall at all logical demilitarized zones ("DMZ") and Internet connection points, with access control restricted to that required for authorized use of InfoChip systems, Software Products and Service Offerings and associated applications.
- Prevent possible bridging of Customer systems or networks with non-Customer systems or networks.
- Allow only authorized individuals, including Authorized End-Users, to access Customer systems in connection with Software Products and Service Offerings and immediately terminate authorization/access for individuals that are no longer InfoChip personnel or authorized third - party providers or agents.
- Prevent unauthorized access to Customer systems, or information/data residing therein, including any personal/mobile device or any other portable media.
- Ensure that all remote personal computing systems, workstations and laptops that access Customer systems or process Customer information or data have up-to-date antivirus and firewall software and most recent security patches related to all programs/systems/services accessed and used.

InfoChip will use reasonable efforts to further ensure that all InfoChip personnel or third- party providers or agents with any access to any Customer system comply with the following procedures:

- Have agreed in writing to confidentiality, non-disclosure and security requirements prior to gaining access to any Customer system.
- Not attempt to access any Customer system with anything other than his or her individual Authorized End- User ID provided by Customer; "group IDs" or "generic IDs" are not authorized.
- Not exceed authorized access or attempt to gain unauthorized access to any Customer system, device or asset, including program and data files.
- Not connect any network, computer system, device, site or asset to any Customer system without explicit authorization from Customer.
- Not access any Customer system, device or site from any unauthorized device, location, or software.
- Not remove, copy, compromise or replace system files or processes on any Customer system.
- Not install software on any Customer system unless authorized by Customer Information Technology.
- Any data, software, hardware or other material, equipment or property, including keys, identification badges, cell phones, computers, documentation, computer files or any other such material, owned, leased or operated by

Customer that has been provided to InfoChip in order to provide Software Products and Service Offerings to Customer must be returned to Customer immediately upon termination or expiration of any Customer Agreement; and with respect to any such materials provided to InfoChip personnel or third party providers or agents, at the conclusion of the earliest of its or their relationship with InfoChip and/or Customer.

If so required by Customer, InfoChip shall complete such additional forms, provide such additional information, comply with such additional requirements, and otherwise cooperate with Customer, as Customer shall reasonably require from time to time.

This Policy is subject to revision by InfoChip at any time. If a Policy Change is made, InfoChip will notify the designated representative of Customer.