Information Security Addendum

This Information Security Addendum ("Addendum") is a part of the Agreement and/or SOW to which it is attached and/or incorporated by reference and is subject to the terms and conditions of the Agreement. In the event of any conflicts between this Addendum and the Agreement, this Addendum will prevail.

1.) Information Security Programs and Policies

1.1 Programs and Policies. Zebra's information security program addresses the management of information security and the information security controls employed by Zebra and consisting of:

1.1.1 Documented policies that Zebra formally approves, internally publishes, communicates to appropriate personnel and regularly reviews and updates, as needed.

1.1.2 Documented assignment of responsibility and authority for information security program activities.

1.1.3 Policies or standards covering, as applicable, information asset use, record retention/destruction, information asset classification and management, cryptographic controls, access control, legal and regulatory compliance, operations and communications security and facility security.

1.1.4 Regular testing of the key controls, systems and procedures of the security program.

1.1.5 Use of reasonable administrative, technical and operational measures to ensure Customer's Personal Data is secure.

2.) Risk and Asset Management

2.1 Risk Management. Zebra regularly performs risk assessments and includes controls for risk identification, analysis, monitoring, reporting, and corrective action.

2.2 Asset Management. Zebra appropriately classifies and controls hardware and software assets throughout their life cycle.

3.) Human Resources

3.1 Responsibilities. Zebra employees are informed of their information security and privacy responsibilities under Zebra's policies.

3.2 Employee Controls. Zebra employees who create, process, receive, access, transmit or store ("Handle" or "Handling") Customer's Personal Data:

Must undergo pre-employment background checks and screening.

Are subject to disciplinary processes for violations of information security or privacy requirements.

Must upon termination or applicable role change, return Customer's Personal Data and be denied further access thereto.

4.) Physical and Environmental Safety

4.1 Physical and Environmental Security Controls. Zebra's physical and environmental controls at its data centers are appropriate for the risk associated with Handling Customer's Personal Data and for the Zebra equipment, assets, and/or facilities used to hold and process such information.

4.2 Ongoing Operations. Zebra's data centers containing Customer's Personal Data and Zebra systems are protected from failures of power, networks, telecommunications, water supply, sewage, heating, ventilation, and air-conditioning.

5.) Communications and Operations Management

5.1 Controls. Zebra's communications and operations management control policies and standards address: hardening, change control, segregation of duties, separation of development and production environments, network security, virus protection, media controls, information in transit, encryption, audit logs, and network segregation.

6.) Access Control

6.1 Access Control. Zebra's access controls maintain the confidentiality of Customer's Personal Data as follows:

6.1.1 Authorization process for physical, privileged, and logical access to facilities, systems, networks, wireless networks, operating systems, mobile devices, and system utilities containing Customer's Personal Data.

6.1.2 Zebra employee and third-party access granted only if it is logged, controlled, and needed for the performance of their job function.

6.2 Authentication. Zebra authenticates each employee's identity through appropriate authentication controls such as strong passwords, token devices, or biometrics.

6.3 Customer Systems Isolation. Zebra segregates logically all Customer Personal Data Handled under this Agreement from all other information when such segregation is specified in the Agreement and/or SOW to which this Addendum is attached and expressly incorporated.

6.4 Account Controls. Zebra's account controls include having unique user IDs and restricting access of inactive users.

7.) Information Systems Acquisition, Development and Maintenance

7.1 Systems Development Security. Zebra considers information security to be an important part of all information systems acquisition and/or development and operations.

7.2 Network Diagrams. Zebra develops, documents, and maintains physical and logical diagrams of networking devices and traffic.

7.3 Vulnerability Assessments. Zebra performs vulnerability assessments on systems and applications that Handle Customer's Personal Data.

8.) Information Security Incident Management

8.1 Incident Management Program. Zebra's information security incident management program addresses management of information Security Incidents and system weaknesses. Security Incidents

are any loss, theft, misuse of or unauthorized access, disclosure or destruction of any Customer's Personal Data ("Security Incident").

8.2 Security Incident Reporting. Zebra shall as promptly as commercially reasonable notify Customer if there is a Security Incident involving Customer's Personal Data. Such notice will be given as provided for under the Agreement and to any specifically designated Customer contact.

8.3 Response. Zebra shall reasonably assist Customer to respond to a Security Incident. Customer's response may include: investigating the Security Incident, providing regular updates, determining notice obligations and identifying and executing remediation plans.

9.) Audits and Monitoring

9.1 Reviews and Assessments. Customer or its designated representative may upon thirty (30) days prior written notice to Zebra, no more frequently than annually and at Customer's expense have the right to reasonably monitor, review and assess, in an agreed upon scope and length which shall not unreasonably interfere with Zebra's business and operations, Zebra's security and privacy practices related to Zebra's Handling of Customer's Personal Data.

9.2 Compliance. Zebra maintains compliance at its data centers with SOC 2.

10.) Facilities Security

10.1 Zebra will, at all times: (i) comply with all security rules and regulations in effect when its employees or agents are on the premises of Customer or are accessing its data/systems (regardless of the location); and (ii) maintain internal security measures for physical and electronic access, as appropriate for the industry from which the data is collected (e.g., healthcare, biometric, finance).

11.) Miscellaneous

11.1 Payment Card Industry Data Security Standards. To the extent Zebra agrees in a product-specific offering or SOW to Handle cardholder information (e.g., credit or debit card information), Zebra will be in material compliance with the PCI Security Standards Council's Payment Card Industry Data Security Standard ("PCI DSS") requirements.

11.2 Network Risk Insurance. Zebra currently maintains network risk insurance with minimum limits of coverage of not less than (i) $5,000,000 per claim, covering (exclusive of coverage required under the following clause (ii)) all acts, errors, omissions, network security, and privacy risks (including but not limited to unauthorized access to data or systems, failure of security, breach of privacy, wrongful collection, and disclosure or other mishandling of Personal Data), and coverage for related regulatory defense and penalties, and (ii) $5,000,000 per claim, covering data breach expenses, consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity theft monitoring or remediation services, including, without limitation, on behalf of individuals, and all other incurred remediation expenses. The coverage shall be written on either: (a) an occurrence basis; or (b) a claims-made basis, provided the coverage remains in effect for three (3) years following the date Zebra; (i) no longer Handles Customer Personal Data, and (ii) has completed the destruction of all such information in Zebra's possession or control. Zebra's insurance must be primary and must respond to and pay before any other available coverage of Customer. Zebra will provide to Customer upon its written request certificate(s) of insurance evidencing the current coverage.

11.3 Personal data collected under the Agreement (1) may be transferred, stored and/or processed in the United States or any other country in which Customer, Zebra or its service providers maintain facilities and (2) will be subject to the privacy terms specified in Zebra's online privacy policy and may be processed as specified in the Agreement including its exhibits and SOWs. Zebra and Customer will

abide by the requirements of EU and Swiss data protection laws regarding the collection, use, transfer, retention, and other processing of personal data from the EU and Switzerland as applicable. Customer agrees to ensure personal data provided to Zebra under the Agreement is provided to Zebra in a manner that satisfies the requirements of EU and Swiss data protection laws.

11.4 Applicability of Information Security Addendum. This Addendum is only applicable to an SOW to this Agreement to which it is attached and expressly incorporated.