CONFIDENTIAL INFORMATION AND DATA SECURITY MEASURES

Supplier and Partner shall each meet the additional security and data protection requirements in the mutual protection of End User Data and the protection of Confidential Information, whether belonging to Supplier or Partner. "Confidential Information & Data" includes all Confidential Information, whether belonging to Supplier or Partner, and End User Data. The additional security and data protection requirements include the following:

a. Confidential Information & Data Security Program: Supplier and Partner shall each develop, implement, and maintain a comprehensive information security program to protect Confidential Information & Data (for each of Supplier and Partner, the "Program") that includes all of the following requirements set forth in this part (a):

i. is written (in one or more readily accessible parts);

ii. designates one or more employees to maintain the Program;

iii. sets forth the technical, organizational, and other security measures for identifying, assessing and mitigating reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Confidential Information & Data, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;

2. employee compliance with policies and procedures; and

3. means for detecting and preventing security system failures;

iv. develops security policies for employees (including temporary and contract employees) relating to the storage, access and transportation of records containing the other Party's Confidential Information outside of business premises;

v. has in place an effective program for conducting background checks, in each case only to the extent permissible under applicable law (including any such law requiring such person's consent), on its employees or employee candidates to whom Supplier or Partner, as the case may be, proposes to grant access to PII. For any employee or employee candidate who is proposed to Process PII, background checks will include the following to the extent these items are reasonably available in a given jurisdiction:

1. Criminal Background Check. For any employee or employee candidates in the United States, a criminal background check

covering each country, state, provincial and federal court district, or equivalent, in which such person has lived, worked or attended college or university in the last five years, to verify the absence of a crime involving violence against another person, dishonesty, a sex crime or any other serious crime equivalent to a felony under United States law. For any employee or employee candidates outside of the United States, both Parties must obtain verification for any criminal record with the police, under whose jurisdiction the permanent address or longest stay in the last five years of the subject falls. In such case, a certificate of police authorities, if available, must be provided.

2. ID Verification. Reasonable efforts to ensure that such person has not falsified his or her documents indicating such person's identity, including his or her passport, marriage certificate (if any) and other personal documents.
3. Employment Check. Verification of the employment claimed by such person and such person's qualifications, which may include the education levels and degrees such person claims to have completed and received.
4. Reference Check. Conduct interviews with professional references for such person.
5. Database Check. For any employee or employee candidates outside of the United States, conduct a search for information pertaining to the employee or employee candidate in relevant databases pertaining to court decisions, brokers and brokerages, loan defaults, law enforcement activities, and relevant public information. In addition, the search must be conducted on national news and media resources and the United States Office of the Foreign Asset Control database.
6. Drug Screen. Testing of such person for the unlawful use of illegal drugs.
7. Neither Supplier nor Partner shall allow the Processing of any PII by any employee or employee candidate until the background check of such person passes all of the above elements.

vi. imposes disciplinary measures for violations of the Program's rules;

vii. prevents terminated employees from accessing records containing Confidential Information & Data;

viii. sets forth reasonable restrictions upon physical access to records containing the Confidential Information & Data, and storage of such records and data in locked facilities, storage areas or containers;

ix. regularly monitors to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized Processing of Confidential

Information & Data, and upgrading information safeguards as necessary to limit risks; and

x. reviews the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Confidential Information & Data.

xi. Supplier and Partner shall each educate and train appropriate employees (including temporary employees and contract employees) consistent with their respective Program.

<u>Special End User Data Security Protections:</u>

In order to provide even stricter controls with respect to protecting End User Data (which includes but is not limited to End User PII), Supplier and Partner shall each develop, implement, and maintain the following additional requirements set forth in parts (b), (c), and (d) below:

b. <u>Tenant Role Based Responsibility</u>. Implement access control measures that restrict access to records and files containing PII using industry standard access controls to those who need such information to perform the business function using the "least privilege" model for access. These measures must: be reasonably designed to maintain the integrity of the security of the access controls; require special access rights for access to PII; and limit the number of super-users or users with administrator access to PII.

c. <u>Encryption Key Management</u>. All End User Data must be encrypted at rest. In case of a multi-tenant environment, the keys must be separate per client/tenant. A Key Management Solution must be used to store keys securely.

d. <u>Audit Logging</u>. Audit logs shall be created, where possible, whenever any of the following activities are requested or attempted to be performed by the system/solution:

i. Authentication

A. Account authentication and authorization, whether successful or unsuccessful, such as account login and logout.

B. Failed access attempts and credential suspensions/un-suspension.

ii. Access Controls

A. Grant, modify, or revoke access rights, including but not limited to adding a new account or group, changing account privilege levels, changing file permissions, changing database object permissions, changing firewall rules.

B. Password changes and password resets.

iii. Access to Sensitive Files and Information

A. Create, read, update, or delete confidential information, including confidential authentication information such as passwords.

B. Create, update, or delete information not covered in iii(A) immediately above– note: reads on information not classified as confidential do not need to be logged.

C. Creation, modification, or deletion of system-level objects.

D. Initialization of audit logs.

E. Audit process startup, shutdown, or restart.

F. Logging process startup, shutdown, or restart.

G. Privileged access, operations, and maintenance functions.

H. Use of administrator privileges/functions.

I. All actions performed using root or administrative privileges.

J. For systems subject to PCI Compliance, all individual access to cardholder data.

iv. Network Activity

A. Initiate or accept a network connection.

B. System, network, services or application configuration changes, including installation of software patches and updates, or other installed software changes.

C. Application process startup, shutdown, or restart.

D. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.

E. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system or other security monitoring software or device.

Logs shall identify or contain at least the following elements listed below, directly or indirectly, whenever possible.

Date and Time	Timestamp action was performed, including relevant time-zone information if not in Coordinated Universal Time.
Account ID	Account login identifier
Action Type	Examples include authorize, create, read, update, delete, and accept network connection.
Subsystems	Examples include process or transaction name, process or transaction identifier.
Component Identifiers	Examples include account name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
Process Identifiers	Examples include program or command name.
Target Identifiers	Examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address.

	Note that such identifiers should be standardized in order to facilitate log correlation.
Change Detail	Contains both the before and after values of an updated data element, if feasible.
Violation	Whether the action was allowed or denied by access-control mechanisms.
Description and/or reason-codes	These indicate why the action was denied by the access-control mechanism, if applicable.