Appendix – Security Measures at ICE Datacenter

RISE ICE Data center has implemented and will maintain the following security measures.

Organization of Information Security

Security Ownership
RISE has appointed one security officers responsible for coordinating and monitoring the security rules and procedures.
Security Roles and Responsibilities
RISE personnel with access to Customer Data are subject to confidentiality obligations.
Risk Management Program
RISE performs a risk assessment before processing the Customer Data or launching the services.

Asset Management

Asset Inventory
RISE maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to RISE personnel only.
Asset Handling
RISE classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.

Human Resources Security

Security Training
RISE informs its personnel about relevant security procedures and their respective roles. RISE also informs its personnel of possible consequences of breaching the security rules and procedures.

Physical and Environmental Security

Physical Access to Facilities.
RISE limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.
Protection from Disruptions.
RISE uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference or dysfunction of media components.
Component Disposal
RISE uses industry standard processes to delete Customer Data when it is no longer needed.

Communications and Operations Management

Operational Policy
RISE maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.
Data Recovery Procedures

On an ongoing basis RISE maintains multiple copies of Customer Data from which Customer Data can be recovered. If RISE is notified it stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

Malicious Software

RISE has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

Data Beyond Boundaries

RISE encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.

Event Logging

RISE logs access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

Access Control

Access Policy.

RISE maintains a record of security privileges of individuals having access to Customer Data.

Access Authorization

RISE maintains and updates a record of personnel authorized to access RISE systems that contain Customer Data. RISE deactivates authentication credentials that have not been used for a period of time. RISE ensures that where more than one individual has access to systems containing Customer Data. The individuals have separate identifiers/log-ins.

Least Privilege

RISE restricts access to Customer Data to only those individuals who require such access to perform their job function.

Integrity and Confidentiality

RISE stores passwords in a way that makes them unintelligible.

Authentication

RISE uses industry standard practices to identify and authenticate users who attempt to access the services. RISE ensures that de-activated or expired identifiers are not granted to other individuals.

Passwords

RISE maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. RISE uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network Design.

RISE has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.

Information Security Incident Management

Incident Response Process

RISE maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach and the procedure for recovering data.

Service Monitoring

RISE security personnel verify logs at least every six months to propose remediation efforts if necessary.

Business Continuity Management

Emergency and contingency plans

RISE maintains emergency and contingency plans for the facilities in which RISE information systems that process Customer Data are located.

Redundant storage

RISE's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.