Security Standards

Symantec shall maintain administrative, technical, and physical safeguards for the Symantec Network designed to (i) protect the security and integrity of the Symantec Network, and (ii) protect against the accidental or unauthorized use, destruction, access, disclosure or alteration of Customer Content in the possession or under the management of Symantec as provided under the Services (the "Security Standards"). The "Symantec Network" means Symantec's own data center facilities, servers, and networking equipment/software involved in hosting Customer Content or Data that are under Symantec's reasonable control and are used to provide the Services. The Security Standards will be substantially equivalent to the generally accepted security standards in the IT industry for hosted services similar to Symantec's archiving services. Symantec will conform to the Security Standards during the Term of this Agreement, including the Security Standards in this Appendix ____ to the

Agreement. Symantec may modify its Security Standards under the Agreement for the Services only upon mutual written consent.

1. Logical Access Control

   To enable compliance with Customer's access security control requirements, Symantec shall commit and adhere to:

   (a) access controls

   (b) protect all passwords or access codes assigned to Symantec by Customer

   (c) change passwords immediately upon receipt and every ninety (90) days using complex passwords

   (d) prompt removal of logical access privileges for Symantec staff no longer involved in processing Customer data.

2. Change Control

   Reliably developing, testing and documenting each change according to Symantec change management and control standards, procedures and processes associated with a given Service, while maintaining logical integrity of data, programs and audit trails

3. Back-up and Recovery

Comply with Customer requirements and industry best practices for back-up and recovery, Symantec shall:

(a) deploy appropriate data protection measures, including the placement of data files in secure off-site storage as back-up files, replication of data to other secure DR site, or other to enable efficient system recovery

(b) ensure prompt restart of critical applications and business activities in a timely manner following an emergency or disaster

(c) have a documented disaster recovery plan in place for the Services and test it annually.

4. Staff Accountability

Symantec shall:

(a) use Customer information processed on Symantec systems only for purposes explicitly approved by Customer, except, Symantec may use certain information obtained from the Services, once anonymized ("**Anonymized Information**") for the following purposes: (a) preparing and distributing statistical reports related to security trends and data patterns; (b) distributing Anonymized Information to Symantec customers, in compiled or original formats, for the purposes of providing computer security information; and/or (c) analysis; internal research, product or services development, system improvements, marketing purposes, or for providing general security related services. Anonymized Information shall not include personal information or any information that could identify Customer

(b) certify that all devices, used by Symantec employees and/or by its contractors and connected to Customer's processing environment, are and will continue to be in compliance with the following requirements:

- the most current security patches applicable to all operating systems and software on the device must be applied and be up to date within thirty (30) days of patch release,
- the device must have industry-standard anti-virus and

anti-spyware software installed, running and updated with the latest signature file,

- an industry-standard personal firewall product must be installed and active on the device.

5. Server Security

To enable the integrity, confidentiality and availability of any and all servers used to process Customer information and/or data and to mitigate the threat, risk and impact of external or internal misuse and/or abuse of server platforms, Symantec agrees to:

(a) Restricting employee access to servers and any related systems on a need-to-know / need-to-use business-only basis

(b) Protecting all server access, at a minimum, by a combination of User ID and secret password

(c) Changing all factory pre-set server passwords before commencement of processing and changing them thereafter every ninety (90) days or more frequently

(d) Ensuring that servers are housed in physically secured areas

(e) Hardening of all servers used to process, store and/or transmit Customer data and/or information with such hardening to include, but not be limited to, the removal of all privileges and services, except those that are essential for the performance of the operations for which the servers were installed

(f) Deploying server security scanning tools to periodically report on the status of each server and verify that all settings, parameters and options are in accordance with the agreed upon hardened state for that device and to detect unauthorized changes from the approved server configuration baseline

(g) Retain for a total of fifteen (15) months (three (3) months online and an additional twelve (12) months offline on tape) the following Services specific logs: application logs, Windows security event logs, Intrusion detection system logs, SQL database logs, Firewall logs, Load Balancer logs, Routers/switches logs, IIS web server logs, DNS

server logs, Symantec Endpoint Protection logs. [Pending confirmation.

(h) Reviewing all server security controls defined above on a periodic basis (at least once per year) to enable that they are still in effect.

6. Security of Databases and Data Files

To enable the integrity, confidentiality and general security of any and all databases and data files used to store Customer information and/or data, Symantec shall commit and adhere to:

(a) Storing Customer "Confidential" information (e.g. passwords, customer data, etc.) in an encrypted format

(b) Storing all database servers, data file servers and repository devices containing Customer data in a physically secured area

(c) Restricting all physical and logical access to databases, data files and their resident information and/or data and any systems or network components relating to the processing of transactions on a need-to- know / need-to-use business-only basis

(d) Protecting all access to databases and data files using, at a minimum, a combination of user ID and secret password

(e) Changing all factory pre-set passwords for databases before commencement of processing and changing them thereafter every ninety (90) days or more frequently

(f) Logging all database and data file access activities and storing this activity data in an appropriate manner for a minimum period of ninety (90) days

(g) Logging all transaction data activities and storing this activity data in an appropriate manner for at least ninety (90) days from the date of the transactions

(h) Handling all back-up copies of all database and data file records according to stringent safe-keeping measures and access controls,

with such controls identical or similar to those employed for the primary database or data files

(i) Deploying database security scanning tools to periodically review database configurations and enable compliance with Symantec expected base configurations

(j) Deleting and destroying all instances of any and all Customer information and/or data and related printed matter to enable that transaction and other data cannot be recovered by unauthorized persons in accordance with Symantec's internal policies

(k) Reviewing all database security controls defined above on a periodic basis (at least once per year) to enable that they are still in effect.

7. Network Security

To mitigate the threat, risk and impact of system and/or network intrusion, abuse or misuse, Symantec shall commit and adhere to:

(a) The installation, configuration and activation of a comprehensive, intrusion protection system to continuously prevent, detect and report the occurrence of detected unauthorized network attacks against its systems, such as, but not limited to, penetration attempts, denial of service attacks and excessive probing

(b) Installing network firewalls between servers and public network facing gateways to screen out communication protocols not required for processing Internet traffic

(c) Logging all firewall and gateway activity and storing such activity data in an appropriate manner for a minimum period of twelve (12) months in accordance with Symantec's policies

(d) The protection of data from unauthorized disclosure while in transit through public networks to Customer, or its authorized agents, or its customers, to enable the security of any Bank-owned or Bank- related data

(e) The application of cryptographic techniques, using Secure Sockets

Layer (SSL) Version 3.0 for mutual certificate authentication (Client to Server or Server to Server) and a minimum key length of 128 bits or an equivalent industry-standard cryptographic technique.

8. Protection against Malware

To mitigate the threat, risk and impact of computer viruses, worms, Trojan horses and other malicious types of software, collectively called "malware", Symantec shall commit and adhere to:

(a) The installation, configuration, activation and currency of a comprehensive, , anti-virus and anti-spyware program,

(b) The installation of such anti-virus and anti-spyware software on any and all servers, devices, laptops and workstations that process or store transactions and any other Customer data covered by this Agreement,

(c) The configuration of such software to automatically invoke on start- up and run interactively on a continuous basis on all devices where installed,

9. Security Vulnerabilities and Installation of Security Patches

To mitigate the threat, risk and impact of system and/or network security vulnerabilities, Symantec shall commit and adhere to:

(a) The development and deployment of a process to continually monitor reliable sources for advisories on emerging security vulnerabilities

(b) The identification of specific vulnerabilities that may impact operating environments or platforms used by Symantec on behalf of Customer

(c) An assessment of the criticality of the vulnerability in relation to overall operations to determine the appropriateness of installing the associated security patch applicable to the Services

(d) testing and installation of required security patches in a timely manner.

10. Problem Alert and Escalation and Security Incident Management

To enable appropriate levels of problem alerting and escalation and timely management of security-related incidents, Symantec shall commit and adhere to:

(a) The implementation, maintenance and compliance with Symantec documented problem alert and escalation procedures and

(b) Promptly notifying Customer, in person or by phone, of a confirmed breach affecting Customer's data that results in a comprise of such data. [Pending confirmation]

11. (a) Symantec will make available TLS encryption such that data sent by Customer gateways top any host outside Customer will be encrypted. The control of enforcing the encrypted connection shall be maintained by Customer. Data at rest will be encrypted as stated above and in the Services Description. Such encryption method must use an encryption key or keys that are unique to Customer and different from any other Symantec customers. The private portion of the encryption keys must not be stored on disks without strong cryptographic protections.