ANNEX 1

VERITAS EV.CLOUD SERVICE

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Customer and those of its Affiliates that are permitted contractually to use the Veritas hosted archiving service known as E.V.Cloud ("Service")

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Veritas Technologies LLC in the following circumstances:

a) *as the Veritas entity that procures the provision of "follow the sun" and technical support by the following Veritas entities in the following locations:*

Veritas (Australia) Pty Ltd
207 Kent Street
Level 11 Sydney NSW 2000
Australia

Veritas Technologies (UK) Ltd
350 Brook Drive
Green Park Reading Berkshire RG2 6UH
United Kingdom

Veritas Technologies LLC
2815 Cleveland Avenue
Roseville, MN 55113
USA

Veritas Technologies LLC
801 International Parkway
Suite 1053 Heathrow, FL 32746
USA

Veritas Software Technologies India Private Ltd
EON Wing 4, Cluster A, PlotNo.1 SNo.77
MIDC Knowledge Park, Kharadi Pune- 411014
India

b) where Customer has stipulated that the Service shall be provided from a data center in the U.S.

Data subjects
The Personal Data transferred concern the following categories of data subjects (please specify):

In the context of "follow the sun" support: Workers of the Data Exporter that are named as persons authorised to contact Veritas for support.

In the context of usual Service requests made via cloud.dm@veritas.com address: Workers of the Data Exporter

In the context of the processing of the Customer Data in the Service: Workers of the Data Exporter, its Affiliates and the suppliers and customers, and any other categories of individuals that correspond or interact with the Data Exporter in the course of its business.

Categories of data
The Personal Data transferred concern the following categories of data (please specify):

In the context of "follow the sun" support: name, email name, email address, company name and address, job title, contact number.

In the context of usual service requests made via cloud.dm@veritas.com: name, email address, company name and address, job title, contact number, ip address

In the context of the processing of the Customer Data in the Service: Miscellaneous categories of Personal Data that exist in the various communications and documents archived in the Service.

Special categories of data (if appropriate)
The Personal Data transferred concern the following special categories of data (please specify):

In the context of "follow the sun" support: N/A

In the context of usual service requests made via cloud.dm@veritas.com: N/A

In the context of the processing of the Customer Data in the Service: Miscellaneous categories of Sensitive Personal Data that exist in the various communications and documents archived in the Service.

Processing operations
The Personal Data transferred will be subject to the following basic processing activities (please specify):

In the context of "follow the sun" support: employee/worker contact details are used to verify that the person contacting Veritas for support is the employee/worker of Customer and therefore authorised to seek support on Customer's behalf.

In the context of usual service requests made via cloud.dm@veritas.com: details are used to action and fulfil Customer requests.

In the context of the processing of the Customer Data in the Service: the Personal Data is held by the Customer in the Service for archiving purposes.

ANNEX 2

Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

Details:

Veritas EV Cloud utilizes secured rooms inside secured data centers for the service. All day-to-day business and activity is managed by Veritas Employees.

EV Cloud data is stored in secured rooms in secured data centers. These data centers have:

- 24/7 security patrols, CCTV surveillance
-biometric and/or key card access into the data center room and
-management approved pre-programmed ACLs determine facility access.
- Facility ingress/egress is logged

1. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

Details:

Customer's EV Cloud administrators are responsible for user provisioning of customer personnel.

-Password management rules used for password complexity definition, minimum length, forced password change requirements; retention can be enforced.

-Unique user accounts are provisioned by customer's EV Cloud administrator from Active Directory.

-Veritas does not have access to Customer's content and does not determine how customer shares its content. The customer governs appropriate access to and how the service is used.

2. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised [input, reading, copying, removal] modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

Details:

Role Based Access Controls are available for built in and customer defined roles.

-Roles have segregated duties

-Customer EV Cloud administrators can perform audits /view activity log tracking unique User login access, password reset, search, email volume, exports, and management changes or created surveillance alerts.

-EV Cloud validates SAML 2 assertion cookie back to identity provider SSO URL for login authentication.

- (For Europe) AES customer keys are stored in the regional data center server infrastructure. The keys are encrypted with AES 256 bit encryption

3. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.

- Prohibition of portable media
- Creating an audit trail of all data transfers

Details:

-Private networks are not used. Customers send email archive information through secure encapsulated tunnels using Transport Layer Security v1.2 encryption protocol if customer's gateway supports TLS v1.2.

-All data are encrypted in transit using AES 256 bit encryption.

-Customers must prohibit portable media use
-Note: Veritas has no control over how the customer chooses to transfer or share their content.

-EV Cloud tracks email archive exports

-Isilon's clustered Network Attached Storage (NAS) is used to store data. The proprietary technology file system provides sharding which stripes data across every hard drive and node in a given Isilon cluster. Any email or file is spread across the drives and nodes. Thus anyone gaining access to an Isilon cluster hard drive or node cannot read or reconstruct data.

4. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input;

Details:

-Log tracks unique User login access, password reset, search, email archive exports, management changes

-User activities in database are identified to unique journal addresses, unique database ID and data partitions.

-Note: Veritas has no control over how the customer chooses to transfer or share their content on the web service.

5. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

Details:

-Veritas has included specific language regarding data processing contract instructions and contract performance monitoring into its standard master service agreements (MSAs) or contracts.

6. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

Details:

-EV Cloud uses active/warm data center model. Data is replicated to multiple data center nodes before it is backed up to Tier-2 data storage and replicated over IPSec VPN tunnels to alternate geographically dispersed data center.

-EV Cloud infrastructure has monitoring platforms that evaluate operational performance and alert Veritas Data Center, Engineering and management teams to identify potential issues.

-Tier-2 storage devices hold backups of Tier-1 storage and are stored on separate storage servers from Tier-1 storage. As part of disaster recovery procedures, Tier-2 storage is replicated over IPSec VPN tunnels or unencrypted Veritas private MPLS circuits across geographically separated Veritas Tier 4, SSAE 16/ISAE 3402 Type II compliant data centers daily to ensure that data is stored in more than one data center.

-Veritas Tier 4, SSAE 16/ISAE 3402 Type II compliant data centers have continuous server monitoring, video surveillance, redundant UPS power supplies, and emergency on site generators.

'-Redundant firewalls are used to block internet attacks and promote high availability.

-A network IDS/IPS is uses to analyze and traffic flow based on rules.

-A Security Information Event Management System is managed by the24X7 staffed Security Operations Center

7. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

Details:

-All access is denied except which is specifically granted by management. Access is granted to individual users' accounts performing roles which have limited responsibilities to perform their jobs (least privilege)

-Customer facing systems are on a separate production network and store data at data centers different from internal business systems.

-Applications are developed, tested and promoted production domains which are separate environments. Each environment has management approved personnel assigned roles for responsibilities within domains.