VERITAS™

ANNEX 1

MAINTENANCE/SUPPORT SERVICE

Data exporter

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

Customer and its Affiliates that are contractually entitled to use the Service

Data importer

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

Veritas Technologies LLC as the Veritas company responsible for arranging and supervising 'follow the sun" Maintenance/Support for Veritas Licensed Software.

Data subjects

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

1. *Individuals whose personal data may be being processed within the network of the Customer, whose personal data may be disclosed incidentally in the course of the provision of the Service.*

Categories of data

The personal data transferred concern the following categories of data (please specify):

1. *In relation to the individuals whose personal data may disclosed incidentally, the categories are miscellaneous, but likely to be personal data contained in user names, file names, meta data and system logs.*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

1. *None*

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

1. *Any personal data that the Customer may choose to disclose to the data importer, in the course of the provision of the Service is not required for the provision of support, but when supplied may be processed incidentally to the provision of the Service.*

The Personal Data may be processed at any of the following Veritas locations as part of the provision of '1ollow the sun" Maintenance/Support, which are subject to change on reasonable notice:

Sydney, Australia

333 George St., Sydney NSW 2000, Australia

Reading, UK

1320 Arlington Business Park
Theale, Reading, Berkshire, RG7 SA

Roseville, USA

2815 Cleveland Avenue
Roseville, MN 55113

Heathrow, USA

1001 International Park Lane
Heathrow, FL 32746

Santa Clara, USA

2625 Augustine Drive,
Santa Clara, CA 95054

Pune, India

Tower C, Level 4 & 11-16, Panchshil Business Park – Phase 2, Balewadi High Street, Balewadi, Pune,
Maharashtra 411 045, India

Beijing, China

Tsinghua Science Park B1 No. 1, Zhongguancun East Road, Ste. 601, Tower B Innovation Plaza, Beijing,
Haidian Dist, 100084, China

Seoul, South Korea

Lotte World Tower, 35th Floor, 300 Olympic-ro, Songpa-gu, Sincheon-dong, Seoul, 05551, Korea,
Republic of

Singapore, China

9 Temasek Boulevard, Floor 39, Suntec Tower Two, Singapore, 038989, Singapore

Tokyo, Japan

1-11-44 Akasaka, Minato-ku, Akasaka Intercity 4th Floor
Tokyo, Tokyo 107-0052

Blanchardstown, Ireland

Blanchardstown Corporate Park
2 Stemple Exchange Blanchardstown
Dublin
15
Ireland

Veritas Technologies Armenia"
Adonts 2, Yeraz Business Center, 5th Floor, Yerevan, 0021, Armenia

Veritas Software India LLP
Bangalore, India
135/1, Purva Premier, Residency Road, Purva Premier, Bengaluru, Bangalore, Klarnataka, 560025

Veritas Sofia
Sofia, Bulgaria – 2 Ivan Abadzhiev Street, Sofia, Bulgaria 1784

Please also see Sub processors for Veritas services documentation available at
www.veritas.com/privacy

Access control to premises and facilities

1. **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

2. **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 ccess

    *   Access to IT systems subject to approval from HR management and IT system administrators

3. *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

4. **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

- Using a VPN for remote access, transport and communication of data.

- Prohibition of portable media

- Creating an audit trail of all data transfers

5. **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.

6. **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

7. **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

8.   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.