ANNEX 1

VERITAS INFOMAP

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 service known as InfoMap ("Service")

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

Veritas Technologies LLC as the provider of the Service, either in its own right where the Customer has contracted directly with the Data Importer, or as sub-contractor to Veritas Storage (Ireland) Limited.

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

Any individual whose name appears in the Customer's file names.

Categories of data

Names of individuals who names appear in metadata about files.

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

N/A

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

The metadata are processed to enable the Data Exporter to see the locations and quantities of data held throughout the world as the output of the InfoMap Service. The processing of Personal Data contained within the metadata is incidental to the purposes of the processing.

ANNEX 2

Security Measures

1. 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

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 access
- 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.

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

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

- Firewall and intrusion detection 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