ENCRYPTION KEY
RECOMMENDATIONS AND DISCLOSURES - ORBS

When utilizing RenovoData's ORBS service powered by Asigra Software, customers will have the opportunity to create and manage their own Encryption Keys upon initial installation and configuration of their Asigra DS-Client software giving Customer control of the security and access of their Data.

Upon activation of Services, Customer will be given the opportunity to create two encryption keys, (1) an "Account Key," and (2) a "Private Key."

Account Keys.
Typically the same across all DS-Clients of Customer but dependent on Customer's size, billing structure and internal policies. File de-duplication will work with all DS-Clients with the same Account Key.

Private Keys.
Usually different for each DS-Client of Customer, Customer may request Private Keys to be the same.

RECOMMENDATIONS FOR CUSTOMER'S CARE OF ENCRYPTION KEYS

Access of Data.
Renovo highly recommends Customers use diligence and care when creating and managing their Encryption Keys, as they would handle any other mission critical passwords (hard copy and soft copy stored in secure manner). Once configured, Encryption Keys are stored in an encrypted format in Customer's DS-Client software. **An Encryption Key is the only way the Customer can access or recover the DS-Client software and their backed-up Data.** Loss of Customer's Encryption Keys will prevent anyone from accessing or restoring its Data in the event of a disaster or loss of any server installed with the DS-Client software. At no time will Renovo be able to see Customer's Data.

Loss of Keys.
If Customer loses Encryption Keys, Customer should immediately contact Renovo at support@renovodata.com to set up a new DS-Client with new Encryption Keys and begin the Customer's account refresh process. Customer agrees to pay up to $500.00 for each incident involving a lost Encryption Key and $150.00 per hour for support services related to extensive data migration (2 TB or above) or other specialized services required for Customer to resume backups and gain access to Data.

Quarterly Testing.
Renovo recommends a quarterly test of the encryption keys via the "validation tools" built in to the DS-Client software. For details on how to perform the quarterly test, see "Perform on Demand Validation," in the DS-User Software Guide.

ENCRYPTION KEY SAFEGUARDING

Encryption Key Safeguarding is an additional convenience and security provision that can be enabled from the DS-Client software installed at Customer's site. Customers may manage their Encryption Keys by enabling the "Encryption Key Safeguarding" option at any time. Enabling Encryption Key Safeguarding will forward an encrypted copy of the Encryption Key(s) for storage in RenovoData's DS-System Database.

Instructions for Encryption Key Safeguarding. Instructions are also available in DS-Client User Guide.

To enable Encryption Key Safeguarding of your DS-Client's encryption key(s):

1. Open "DS-User" software and login, go to Main Menu, click "Setup" > Configuration. The DS-Client Configuration screen appears, click on the "Setup" Tab.

2. Click "Enable encryption key forwarding to DS-System"

3. Click Apply.

To forward or delete the encryption keys from the DS-System Database:

1. From DS-User main menu: Click "Setup" > Configuration. The DS-Client Configuration screen appears on the Setup Tab.

2. In the Encryption key safeguard section: Click Forward Now or Request Deletion.

3. The screen will update to indicate if the Encryption Key(s) are Forwarded or Not Forwarded.

Upon forwarding your encryption keys, RenovoData will not be able to read Customer's Encryption Key(s), but will be able to create a Customer Registration Information (.CRI) file with the Customer's Encryption Key(s) embedded for distribution to Customer upon request to Renovo. Requests must be made by emailing support@renovodata.com or calling our office. Any person contacting Renovo for this purpose will be able to recreate a functioning DS-Client that will be able to perform backups and restores for the corresponding Customer account on the DS-System, but keys are not readable or available in clear text.

All Customers should have a policy in effect regarding critical passwords and Encryption Key Management. Use of Encryption Key Safeguarding is not intended to replace an internal, Encryption Key management policy including: (1) recording Encryption Key(s) for each DS-Client and storing a hard copy and soft copy in secure, offsite location; (2) recording of the location of all Encryption Keys; (3) informing multiple people about the location of Encryption Keys and how to access them in the event of a disaster (i.e. recorded in a "run book" or Disaster Recovery Manual).