

# Storage Guardian Proposal

hypothetical

**Jason Henning**

March 8, 2016

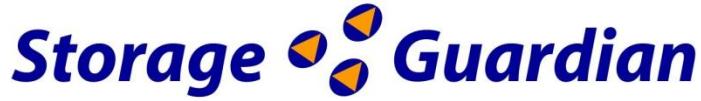
**Storage Guardian Inc.**

Sales Manager

[Jason@storageguardian.com](mailto:Jason@storageguardian.com)

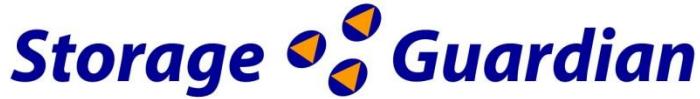
Phone: 1-647-428-5827 x5310

Toll Free 1-888-663-2807 x5310



## Summary of Contents

Management Summary .....	3
Storage Guardian Service Implementation Guide .....	6
DS-Client Installation Support.....	7
Network Diagram.....	8
Storage Guardian Summary.....	9
Storage Guardian Service Guide .....	10



## Management Summary

---

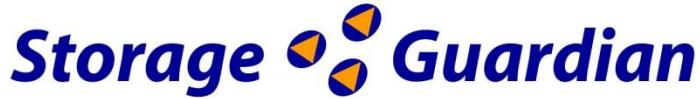
Storage Guardian Inc. would like to thank hypothetical for the opportunity to discuss your needs and submit this overview for Storage Guardian Cloud Backup Services.

Storage Guardian is a reliable, cost-effective alternative to traditional backup methods, with a fully automated, agentless, online solution backing up to Storage Guardian's secure, SSAE Type 1 SOC-2 certified offsite data storage infrastructure. It provides centralized and automated backups of PCs, physical and virtual file and database servers and corresponding immediate online recoveries.

- 👉 **Reduces Risk** – the vulnerability to your organization caused by incomplete backups is essentially eliminated.
- 👉 **Removes the tedious task of managing the backup and restore process.**
- 👉 **Provides a Disaster Contingency** – the service has inherent disaster recovery capabilities, thereby allowing your company to continue in spite of unforeseen disasters.
- 👉 **Dramatically Reduces Restore Times** – for accidentally deleted files, making your employees more productive.
- 👉 **Ease of future planning** – the Storage Guardian service simply expands as your data volumes increase.
- 👉 **Cost Effective** – the Storage Guardian service is priced to be competitive with hardware/software offerings trying to address the same issues.
- 👉 **No capital outlay** – Storage Guardian is charged on a monthly 'utility' basis.
- 👉 **Dramatically Reduces Backup Times** – through advanced software functionality, reducing the actual amount of data transmitted to Storage Guardian.

This proposal reflects the installation of the agentless DS-Client software on any Windows, Mac and Linux system at hypothetical (Windows under VMware or Hyper-V also supported). The DS-Client will connect to the Storage Guardian Data Center via an internet connection.

A full technical overview of the solution is provided in this document for your review.

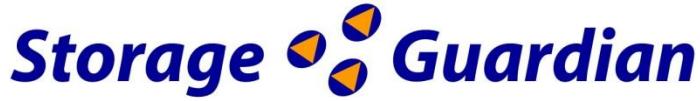


Our pricing model is based on monthly volume, in TBs, protected at the Storage Guardian's Data Storage Center:

<b>Cloud Backup Services, per TB</b>	<b>\$50.00 month</b>
<b>Local Only Backup Services, per TB</b>	<b>\$50/month</b>
DS-Client (Win/Linux/Mac) Backup Software	Included
MS Exchange Plug-In (Message Level Plug In)	Included
MS SQL and MS Sharepoint Plug-Ins (Open and Hot Plug-In)	Included
MS Office 365 Backup	Included
Google Apps Backup	Included
Salesforce.com Backup	Included
Local Restore Option	Included
All installation, consultation and other support (available 24 hours)	Included

Storage Guardian believes that this service will drastically improve current backup and restore services at hypothetical and its customer locations .

***30-day, No Obligation Evaluation Test Software is included with  
FREE training and implementation assistance.***



## Storage Guardian Implementation Guide

---

### Stage 1

- ➊ Installation of DS-Client Evaluation Client
- ➋ Recovery of data backup statistics

### Stage 2

- ➌ Testing and sign-off of functional operation as defined in the Service Level Agreement

### Stage 3

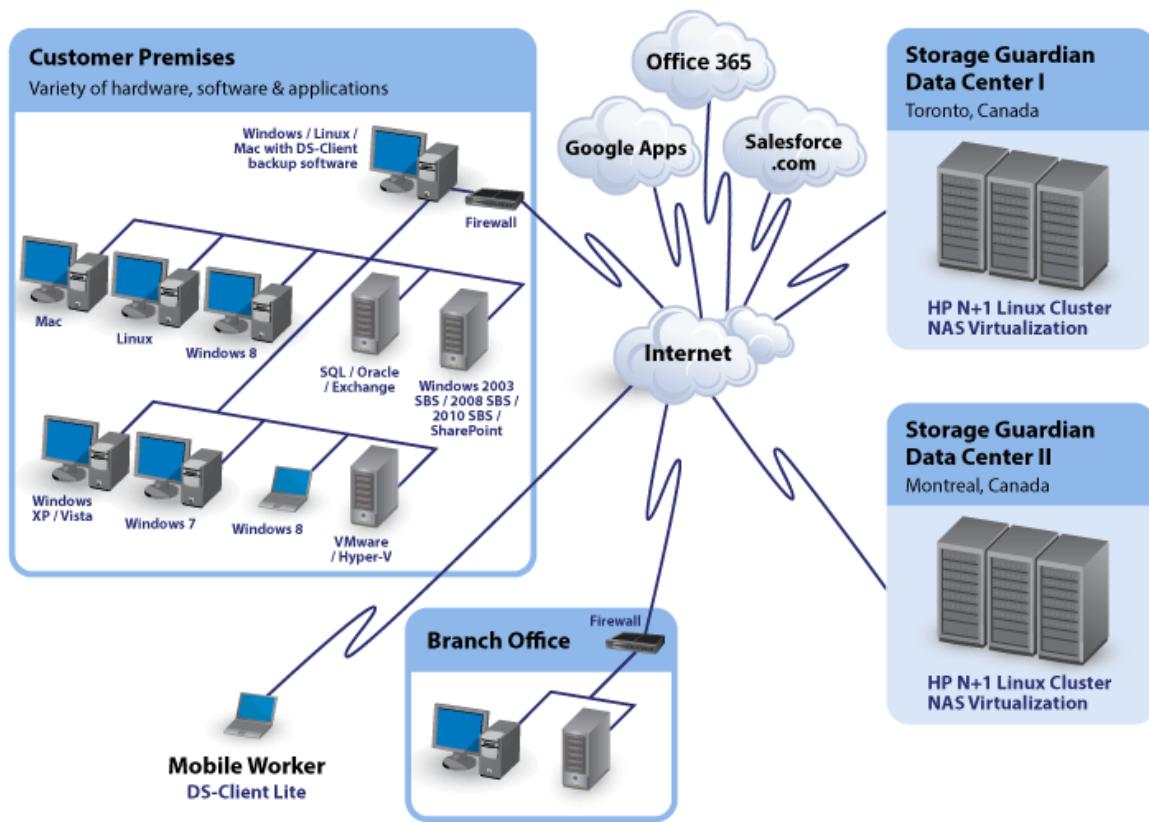
- ➍ Completion of communication between DS-Client and customer's location(s).
- ➎ Initial transfer of customer data offsite, testing and sign-off, as defined in the Service Level Agreement.

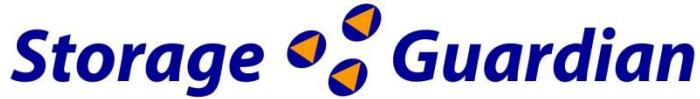
## DS-Client Installation Support

---

Type	OS	Database
<b>Windows (Native or virtual)</b>	<b>Vista</b> <ul style="list-style-type: none"> <li>• Ultimate SP2</li> <li>• Enterprise SP2</li> <li>• Home Basic &amp; Premium SP2</li> <li>• Business SP2</li> </ul> <b>Windows 7</b> <ul style="list-style-type: none"> <li>• Ultimate SP1</li> <li>• Professional SP1</li> <li>• Enterprise SP1</li> </ul> <b>Windows 8</b> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Pro</li> <li>• Enterprise</li> </ul>	<b>MS SQL Server 2005</b> <ul style="list-style-type: none"> <li>• SP4</li> <li>• Express SP4</li> </ul> <b>MS SQL Server 2008</b> <ul style="list-style-type: none"> <li>• Express R2 SP2</li> <li>• Express SP3</li> <li>• Express SP3 R2 SP2</li> <li>• R2 SP2 Express</li> <li>• R2 SP2</li> <li>• SP3 R2 SP2</li> </ul> <b>MS SQL Server 2012</b> <ul style="list-style-type: none"> <li>• SP1 Express</li> <li>• SP1</li> </ul> <b>MS SQL Server 2014</b> <ul style="list-style-type: none"> <li>• Express</li> </ul>
	<b>Windows Server 2008</b> <ul style="list-style-type: none"> <li>• Standard SP2</li> <li>• Enterprise SP2</li> <li>• SBS SP2</li> <li>• Data Center SP2</li> </ul> <b>SBS 2011</b> <ul style="list-style-type: none"> <li>• Standard</li> </ul> <b>Windows Server 2012</b> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Essentials</li> <li>• Data Center</li> </ul>	
<b>Unix (Native or virtual)</b>	<b>SUSE Linux</b> <ul style="list-style-type: none"> <li>• Enterprise Server 11 SP3</li> </ul> <b>Red Hat Linux</b> <ul style="list-style-type: none"> <li>• CentOS 6.5</li> <li>• RHEL 5.9, 5.10</li> <li>• RHEL 6.4, 6.5</li> </ul> <b>Mac OSX</b> <ul style="list-style-type: none"> <li>• Mountain Lion 10.8</li> <li>• 10.9, 10.10</li> </ul>	Embedded PostgreSQL 9.1  PostgreSQL 9.3

## Network Diagram

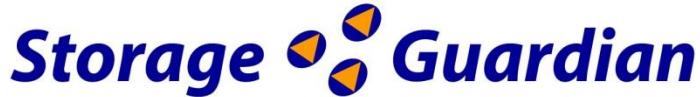




## Storage Guardian Summary

---

- Storage Guardian provides an automated and unattended backup process ensuring that data held on PCs, laptops, file servers, and application/database servers is securely backed up and transferred offsite via the DS-Client software.
- Backup data is transferred offsite to the Storage Guardian secure datacenter via a TCP/IP connection.
- Sophisticated data compression technology, including common file elimination and delta blocking, maximize data transfer over the line connection.
- All AES encryption is performed at customer's site prior to transmission offsite.
- If a dedicated leased line is chosen, then incorporated additional link-level security is increased.
- A Firewall must be incorporated or enabled within the Storage Guardian offering to protect the customer and Storage Guardian network from unauthorized access.
- Storage Guardian provides an easy-to-use interface that simplifies the backup & recovery process and provides detailed information about scheduled operations.
- Centralized configurations of the Storage Guardian DS-Client software enables a network administrator/IT manager to specify exactly what data is to be backed up, ensuring investment is not wasted by backing up unauthorized or unnecessary information.
- Storage Guardian evaluation client enables accurate sizing of data volumes and transfer rates prior to full implementation of service.
- A user-definable number of backup versions of files are retained on disk, for immediate online restore.
- Backup data required for legal or audit purposes can be held archived upon request.
- Backup data can easily be selected and restored online without the need to locate and identify tapes.
- Storage Guardian's response team is on round-the-clock standby to support major data recovery by delivering requested backup data to the customer site.
- In the event of a major customer site disaster, a portable DS-System is delivered to the customer site or to a specified disaster recovery site.



## Storage Guardian Service Guide

---

Storage Guardian is an efficient alternative to traditional backup methods, replacing conventional tape-based systems with a fully automated online solution. It provides centralized and automated backups of PC's, file servers and application/databases servers with secure offsite storage and immediate online restorations.

### **DS-Client Software**

The DS-Client software runs on one server located on the local network. It utilizes standard Microsoft® Windows networking resources to connect to the customer's systems to be backed up and restored. To backup and restore Exchange® and SQL® servers, the DS-Client uses standard Microsoft® applications processing interfaces (APIs) and must be installed on a Windows® system: Windows® 2003/8, Vista, or Windows 7.

Depending on the customer's network configuration, Storage Guardian may require the customer to set up appropriate permissions on any network resource requiring backup and restore capabilities.

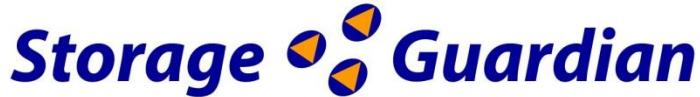
The Storage Guardian DS-Client software is completely agentless, making the application easy to deploy and support.

### **Installation Configuration of the DS-Client**

Storage Guardian will arrange an FTP server to perform the installation and configuration of the DS-Client software. This will involve configuration of the client settings, defining network addresses to the DS-System, registering the DS-Client with the DS-System, and entering the customer's specified encryption keys.

### **Encryption Keys**

For the security of customer's backup data, the DS-Client encrypts every file it sends with an encryption key provided by the customer. The files are stored and remain encrypted on the DS-System at all times. The decryption process occurs during the restore operation of the backup data by the Storage Guardian DS-Client. This ensures that all backup data transferred and stored outside the customer location is always encrypted. Storage Guardian uses a 256-bit AES encryption algorithm and can be configured with two encryption keys: Private and Account.



### Private Key

The private key is the default, and is used by any individual DS-Client to encrypt backup data before it is transmitted to the DS-System at the Storage Guardian data centre.

Backup files that are unique to a DS-Client are encrypted using the DS-Client private key and stored in the Storage Guardian DS-Client private area of the Storage Guardian DS-System.

### Account Key

For customers with more than one DS-Client, an account encryption key is also defined. The account key is used to encrypt files that are common to multiple DS-Clients connected to the same DS-System. These common backup files are encrypted with the account key and stored in that account library area on the DS-System. DS-Clients that share a Storage Guardian DS-System must be configured with the same account key.

The DS System uses encryption cookies to verify every connection by the DS-Client. Cookies are a piece of code generated using the encryption key, but not the key itself. The DS-Client sends its cookie on every connection requested, which the Storage Guardian DS-System compares with the original received during the initial Storage Guardian Client configuration. This verification process ensures integrity of both private and account keys. After initial configuration, the authentication between DS-Client and the DS-System is transparent.

Both private and account encryption keys can be up to 32 alpha/numeric characters long, and are configured during the DS-Client installation. Encryption keys are stored in the Registry in encrypted form, so that even if you have full access to the DS-Client processor (such as the Storage Guardian Customer Support), they cannot be read. Intentional or unintentional changes to the encryption key will make data stored on the Storage Guardian DS-System unusable.

It is the responsibility of the customer to supply appropriate values for the private and account encryption keys. These values, once entered, will not be required again except in the case of a disaster recovery situation where the Storage Guardian client must be re-configured.

***IMPORTANT: The customer is responsible for storing original encryption keys in a secure location. Loss of the keys will prevent recovery of the DS-Client and the customer's backup data. Storage Guardian has no knowledge of the customer's encryption keys.***

# Storage Guardian

## Customer Administrator Console

The Customer Administrator Console is the GUI for the DS-Client and is operated by the customer network administrator to define backup sets and schedules, monitor backup sets and schedules, monitor backups, and perform restores.

The Customer Administrator Console can be installed on one or more of the customer's Windows 7, Vista, and Windows Server 2003, 2008 and 2012 systems. It will be installed and demonstrated during the initial DS-Client configuration.

Customer Administrator Console access is integrated into Windows network security. Individual user accounts, or groups of users, can be defined and granted authority to perform different levels of the Storage Guardian functions.

## Storage Guardian DS-Operator

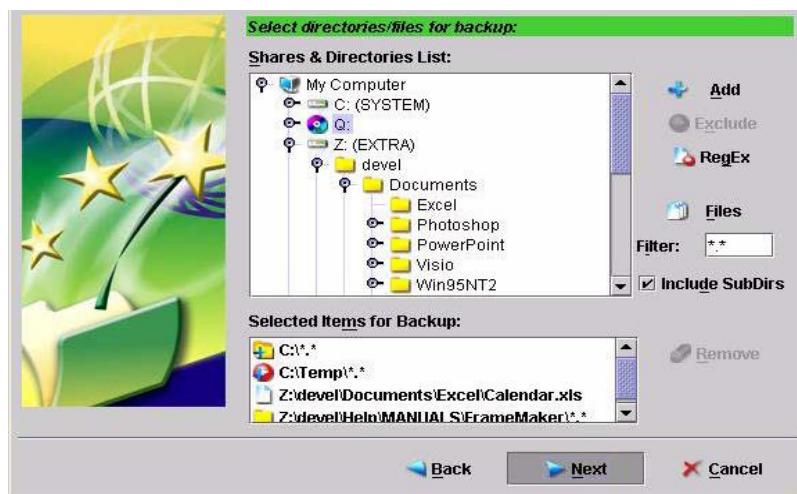
All Storage Guardian operations are performed using the Customer Administrator Console. Authority to perform operations can be controlled by defining access to authorized users or groups of users, thus preventing backup and restoration of data by unauthorized personnel.

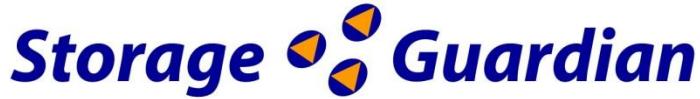
## Backups

Storage Guardian solutions are based on backup sets that define the scope of the backup operation to be performed. Backup sets are executed to perform the specific backup operation and can be executed manually or scheduled to run automatically.

## Backup Sets

A backup set defines the files or databases that are to be backed up. They can include or exclude files or databases by directories, or by filtering the file type. This allows the customer administrator to define backup sets that precisely meet the customer's requirements, thus eliminating the backup of unnecessary data.





In addition, these sets define the number of retained generations, or versions of files and databases backed up. This enables the customer to selectively restore any of the previous versions of files that have been backed up. The default is set at ten generations.

Multiple backup sets can be defined for the same customer system. This feature enables the customer to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be actioned independently.

A backup set can only include data from a single customer system; one or more backup sets must be defined for each system to be backed up.

Backup sets are defined in a similar manner for Microsoft Windows and for backups of Microsoft Exchange, SQL and Sharepoint servers. This single interface enables efficient administration of the Storage Guardian Service.

Authorized administrators can manually execute ad-hoc backups, however, the normal method will be to schedule automatic execution of the backup sets.

### **Open file backup**

By default, Storage Guardian will attempt to backup files that are opened, but not locked, by other applications on the customer system. The customer administrator can further configure this functionality, either globally or by individual backup set, to define the method for handling open files and the number of backup re-tries to perform. The Customer Administrator Console provides comprehensive online help information for defining these options.

Files that are completely locked by another application, such as Microsoft Outlook PST files, will only be backed up using the Message Level Restore Agent available on the Storage Guardian website.

All open files that fail to backup are reported in the activity log on the Customer Administrator Console and in the Storage Guardian status report provided by the Storage Guardian DS-Client GUI.

Storage Guardian provides for the long-term storage of non-critical backup data. This is typically backup data no longer required for day-to-day operations, but required for other business, such as legal or auditing purposes.

# Storage Guardian

Long-term storage backup is performed by defining and executing additional backup sets for the appropriate customer file or data bases systems. These long-term storage backup sets are typically scheduled to execute on a monthly or quarterly cycle, and complement the regular day-to-day backups.

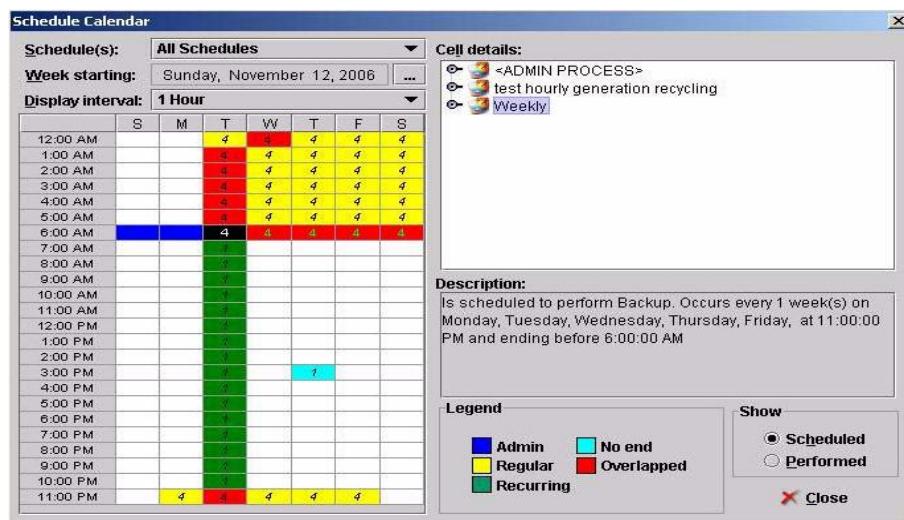
Backup data generated by these long-term storage sets is stored in a separate disk area on the Storage Guardian System and is copied to lower-cost media after a customer-defined interval.

## Backup Schedules

Storage Guardian has an extensive calendar scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or on a more randomly-defined frequency.

Multiple schedules can be defined, and multiple backup sets can be associated with a schedule. Where multiple backup sets are associated with a schedule, the customer administrator can define the number of concurrent backup sets to be executed and the priority in which they should be executed.

The Customer Administrator Console provides a graphical view of the backup schedules. This allows the customer network administrator to quickly view the status of the backups and identify any conflicting or overlapping schedules.



## Monitoring Backups

In addition to the Customer Administrator Console, a web-based interface from the Storage Guardian system presents daily management reports on the status of the Storage Guardian service. This web interface includes a summary of scheduled backups, highlights of any errors that may have occurred, and statistical information detailing the quantity of the backup.

# Storage Guardian

The Customer Administrator Console provides extensive monitoring and reporting capabilities for customer administrators. This includes detailed logs of backup activity, and detailed logs of all files backed up, error reports and audit trails for all backup and restore activity.

## Initial Data Collection

The primary method of backup is over a TCP/IP network DS-Client and the DS-System at the Storage Guardian remote off-site data center.

## Restorations

The Customer Administrator Console allows the authorized customer network administrator to quickly and easily select and restore data. Data can be restored to a remote system; for example, the administrator could use their desktop machine to restore data from a remote server. Multiple restore operations to separate servers can be performed from a single Customer Administrator Console, making this particularly suitable for a Help Desk role.

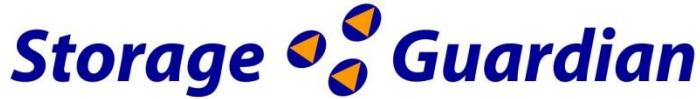
There are two methods in which data can be restored. The first is online, where data is restored across the TCP/IP or dedicated line. The second is where the restore data is delivered via a portable Storage Guardian DS-System. This method is used in the event of a disaster or when a large amount of data needs to be restored.

The primary method of data restoration is online. The Customer Administrator Console provides a Restore Wizard that guides the Customer Administrator through the process of selecting and restoring data. The Restore Wizard allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery.

The screenshot shows the 'Restore' dialog box with the following settings:

- Show:**
  - Latest generation of all data (except deleted data)
  - Latest generation of all data
  - Selective data (from a certain period)
- Restore period:**
  - From: Oct 29, 2003 10:35:05 AM >>
  - To: Nov 1, 2004 11:41:19 AM >>
- Filter:**

Hide data (dirs/files) deleted from source on / before:  
 Nov 1, 2004 11:38:20 AM >>
- File overwrite:**
  - Restore all
  - Restore newer
  - Restore older
  - Restore different
  - Skip existing
- Buttons:** OK (green checkmark) and Cancel (red X)



Having selected the data to be restored, the Storage Guardian DS-Client delivers the data across the communication network from the Storage Guardian DS-System at the Storage Guardian Data Center. The Storage Guardian DS-Client then delivers the data to the specified system on the customer's network. As a part of the operation, all associated security permissions for the data are also restored.

#### **Portable Storage Guardian DS-System Restores**

For larger quantities of data, the customer administrator can invoke the Disaster Recovery Wizard to request that a copy of the backup data be copied to a portable Storage Guardian DS-System.

The Disaster Recovery Wizard provides the same level of restore granularity as the Restore Wizard, but rather than restoring the data across the network, it is copied to a portable Storage Guardian DS-System, which is then transported to the customer site. The customer network administrator can then use the Customer Administrator Console to restore the requested data directly from the Storage Guardian DS-Client to the system being restored.

The only data that can be restored from the portable Storage Guardian DS-System is that which was specified when initially requested. If additional backup data is requested then this can be restored either online or by a new request for a portable Storage Guardian being initiated.

***IMPORTANT: The customer's encryption key must be made available for the data to be successfully restored.***