Securepoint GmbH
Bleckeder Landstrasse 28 21,337 Lüneburg
Tel.: +49 4131 / 24 010
www.securepoint.de | info@securepoint.de

Securepoint Unified Backup

Description of Services

1. 1. Product Description

In Securepoint Unified Backup, Securepoint GmbH provides customers with an internet-based data storage system. With Unified Backup, Securepoint GmbH enables customers and their authorised users (hereinafter referred to as “Clients”) to store the data from their systems on a central, online backup platform operated by Securepoint GmbH. Within the framework of this contract, one or more end-user devices (e.g. PC, notebook, tablet, server) may be configured to use Unified Backup and provided with the necessary access privileges and client software packages.

2. 2. Service Elements

3. 2.1 Standard Services

Unified Backup is provided for the following user scenarios:

- Unified Backup PC Client for PCs and notebooks
- Unified Backup Server Client for servers

The “backup data size” refers to the uncompressed size of data in the defined jobs. The total data size is taken from the latest snapshot at the time of invoicing. The current status thus forms the basis of billing.

A Packet contains 250 GB of data to be saved. Geo-redundant mirroring of data takes place in Hüllhorst and Düsseldorf.

The packet price may be found in the current Securepoint pricelist or requested from your Securepoint reseller.

2.2 Storage Space

Securepoint GmbH provides storage space for data in blocks of 250 GB (also called a “Packet”) on its central online backup platform.

- A separate Packet must be reserved per customer to ensure that customer data are kept separate.
- The maximum number of agents per Packet is unlimited.

2.3 Securepoint Unified Backup

Customer backup data are stored in compressed form on the online backup platform. Once the data is successfully backed up, it is secured with redundant storage.

The system is located in data centres in Hüllhorst and Düsseldorf. Both data centres are within Germany.

2.4 Retention Periods

As the volume of data to be stored forms the basis of invoicing, the following restrictions have been established:

- The maximum retention period for a backup job is 365 days
- The maximum number of restoration points (snapshots) is limited to 44

The customer may define its own retention periods, provided the values listed above are not exceeded. Securepoint GmbH shall ensure that sufficient storage capacity is provided for the defined number of snapshots. This shall not result in any additional cost to the customer.

Where a customer produces a backup plan with more than 44 snapshots, Securepoint is entitled to delete this plan.

2.5 Exceeding Booked Capacity

Should a customer exceed the booked data capacity, e.g. by backing up more data than in the predetermined volume, further Packets will be automatically added in the next month until such time as the data volume is covered. Backup jobs and restore functionality are fully maintained.

26 Client Software

Via the Online Backup Portal, Securepoint GmbH provides the customer and the customer's authorised users, free of charge, with the Client software required for access and usage of online backup. It is up to the customer to install this software on the Client.

Client software must be linked with the Securepoint Unified Backup Portal. This allows for all servers to be centrally administered. It is therefore neither necessary nor possible to administer agents locally.

27 Encryption of Data

The Client software encrypts data for backup using current encryption standards (AES 256-bit CBC) before transmission to the Online Backup Platform. In addition, the backup transmission itself is completely encrypted (AES 128-bit).

A password must be assigned when a backup job is created. This password protects the data from unauthorised access.

The user must retain the password safely, as it cannot be reconstructed. Securepoint GmbH is unable to view backups, change their content or retrieve the encryption password.

Checking data for malware or similar problems must be undertaken by the customer as it cannot be done by Securepoint GmbH. Data infected with malware could infect other Clients when restored at a later date.

2.8 Restoration of Stored Data

Users may restore the encrypted data saved on their user-based data account. In order to restore, the customer must authenticate using the password for the job.

2.9 Working with the Volume Shadow Copy Service

The backup agent uses the Microsoft VSS provider to store data during ongoing operations. The customer is responsible for the orderly function of the VSS provider. The backup agents do not install any separate VSS provider.

2.9.1 Third Party VSS

Third-party VSS providers cannot be used and result in errors. They must be removed from the system in order for it to function correctly.

2.9.2 Contact Person in Case of Failure

In case of a system failure, Securepoint GmbH shall endeavour to provide the best possible support to the customer. More extensive problem analysis, along with support related to VSS faults, can only be provided by Microsoft. Support costs are to be borne by the customer.

2.10 Changes/Extensions to Service

Maintenance slots necessary for changes and extentsions are announced in advance on the website https://status.securepoint.de.

Changes and extensions may mean that the system is unavailable for short periods or must be restarted. This scheduled downtime is excluded from calculating availability and is carried out primarily in the predetermined maintenance slots, with the agreement of the customer or partner.

2.11 One-off Services

One-off services may be requested by email, by telephone or using the Securepoint Reseller Portal.

- Resetting password for Backup Portal
- Sending an existing dataset as the initial backup
- FTP import of uploaded dataset as the initial backup
- Consulting or concept production for customer data backup
- Administrator and user training via the Securepoint partner programme
- Hotline support to answer questions on use of Online Backup and on the installation/deinstallation of the Client software
- Requests for data deletion

2.12 Secure Deletion of Data

The following information must be provided in writing for data deletion: Vault Name, Vault Account Name, Computer, and where appropriate Job.

User data are deleted in compliance with DOD 5220.22-M. The customer/partner shall receive confirmation of deletion once the deletion is successfully completed.

2.13 Operation of Server and System Components

All server and system components necessary for the operation of Online Backup are operated on a technically and organisationally secured high-performance computer network, protected against attacks and unauthorised access via the internet. The Online Backup service is provided with a mean availability of 99.5%, averaged annually. The internet connectivity of the computer network is redundant and with bandwith in line with current technology. The following performance specifications apply to operation and system management:

- 24-hour daily operation;
- automatic recognition of faults within the computer network;
- 24-hour acceptance of fault reports every day(by email or ticket);

- mirroring of data in a second, physically separate data centre

2.14 Access Data

The customer shall receive the necessary access data by email when the Securepoint Unified Backup package is set up.

Access to the Online Backup platform is via the internet. Every use of Online Backup requires authentication of the customer (and/or the customer's authorised user) by way of username (in the form of an email address) and password.

It is not possible to reconstruct the encryption password for a job if this is lost! Securepoint GmbH cannot view backup data.

2.15 Administration and Backup

The customer, or an administrator nominated by the customer, may add users and assign rights with various user roles on the Securepoint Unified Backup Portal. The possible roles may be found on our Wiki at https://wiki.securepoint.de/SUB/Berechtigungen.

The customer and/or administrator will also be advised and warned by email when roles are configured. This requires an independent SMTP server.

The customer is responsible for operation (installation of agents, configuration, test restoration).

3 General

This contract is governed by the General Terms and Conditions of Business, the General Terms and Conditions of Business for Cloud Services and the current pricelist of Securepoint GmbH.