

# Securepoint Unified Backup

## Funktionsumfang

Stand: 07.06.2021 – Version 1.0 – Autor: Jan Michel Jockheck

### 1. Produktbeschreibung

Die Securepoint GmbH überlässt dem Kunden mit Securepoint Unified Backup ein Datensicherungssystem über das Internet. Mit Unified Backup ermöglicht die Securepoint GmbH dem Kunden und den von ihm dazu autorisierten Nutzern (im Folgenden Clients genannt) die Sicherung der in ihren Systemen vorhandenen Daten auf einer von der Securepoint GmbH betriebenen zentralen Online Backup-Plattform. Im Rahmen dieses Vertrages können ein oder mehrere Endgeräte (z. B. PC, Laptop, Tablet-Computer, Server) für die Nutzung von Unified Backup konfiguriert und die hierfür jeweils erforderlichen Zugangsberechtigungen und Client-Softwarepakete abgerufen werden.

### 2. Leistungselemente

#### 2.1 Standardleistungen

Unified Backup wird für die folgenden Anwendungsbereiche erbracht:

- Unified Backup PC-Client für PC und Laptop
- Unified Backup Server-Client für Server

Die „zu sichernde Datenmenge“ bezieht sich auf die unkomprimierte Datenmenge der in den Jobs definierten Daten. Berücksichtigt werden dabei die Gesamtmenge der Daten, die in dem jeweils neuesten Safeset zum Zeitpunkt der Rechnungsstellung erfasst wurden. Der jeweils aktuelle Stand ist damit Grundlage für die Berechnung.

Ein Paket enthält 250 GB zu sichernder Datenmenge. Die Daten werden georedundant in Hüllhorst und Düsseldorf repliziert.

Den Preis für das Paket entnehmen Sie bitte der aktuellen Securepoint Preisliste, bzw. erhalten diese von Ihrem Securepoint Fachhändler.

#### 2.2 Speicherplatz

Die Securepoint GmbH stellt dem Kunden zum Abspeichern seines Backup-Datenvolumens auf ihrer zentralen Online Backup-Plattform einen Speicherplatz (auch Paket genannt) von 250 GB zu sichernden Datenvolumens bereit:

- Je Endkunde muss ein eigenes Paket gebucht werden, um sicherzustellen, dass die Endkundendaten sauber voneinander getrennt werden.
- Die maximale Anzahl von Agenten pro Paket ist unbegrenzt.

## 2.3 Securepoint Unified Backup

Die Speicherung der Backup-Daten des Kunden auf der Online Backup-Plattform erfolgt in komprimierter Form. Nach erfolgreichem Backup des Kunden werden die Daten auf redundant aufgebauten Speichersystemen gesichert:

Die Speicherung erfolgt auf einem System in Rechenzentren in Hüllhorst und Düsseldorf. Beide Rechenzentren befinden sich in Deutschland.

## 2.4 Aufbewahrungsfristen

Da die Berechnungsgrundlage für das Online Backup das zu sichernde Datenvolumen ist, sind folgende Einschränkungen festgelegt:

- Die maximale Aufbewahrungsfrist für einen Backup Job beträgt 365 Tage
- Die maximale Anzahl der Wiederherstellungspunkte (Safesets) ist auf 44 festgelegt

Der Kunde darf eigene Aufbewahrungsfristen definieren, sofern die oben genannten Werte nicht überschritten werden. Im Gegenzug stellt die Securepoint GmbH sicher, dass eine entsprechende Speichermenge für die definierte Anzahl an Kopien bereitgestellt wird. Dem Kunden entstehen hierdurch keine weiteren Kosten.

Erstellt der Kunde Sicherungspläne, die mehr als 44 Safesets erzeugen, ist Securepoint berechtigt diese zu löschen.

## 2.5 Überschreitung der gebuchten Kontingente

Überschreitet der Kunde das von ihm gebuchte Kontingent, indem er z.B. mehr Daten sichert als in dem festgelegten Datenvolumen definiert, so werden automatisch im nächsten Monat weitere Pakete hinzugefügt, bis die Datenmenge gedeckt ist. Die Backup Jobs und Restore Funktionalitäten bleiben in vollem Umfang erhalten.

## 2.6 Client-Software

Die Securepoint GmbH überlässt dem Kunden sowie den von ihm autorisierten Nutzern die für den Zugang und die Nutzung von Online Backup erforderliche Client-Software kostenfrei per Download aus dem Online Backup-Portal im Internet. Die Installation dieser Software auf den Client erfolgt durch den Kunden.

Die Clientsoftware muss mit dem Securepoint Unified Backup-Portal verknüpft werden. Dies dient zur zentralen Administration aller Server. Es ist daher nicht erforderlich und nicht möglich den Agenten lokal zu administrieren.

## 2.7 Verschlüsselung der Daten

Mittels der Client-Software wird eine Verschlüsselung der zu sichernden Daten mittels aktuellem Verschlüsselungsstandard (AES 256 Bit CBC) vor der Übermittlung an die Online Backup-Plattform vorgenommen. Der Backup-Datentransfer ist zusätzlich vollständig verschlüsselt (AES 128 Bit).

Bei der Erstellung des Backupjobs muss ein Passwort vergeben werden. Dieses Passwort schützt den Datenbestand vor unberechtigten Zugriff.

Der Nutzer muss sein Verschlüsselungspasswort sicher aufbewahren, da dieses nicht rekonstruiert werden kann. Die Securepoint GmbH ist weder in der Lage Backups einzusehen oder dessen Inhalt zu verändern noch das Verschlüsselungspasswort auszulesen.

Eine Überprüfung der Daten auf eine evtl. Malware Befall oder ähnliches ist durch den Kunden sicherzustellen und kann nicht durch die Securepoint GmbH erfolgen. Durch Malware befallene Daten können bei einer späteren Wiederherstellung ggf. andere Clients infizieren.

## 2.8 Wiederherstellung der gesicherten Daten

Die Nutzer können eine Wiederherstellung der auf ihrem nutzerbezogenen Datenkonto gesicherten und verschlüsselten Dateien durchführen. Bei dem Wiederherstellungsvorgang muss sich der Kunde mit dem Passwort des Jobs authentifizieren.

## 2.9 Arbeiten mit Volume Shadow Copy Service

Der Sicherungsagent verwendet für die Sicherung im laufenden Betrieb Microsoft VSS-Provider. Für die ordnungsgemäße Funktion der VSS-Provider ist der Kunde zuständig. Es werden keine eigenen VSS-Provider durch den Sicherungsagenten installiert.

### 2.9.1 VSS von Drittanbietern

VSS-Provider von Drittanbietern können nicht genutzt werden und führen zu Fehlern. Sie müssen für eine ordnungsgemäße Funktion vom System entfernt werden.

### 2.9.2 Ansprechpartner im Fehlerfall

Die Securepoint GmbH ist bestrebt, im Fehlerfall den Kunden bestmögliche Unterstützung zu leisten. Tiefergreifende Problemanalysen bzw. Hilfestellungen in Bezug auf VSS-Fehler können nur durch Microsoft erfolgen. Die Supportkosten trägt der Kunde.

## 2.10 Leistungserweiterungen/-änderungen

Die für Änderungen und Erweiterungen notwendigen Wartungsfenster werden vorab auf der Webseite <https://status.securepoint.de> angekündigt.

Änderungen und Erweiterungen können zu einer kurzfristigen Nichtverfügbarkeit des Systems bzw. zu einem Neustart des Systems führen. Diese geplante Ausfallzeit ist von der Verfügbarkeitsberechnung ausgenommen und wird mit Einverständnis des Kunden oder Partners primär in den fest definierten Wartungsfenstern durchgeführt.

## 2.11 Einmalleistungen

Einmalleistungen können per E-Mail, telefonisch oder über das Securepoint Reseller Portal beantragt werden.

- Zurücksetzen des Passwortes zum Backup-Portal
- Einsendung eines vorhandenen Datenbestands als Initial-Backup
- FTP-Import eines hochgeladenen Datenbestands als Initial-Backup
- Consulting bzw. Konzepterstellung für die Datensicherung beim Kunden
- Administratoren- und Nutzer-Schulungen über das Securepoint Partnerprogramm
- Hotline-Support für die Beantwortung von Fragen zur Nutzung von Online Backup sowie zur Installation/Deinstallation der Client-Software
- Anträge auf Datenlöschung

## 2.12 Sichere Datenlöschung

Für die Datenlöschung werden folgende Informationen schriftlich benötigt: Vault Name, Vault Account Name, Computer, ggf. Job.

Das Löschen der Userdaten erfolgt nach DOD 5220.22-M. Nach erfolgreichem Löschvorgang erhält der Kunde/Partner eine Löschbestätigung.

## 2.13 Betreiben der Server und System-Komponenten

Alle Server und Systemkomponenten, die zum Betreiben von Online Backup notwendig sind, werden in einem technisch und organisatorisch abgesicherten, hoch performanten Rechnerverbund betrieben, der vor Angriffen und unberechtigten Zugriffen aus dem Internet geschützt ist. Die Leistung Online Backup steht mit einer mittleren Verfügbarkeit von 99,5 % im Jahresdurchschnitt zur Verfügung. Die Internet-Anbindung des Rechnerverbundes erfolgt über das Internet mit einer dem Stand der Technik entsprechenden Übertragungsgeschwindigkeit und ist redundant ausgelegt. Für Betrieb und System-Management gelten folgende Leistungsmerkmale:

- Betriebszeit täglich von 0.00 bis 24.00 Uhr;
- Automatische Erkennung von Störungen innerhalb des Rechnerverbundes;
- Annahme von Störungsmeldungen täglich von 0.00 bis 24.00 Uhr (per E-Mail oder Ticket);
- Spiegelung der Daten in einem zweiten räumlich getrennten Rechenzentrum

## 2.14 Zugangsdaten

Der Kunde bekommt bei Bereitstellung des Securepoint Unified Backup Pakets die nötigen Zugangsdaten per E-Mail mitgeteilt.

Der Zugang zur Online Backup-Plattform erfolgt über das Internet. Voraussetzung für jeden Zugang zu Online Backup ist die Authentifizierung des Kunden bzw. der von ihm zur Nutzung von Online Backup autorisierten Nutzer mittels Benutzername (in Form einer E-Mailadresse) und eines Passwortes.

Ein Zurücksetzen oder Rekonstruieren des Verschlüsselungspassworts eines Jobs ist bei Verlust nicht möglich! Die Securepoint GmbH hat keine Einsicht in die Backupdaten.

## 2.15 Administration und Backup

Der Kunde bzw. ein vom Kunden benannter Administrator kann über das Securepoint Unified Backup Portal weitere Nutzer anlegen und durch verschiedene Nutzerrollen unterschiedliche Rechte festlegen. Die möglichen Rollen finden Sie in unserem Wiki unter <https://wiki.securepoint.de/SUB/Berechtigungen>.

Zusätzlich erhält der Kunde bzw. Administrator Informationen und Warnhinweise per E-Mail, sofern dies konfiguriert wurde. Dies erfordert einen eigenen SMTP-Server.

Der Kunde ist für den Betrieb (Installation des / der Agents, Konfiguration, Test-Wiederherstellung) verantwortlich.

## 3 Allgemeines

Es gelten die Allgemeinen Geschäftsbedingungen der Securepoint GmbH, die Allgemeinen Geschäftsbedingungen für Cloud Dienstleistungen der Securepoint GmbH sowie die aktuelle Preisliste.