



# SD/SLA

## Cyber Protect CloudCyber Protect Appliance

### 1. Servicebeschreibung

In der heutigen Geschäftswelt sind Daten lebenswichtige, integrale Faktoren und garantieren den Erfolg eines jeden Unternehmens. Umso wichtiger ist somit die Sicherheit und Speicherung der vorhandenen Daten. Cyber Protect eignet sich hervorragend für kleine bis grosse Unternehmen. Es kombiniert eine hochqualifizierte Sicherung ihrer Daten mit zusätzlichen Sicherheitsoptionen.

Unter dem Begriff Cyber Protect ist eine gesamtheitliche Lösung zum Sichern Ihrer IT Infrastruktur zu verstehen.

#### 1.1 Kernfunktionen

##### 1.1.1 Backup und Recovery

Schnelle und zuverlässige Sicherung und Wiederherstellung Ihrer Applikationen, Systeme und Daten – auf jedem Gerät und nach jedem Störfall.

##### 1.1.2 Security

Umfassender Malware-Schutz der nächsten Generation, inklusive KI-basierter Erkennung von Ransomware- und Krypto-Mining-Angriffen.

##### 1.1.3 Cyber Protect Management

Eine umfassende, leistungsfähige Endpunkt-Verwaltung mit einer anwenderfreundlichen Benutzeroberfläche, die hilft, IT-Ressourcen einzusparen.

#### 1.2 Editionen

##### 1.2.1 Cyber Backup

Cyber Backup beinhaltet alle Funktionen zum Sichern und Wiederherstellen Ihrer Daten. Es sind keine Protect Features enthalten. Die Cyber Backup Edition beinhaltet folgende Features:

Sichern und Wiederherstellen von Servern, Workstations, virtuellen Maschinen und Netzlaufwerken

Filebackup und Imagebackup

Backup von Applikationen (ausgenommen Microsoft SQL und Microsoft Exchange clusters, Oracle DB und SAP HANA)

Als Backupziele kann lokaler Speicher oder der Acronis Cloud Speicher mit Standort in der Schweiz ausgewählt werden.

Dashboards und Reports für Monitoring



### 1.2.2 Cyber Protect

Cyber Protect kann in drei Varianten verwendet werden. Die Varianten unterscheiden sich im Umfang der Security, Backup und Protect Funktionen.

### 1.2.3 Essential

Die Variante Essential beinhaltet limitierte Backup Funktionen und legt den Schwerpunkt auf Security und Protect. Geeignet für den Schutz von Thinclients oder Workstations mit geringen Anforderungen bezüglich der Verfügbarkeit bzw. Ausfallzeit.

#### Backup

- Sichern und Wiederherstellen von Servern, Workstations, virtuellen Maschinen
- Nur Filebackup
- Backupziel nur in den Acronis Cloud Speicher mit Standort in der Schweiz

#### Security

- Bewertung der Verwundbarkeit
- Patch-Verwaltung
- Anti-Malware Protection und Web Protection, Exploit prevention, URL Filtering
- Ransomware und Krypto-Mining-Schutz

#### Protect

- Verwalten der Geräte in Gruppen
- Zentralisiertes Planmanagement
- Dashboards und Reports für Monitoring
- HDD Health Überwachung (limitiert)
- Remote desktop und remote assistance
- Software und Hardware Inventory
- Script Execution

### 1.2.4 Standard

Bei der Standard Variante werden die Funktionen von der Essential Variante mit den Funktionen von Cyber Backup ergänzt. Folgende Funktionen kommen bei der Standard Variante hinzu:

#### Backup

- Sichern und Wiederherstellen auch von Netzlaufwerken
- Imagebackup
- Backup von Applikationen (ausgenommen Microsoft SQL und Microsoft Exchange clusters, Oracle DB und SAP HANA)
- Als Backupziele kann auch lokaler Speicher ausgewählt werden.
- Dashboards und Reports für Monitoring



### 1.2.5 Advanced

Cyber Protect Advanced beinhaltet das komplette Feature Set. Folgende zusätzliche Funktionen sind gegenüber der Standard Variante vorhanden:

#### Backup

- Advanced Application Backup von Microsoft SQL cluster, Microsoft Exchange cluster, Oracle DB und SAP HANA)

#### Security

- Forensic Mode
- Backup scan for malware
- Safe recovery
- Corporate whitelist

### 1.2.6 Inkludierter Speicher

Bei den Cyber Protect Varianten Essential, Standard und Advanced ist bei jedem lizenzierten Gerät Cloud Speicher inkludiert. Die Mengen können auf der Webseite von Green oder auf der Preisliste eingesehen werden.

Der inkludierte Speicher wird jedem lizenzierten Gerät dediziert zugewiesen und kann nicht auf andere Geräte angewendet werden. Der inkludierte Speicher ist nicht kummulierbar. Ist der inkludierte Speicher aufgebraucht, wird automatisch zusätzlicher Cloud Speicher (kostenpflichtig) verwendet. Es liegt im Ermessen des Kunden, entsprechende Quotas für die Kostenkontrolle zu definieren.

Cyber Backup beinhaltet keinen inkludierten Cloud Speicher

### 1.2.7 Varianten Upgrades / Downgrades

Ein Wechsel zwischen den Cyber Backup und Cyber Protect Varianten ist jederzeit möglich und kann vom Kunden in eigener Regie durchgeführt werden. Ein Downgrade auf eine kleinere Variante ist nur möglich, wenn die verwendeten Services durch den Kunden vorgängig deaktiviert und entfernt werden.

Green übernimmt keine Verantwortung für möglichen Funktions- oder Datenverlust, welcher aufgrund einer Fehlmanipulation entsteht.

## 1.3 Lizenzierung der Software

### 1.3.1 Lizenzierung pro Gerät

Die entsprechende Lizenzierung der Software erfolgt pro gesichertes Gerät. Wird für die Speicherung der Daten der Acronis Cloud Speicher verwendet, fallen zusätzliche Gebühren pro Gigabyte an (ausgenommen für den in der Lizenz inkludierten Cloud Speicher). Lokaler Backupspeicher oder Speicher auf der Appliance wird nicht mit einer zusätzlichen Gebühr belastet.



### 1.3.2 Lizenzierung per GB

Die Lizenzierung erfolgt pro verbrauchtes Gigabyte im Monat. Lokal verwendeter Speicher wird mit einem reduzierten Preis ebenfalls pro verbrauchtes Gigabyte abgerechnet. Die Anzahl zu sichernden Geräte ist unlimitiert. Es fallen keine Gebühren pro gesichertes Gerät an. Eine reine Lizenzierung per GB ist bei Cyber Protect Cloud und Cyber Protect Appliance nicht vorgesehen.

### 1.3.3 Nicht verwenden des Abonnements

Cyber Protect wird dem Kunden ohne monatliche Grundgebühren zur Verfügung gestellt. green.ch AG behält sich das Recht vor, ein nicht genutztes Abonnement zu kündigen. In jedem Fall wird der Kunde vor einem solchen Schritt per Email darüber informiert. Sollte auf die Information keine Reaktion des Kunden erfolgen, wird das Cyber Protect Portal deaktiviert.

**Ein nicht verwendetes Abonnement besteht dann, wenn über eine Dauer von mind. 3 Monaten keine Gerätelizenzen gelöst sind oder kein Speicherplatz auf der Cyber Protect Cloud genutzt wird.**

## 1.4 Speicherort

Die Verwaltung der Backup- bzw. der Security Funktionen erfolgt immer über das Cyber Protect Cloud Portal von Acronis. Das Portal wird in den Datacenter der Green AG betrieben. Je nach gebuchtem Service kann der Kunde folgende Speicherarten verwenden:

### 1.4.1 Lokaler Speicher (Verwaltet durch den Kunden)

Die Hardware zum sichern der Daten wird vom Kunden im eigenen Netzwerk betrieben und verwaltet.

### 1.4.2 Cloud Speicher (Verwaltet durch Acronis)

Die Daten werden in der Acronis Cloud mit Datenstandort Schweiz gespeichert.

### 1.4.3 Appliance (Verwaltet durch Green)

Die Daten werden auf eine dedizierte Storage Appliance gesichert.

Wird der Speicherstandort nicht durch Green AG verwaltet oder befindet sich die Hardware nicht in einer von Green AG angebotenen Infrastruktur, kann dieses SLA nicht angewendet werden.

### 1.4.4 Appliance Hardware

Unabhängig der Speichergrosse besteht eine Appliance aus 5 Nodes. Jeder Node ist wie folgt ausgestattet:

- 2 GHz, 16 Core Prozessor
- 160 GB RAM
- 5 x 240 GB SSDs (Cache)
- Zwei 1/10GB RJ45 ports und zwei 10GB SFP+ ports



Die Stromversorgung erfolgt redundant mit zwei Stromnetzteilen. Wird die Appliance in einem Rack von Green betrieben, wird die redundante Anbindung an zwei unabhängige Stromfeeds garantiert.

#### 1.4.5 Appliance Speichergrossen

Die Storage Appliance wird mit unterschiedlichen Speichergrossen angeboten. Pro Appliance Typ werden 3 Speichergrossen angegeben.

- 1. Raw capacity (RC)**  
Total zur Verfügung stehender Speicher (Brutto)
- 2. CloudRAID (R1)**  
Spiegelung der Daten über 5 nodes  
(Ausfallsicherheit = n-2)

Appliance Typ	RC (TB)	R1 (TiB)
Appliance S	60	31
Appliance M	120	62
Appliance L	150	78
Appliance XL	180	93
Appliance XXL	210	108
Appliance XXXL	240	124

#### 1.4.6 Appliance Standorte

Der Kunde kann die Appliance innerhalb der Green Datacenter Infrastruktur platzieren. Für die Verwaltung der Backups bzw. Security Funktionen muss der Zugang zum Internet gewährleistet werden. Es stehen folgende Möglichkeiten zur Auswahl.

##### Colocation / Cage

Die Appliance wird in einem Colo Rack oder Cage des Kunden in einem Datacenter von Green betrieben. Die Infrastruktur für den Betrieb der Appliance (Strom, Kühlung, Netzwerk, Zutritt) wird durch den Kunden verwaltet. Der Kunde muss für den Unterhalt der Appliance Green den Zutritt zum Rack oder Cage gewähren.

##### Cube

Die Appliance wird im Swisscube des Kunden installiert und betrieben. Die Infrastruktur für den Cube und somit auch für die Appliance wird durch Green zur Verfügung gestellt. Je nach Grösse bzw. Nutzung des Swisscube muss dessen Ausstattung angepasst werden. Zum Beispiel mittels zusätzlichem Switch für die korrekte Anbindung der Appliance an das interne Netzwerk des Kunden.



### Dedicated Server Rack

Der optimale Standort für die Appliance, wenn der Kunde die Appliance für die Sicherung seiner Virtual Datacenter oder dedicated Server Infrastruktur einsetzt. Die Infrastruktur wird durch Green zur Verfügung gestellt. Die Internetanbindung für die Verwaltung der Appliance wird entweder über die VDC Firewall oder eine Firewall Appliance im dedicated Server Rack zur Verfügung gestellt.

### Shared / Dedicated Rack in anderem Brandabschnitt oder Datacenter Standort

Betreibt der Kunde bereits eine IT Infrastruktur in einem Datacenter von Green, ist es von Vorteil, wenn die Sicherung der Daten in einem anderen Brandabschnitt oder sogar in einem anderen Datacenter stattfindet.

Die Infrastruktur und Anbindung der Appliance an den Standort des Kunden wird von Green eingerichtet.

Darf aufgrund der Data Compliance die Appliance nicht in einem shared Rack betrieben werden, besteht die Möglichkeit zum Einbau der Appliance in ein dediziertes Rack.

### 1.4.7 Anforderungen an die Kundeninstallation

Die Appliance kann in einer Colocation oder in einem Cage des Kunden im Datacenter von Green betrieben werden. Um die Betriebssicherheit zu gewährleisten, werden dafür folgende Anforderungen gestellt:

Umgebungsbedingungen	
Betriebstemperatur	0° bis 40° C
Betriebsfeuchtigkeit	10 bis 85%, nicht kondensierend
Raumluft	Weitgehend staubfrei

Die verfügbare elektrische Leistung am Standort muss den Green Ansprüchen gerecht werden. Green empfiehlt dringend die Verwendung einer unterbrechungsfreien Stromversorgung (verfügbar bei Green), um die Ausfallzeit zu minimieren. Die USV muss entsprechend ausgerüstet sein, um die Stromversorgung der Gerätschaft von Green zu garantieren. Die Ausfallszeit aufgrund eines Stromausfalls beim Kunden vor Ort wird von jeder Vereinbarung in diesem Dokument ausgeschlossen.

Stromversorgung permanent	
AC Eingangsspannung	230 V
AC Eingangsfrequenz	50 Hz
Max. AC Eingangsstrom	2A (230V)



## 1.5 Weiterführende Informationen zum Angebot

Mehr Informationen zum Service (Unterstützte Workloads bzw. Betriebssysteme, Preise, Features ) können unter folgender URL eingesehen werden:

URL für:

Technisches Preis/Factsheet

## 2. Service Level Agreement

Das erfolgreiche Outsourcing von IT-Dienstleistungen erfordert eine transparente Definition der Kunden/Lieferanten-Beziehung. Green AG und der Kunde werden die zu erbringenden Leistungsqualitäten und die zu erbringenden Pflichten (nachfolgend „Service Level“) im nachfolgenden Service Level Agreement („SLA“) regeln.

Das SLA ermöglicht dem Kunden eine definierte Qualität und berechtigt bei nicht erbrachten Leistungen seitens Green AG zur Rückerstattung ihrer monatlichen Gebühren oder eines Teils hiervon (nachfolgend «Service Gutschrift bei Nicht Verfügbarkeit» genannt).

### 2.1 Verfügbarkeit

Green AG ermöglicht die im Folgenden jeweils genannten Verfügbarkeiten der in der Offerte erwähnten Services. Der Ausfall eines Teils eines redundanten Systems wird nicht als Ausfallzeit betrachtet. Kann green.ch die vorerwähnte Verfügbarkeit nicht einhalten, so erkennt der Kunde an und stimmt zu, dass die in den SLA vereinbarten Gutschriften die einzige und ausschliessliche Entschädigung für den Kunden darstellen.

#### 2.1.1 Berechnung der Verfügbarkeit

Verfügbarkeit=  
 $(\text{Betriebszeit} - \text{Ausfallzeit}) / \text{Betriebszeit} * 100$

Green AG bietet Gutschriften, sobald die Serviceverfügbarkeit unterhalb der garantierten Schwellwerte liegt. Dieses Dokument zeigt die Gutschriften als Prozentsatz der Basis der monatlich wiederkehrenden Gebühren (MRC). Diese Gutschriften und Entschädigungen verstehen sich als abschliessend. Weitere oder andere Entschädigungen sind ausgeschlossen.



## 2.2 Allgemeine Massnahmen zur Sicherheit des laufenden Betriebs

Green AG erbringt in seinen Datacentern ausschliesslich Dienstleistungen höchster Qualität und Sicherheit. Die Sicherheit der Kundendaten und die Verfügbarkeit der Dienstleistungen werden unter anderem durch folgende Massnahmen sichergestellt:

- Backbone Leitungen und entsprechendes Equipment ist redundant aufgebaut.
- Segmentierung der Netzwerke und strikte Trennung der unterschiedlichen Datenströme
- Netzwerküberwachung durch hauseigenes NOC („Network Operation Center“)
- Ausschliessliche Verwendung von Markenkomponenten
- Carrier-neutrale und redundante IP-Anbindung des Datacenters

## 2.3 Finanzielle Rückerstattung

Sofern Green AG seine vertraglichen Verpflichtungen nicht nachkommen kann, gewährt Green Gutschriften gemäss den nachfolgenden Abschnitten. Weitergehende Schadenersatzansprüche werden explizit wegbedungen. Der Kunde hat seine Ansprüche bei Green mittels einer Anfrage unter <https://contact.green.ch> geltend zu machen.

### 2.3.1 Nicht wiederherstellbare Daten

Für die Erstellung und Verwaltung der Datensicherung ist der Kunde verantwortlich. Green AG übernimmt keine Haftung für nicht wiederherstellbare Daten, welche nicht über einen managed Service von Green erstellt wurden.

### 2.3.2 Ausschluss von Schadenersatz

In keinem Fall ist eine Partei gegenüber der anderen Partei haftbar für besondere, zufällige, indirekte oder Folgeschäden (einschliesslich entgangener Gewinne oder verlorener Daten), unabhängig davon, ob diese auf Vertragsbruch, unerlaubter Handlung (einschliesslich Fahrlässigkeit), Produkthaftung oder anderweitig beruhen, und unabhängig davon, ob diese Partei auf die Möglichkeit solcher Schäden hingewiesen wurde oder nicht.

### 2.3.3 Mangelnde Verfügbarkeit

Green AG bietet eine Verfügbarkeit pro Kalendermonat von 99.0%.

Kann die Datensicherung aufgrund nicht Verfügbarkeit des Services nicht erstellt werden, können Ansprüche auf maximal 25 % der monatlichen Gebühr geltend gemacht werden.

Eine mangelnde Verfügbarkeit des Services ist gegeben, wenn die Daten aufgrund Nichterreichbarkeit des Services über 24 Stunden nicht gesichert werden können.

Keine SLA-Gutschrift wird gewährt, wenn ein Service für einen bestimmten Zeitraum nicht verfügbar ist, sofern dies insgesamt oder zum Teil durch eine der folgenden Ursachen bedingt ist:





- ein Ausfall von Ausstattung in den Räumlichkeiten des Kunden (falls diese nicht im Besitz von Green AG ist), des Kundenstandortes (etwa durch Stromausfall) oder von Ausstattung eines Lieferanten des Kunden;
- Naturkatastrophen, Terrorangriffe oder andere Force Majeure-Ereignisse;
- ein Ausfall aufgrund von magnetischen / elektromagnetischen Interferenzen oder elektrischen Feldern;
- jede fahrlässige Handlung oder Unterlassung des Kunden (oder von Mitarbeitenden, Vertretern oder Subunternehmern des Kunden), u.a.:
  - Verzögerungen bei der Lieferung notwendiger Ausstattung durch den Kunden;
  - Versäumnis, Green zwecks Tests oder Reparaturarbeiten ausreichend Zugang zu den Einrichtungen zu gewähren;
  - Versäumnis, den Zugang zu den Räumlichkeiten des Kunden zu gewähren um es Green zu ermöglichen, ihren Verpflichtungen hinsichtlich des Services nachzukommen;
  - Versäumnis, entsprechende Gegenmassnahmen hinsichtlich des fehlerhaften Services zu ergreifen, wie von Green empfohlen, oder Hinderung der Anbieterin, diese selbst durchzuführen; oder
  - Versäumnis, Redundanzen zu nutzen, wie sie vom Service Level geboten werden.
  - Fahrlässigkeit des Kunden oder absichtliches Fehlverhalten, darunter auch das Versäumnis des Kunden, vereinbarte Verfahren zu befolgen
- wenn der Kunde den Zugang zum Cage oder den Daten verhindert oder verzögert;
- alle geplanten Wartungszeiträume, wenn der Kunde darüber informiert wurde, und Notfallwartungen, die dazu dienen, künftige Ausfallzeiten zu verhindern; oder
- Abschaltung oder Aussetzung des Services durch Green AG, nachdem der Kunde nicht innerhalb von 45 Tagen ab Rechnungsstellungsdatum bezahlt hat, oder wegen anderer hinreichender Gründe.

## 3. Service Management

### 3.1 Support

Support erfolgt für alle unsere Dienstleistungen über Standardmechanismen:

- Online-Support: via Ticket-System <https://contact.green.ch>
- Live Chat: [www.green.ch](http://www.green.ch)
- Die Green AG Website: <http://www.green.ch/support>
- Als Kunde von Green AG erhalten Sie telefonische Unterstützung unter +41 56 460 23 23 während den Bürozeiten Montag–Freitag von 08.00–17.30 Uhr (ausgenommen vor und an gesetzlichen Feiertagen).
- Kunden mit 7 x 24 Abdeckung kontaktieren während den Bürozeiten ebenfalls die obige Telefonnummer

Bei allfälligen Engineering-Arbeiten, welche durch einen Techniker von Greenausgeführt werden, können kostenpflichtige Aufwände entstehen, welche pro Stunde abgerechnet und dem Kunden in Rechnung gestellt werden können.



### 3.1.1 Erweiterter Support

Der 24/7 Service Desk ist – sofern nicht ohnehin im Leitungsvertrag inbegriffen - als kostenpflichtiger Zusatzservice erhältlich und nur ausserhalb der Bürozeiten zu kontaktieren.

## 3.2 Störfallmanagement

### 3.2.1 Ausfallmeldung

Green AG informiert den technischen Ansprechpartner des Kunden entweder per Telefon oder E-Mail (bei einer schriftlichen Meldung an die Kontaktdaten, die an green.ch mitgeteilt wurden).

### 3.2.2 Ablauf Störfall

Die Philosophie von Green AG ist, dem Kunden eine technisch und betrieblich bestmögliche Verfügbarkeit und Servicequalität zu erbringen. Bei Störungen ist unser Hauptziel die schnelle Bearbeitung und Wiederherstellung der Service-Verfügbarkeit. Der Vorteil für den Kunden ist die Begrenzung des Einflusses auf seine Geschäftstätigkeit. Störfälle und Ausfälle bezüglich "reaktiv" gesteuerten Services müssen vom Kunden gemeldet werden. Nach der Meldung des Ausfalls wird ein Trouble Ticket eröffnet und analysiert. Der Service wird anhand des vereinbarten Service Level wiederhergestellt. Störfälle und Ausfälle auf "proaktiv" gesteuerten Services werden vom Überwachungssystem gemeldet. Der Kunde wird nach Massgabe des vereinbarten Service Level informiert. Wenn sich der Ausfall auf die Geschäftstätigkeit des Kunden auswirkt, hat der Kunde über die entsprechenden Kanäle ein Trouble Ticket zu eröffnen.

### 3.2.3 Pflichten des Supports

- Die Berechtigung der Person, welche die Anfrage einreicht, feststellen und prüfen und mit dem Service Level Agreement zwischen dem Kunden und der Anbieterin vergleichen.
- Den Störfallmanagement-Prozess zu starten, was folgendes umfasst:
  - Erhalt der Anfrage, Eröffnung eines Trouble Tickets und Bestätigung.
  - Den Fehlerbehebungsprozess mit internen und externen Mitteln priorisieren, koordinieren und überwachen.
  - Den Kunden über die ergriffenen Massnahmen, Zwischenlösungen und die Lösung informieren.
  - Den Kunden über die Wiederherstellung der Serviceverfügbarkeit informieren.
  - Analyse der Grundursache und Empfehlungen für das weitere Vorgehen (Änderungsverwaltung).

Im Fall von unerwarteten Verzögerungen bei der Fehlerbehebung, die zu einer Verletzung des SLA führen, wird automatisch eine interne Eskalation gestartet. Je nach Art des Problems sind entweder interne Senior-Mitarbeitende oder der Vertriebs-/Subunternehmer-Support die erste Eskalations-Ebene. Zu diesem Zeitpunkt wird der diensthabende Manager involviert, um sicherzustellen, dass das SLA während des Eskalationsprozesses eingehalten und das Problem rechtzeitig gelöst wird.

### 3.3 Pflichten des Kunden

- Der Kunde liefert alle erforderlichen Kontaktangaben, einschliesslich Kontakte für die Eskalation für alle erbrachten Dienstleistungen, und stellt sicher, dass sie im Falle von Änderungen laufend aktualisiert werden.
- Der Kunde liefert und aktualisiert für Green eine Liste aller Personen, die einen Anspruch auf einen Zugang zum Support haben.
- Der Kunde implementiert und aktualisiert geeignete Mittel für die Identifizierung dieser berechtigten Personen.
- Der Kunde stellt sicher, dass die Informationen zu Änderungen an der Konfiguration, an Schnittstellen, Kanälen, Applikationen und Systemen, die für die Erbringung von Joint-Services relevant sind, der Anbieterin geliefert und jederzeit aktuell sind.
- Der Kunde ist für die ständige Instandhaltung aller Kundenapplikationen verantwortlich. Die Wartung der Kundenapplikationen oder Kundendaten obliegt ausschliesslich in der Verantwortung des Kunden.
- Es darf nur Equipment installiert werden, welches in einwandfreiem Zustand ist und keine Gefahr für Personen und Sachen darstellt.
- Der Kunde hat sicherzustellen, dass Green jederzeit und aus jedem Grund auf die von Green verwaltete Gerätschaft Zugang hat. Falls dies nicht sichergestellt wird, bedeutet dies eine Verletzung der Vereinbarung und kann zu einer Vertragsauflösung führen.
- Bei der Zusammenarbeit mit green.ch Mitarbeitern müssen alle Aktivitäten im Voraus koordiniert werden. Dies beinhaltet den Zusatz von Serviceoptionen wie zum Beispiel zusätzliche Konten oder Netzwerkänderungen.
- Jeder nicht autorisierte Versuch eines Kunden, auf die Gerätschaft von green.ch zuzugreifen ist strikt verboten, sei dies in physischer Art oder in elektronischer. Dies beinhaltet auch CPE (Customer Premise Equipment).

### 3.4 Änderungsverfahren

Änderungen der Kunden-Vereinbarung werden schriftlich vereinbart, soweit nichts Abweichendes vereinbart ist. Änderungen, die nicht in Schriftform vorliegen, sind ungültig. Die im Zusammenhang mit dem Vertragsmanagement entstehenden Kosten werden mangels besonderer Abrede von jeder Vertragspartei selbst getragen.

Die Vertragsparteien prüfen Änderungsangebote und teilen der ersuchenden Partei ihre Zustimmung oder eventuelle Änderungswünsche in der Regel innerhalb von zwei weiteren Wochen nach Vorlage des Änderungsangebots schriftlich mit. Die ersuchte Partei stimmt in der Regel innerhalb von weiteren zwei Wochen nach Vorlage des überarbeiteten Änderungsangebots diesem oder dem alternativen Änderungsangebot zu oder lehnt dieses ab.

Lehnt eine Partei die Abgabe eines Änderungsangebotes begründet ab oder nimmt die andere Partei das Änderungsangebot nicht oder nicht innerhalb der Bindefrist an, so bleiben die vereinbarten Leistungsumfänge und Konditionen unverändert bestehen.



## **4. Rechtliche Bestimmungen**

### **4.1 Vertragsgegenstand, Geltungsbereich**

Dieses SLA gilt nur für das mit dem SLA versendeten Angebot und dem hieraus geschlossenen Leistungsvertrag. Sonstige Verträge zwischen green.ch und dem Kunden bleiben hiervon unberührt. Das SLA ist nur auf die Cyber Security Lösung und seine Optionen, nicht aber auf andere Produktbereiche übertragbar. Im Falle widersprüchlicher Regelungen haben die Vereinbarungen im entsprechenden Leistungsvertrag Vorrang vor den Bestimmungen des SLAs. Daneben gelten die jeweils gültigen Allgemeinen Geschäftsbedingungen der Green AG..

### **4.2 Zustandekommen des Rechtsverhältnisses**

Mit dem Abschluss der Bestellung auf der Website oder durch eine Offerte kommt zwischen Green AG und dem Kunden ein Rechtsverhältnis zustande. Die Messung der SLA-Parameter erfolgt ab dem ersten erfolgreichen Login auf dem Portal.

Dieses Dokument ist ein integrierter Vertragsanhang zur eingereichten Web- oder Offerten Bestellung bei Green AG.

### **4.3 Einhaltung der örtlichen Gesetze**

Der Kunde stellt sicher, dass kein illegaler Datenverkehr über Green AG Verbindungen gesendet wird. Green AG übernimmt dafür keine Haftung.

### **4.4 Beschränkungen**

Alle Entschädigungen für Green AG Services sind auf den in diesem Dokument angegebenen Umfang begrenzt. Keine Gutschrift oder Zahlung erfolgt aus anderen Gründen oder in anderem Umfang als in dem hier angegebenen, einschliesslich – aber nicht beschränkt darauf – Geschäftsverluste seitens des Kunden aufgrund von Ausfallzeiten.

### **4.5 Verwendung von persönlichen Daten**

Kunden akzeptieren ausdrücklich die von Green erlassenen Richtlinien zur Verwendung persönlicher Daten.

Siehe dazu: <http://www.Green/de-ch/übergreench/agb/datenschutz.aspx>

### **4.6 Änderungen**

Green AG behält sich das Recht vor, dieses Dokument zuweilen abzuändern, sofern der Kunde entsprechend schriftlich informiert wird, bevor die Änderungen in Kraft treten. Wenn die Änderungen eine wesentliche Auswirkung auf die Services, die Servicegebühr oder auf andere Pflichten aus diesem Vertrag haben, kann der Kunde diesen Vertrag jederzeit unter Einhaltung der monatlichen Kündigungsfrist schriftlich auflösen.



## 4.7 Versicherung

Green AG Systeme sind gegen entsprechende Risiken versichert. Jedoch werden weder Kundendaten noch die Verfügbarkeit der Services, geliefert vom Kunden zum eigenen Kundestamm, in irgendeiner Weise versichert. Es ist die ausdrückliche Verantwortung des Kunden, Versicherungsschutz zu erhalten. Für Verluste von Geschäftsinformationen oder andere Auswirkungen von Systemausfällen wird kein Schadenersatz gewährt, der über die in diesem Dokument explizit beschriebenen Gutschriften hinausgeht.

## 4.8 Kündigung von Services

Bei Kündigung eines Services muss der Kunde innerhalb von 30 Tagen nach Vertragsende sämtliche Ausstattung die von Green AG zu Erbringung des Services zur Verfügung gestellt wurde, unaufgefordert und in ordnungsgemäsem Zustand an Green AG zurückgeben. Der Kunde ist verantwortlich für alle Gebühren und Kosten, die im Zusammenhang mit dieser Rückübertragung verbunden sind. Der Kunde kann auch einen Techniker der Anbieterin kostenpflichtig beauftragen, die Ausstattung abzuholen, per Post zu schicken oder sich ggfs. Für eine andere Option entscheiden. In den folgenden Fällen ist der Kunde schadenersatzpflichtig für die Kosten von Ersatzhardware:

- Falls die Ausstattung verloren gegangen ist oder nicht innerhalb von 30 Kalendertagen nach Vertragsende zurückgegeben wird.
- Falls die Ausstattung in solch einem Zustand ist, dass die Anbieterin die Hardware nicht mehr für andere Klienten verwenden kann; eine zeitbedingte Abnutzung bleibt vorbehalten.

## 4.9 AGB

Die allgemeinen Geschäftsbedingungen der Anbieterin (Allgemeine Geschäftsbedingungen Green AG) sind integraler Bestandteil der Kunden-Vereinbarung. Allgemeine Geschäftsbedingungen des Kunden finden keine Anwendung. Anderslautende Regelungen in den Unterlagen des Kunden sind nicht anwendbar. Kündigungen, Änderungen und Ergänzungen der Service-Vereinbarung und der Leistungsverträge bedürfen der Schriftform. Auf die Schriftform kann nur schriftlich verzichtet werden. Sollten einzelne Regelungen dieser Service-Vereinbarung oder der Leistungsverträge oder anderer Anhänge zur Kunden-Vereinbarung sich als rechtsunwirksam oder nicht durchführbar erweisen, so tritt an die Stelle der unwirksamen oder undurchführbaren Regelung eine wirksame oder durchführbare, die dem bei Vereinbarung der jeweiligen Regelung vorhandene Willen der Vertragsparteien am nächsten kommt sowie den in der Präambel dieser Service-Vereinbarung aufgeführten gemeinsamen Zielen entspricht. Die neugewählte Regelung darf keine Beeinträchtigung des Verhältnisses zwischen der Leistung der Anbieterin und des Kunden zur Folge haben.

[Green Datacenter AGB's](#)