Leistungsbeschreibung

Cyber Protect Cloud
Cyber Protect Appliance

Version	Datum	Autoren
2.0	29.06.2021	Product Management Green

moving. forward. together.

Inhaltsverzeichnis

1. Service Ausprägungen

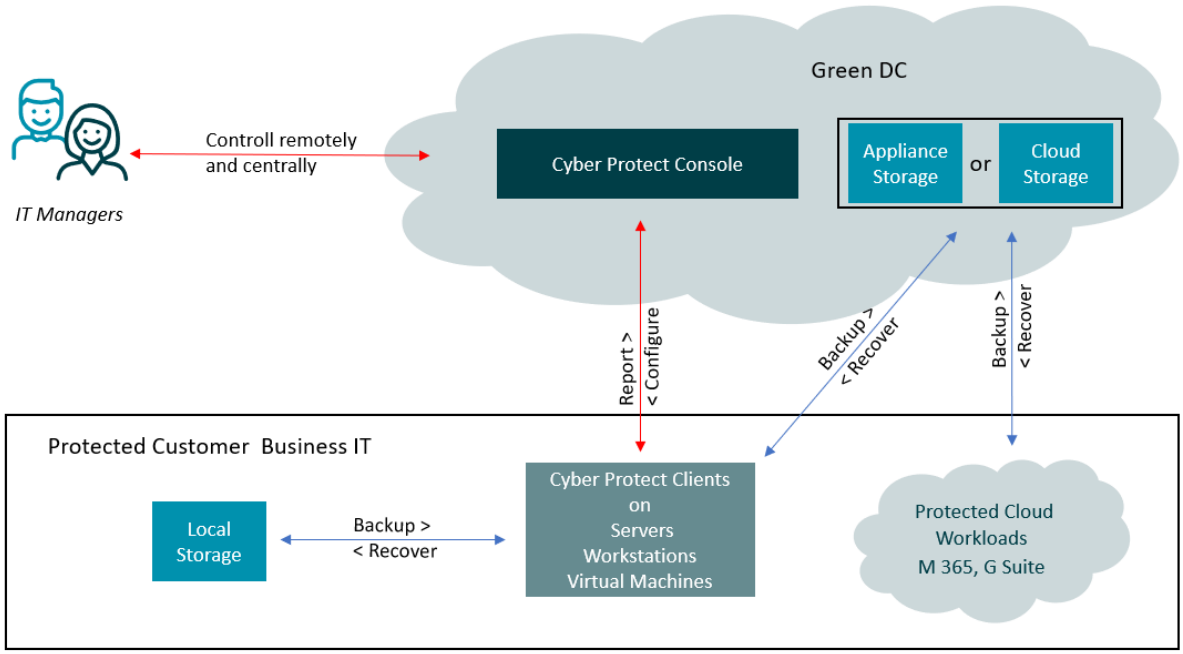
Cyber Protect Cloud vereint professionelle Backup-Funktionen mit einer KI-basierten Antimalware Protection der nächsten Generation und unternehmensgerechten Endpoint Protection Management-Fähigkeiten in einer einzigen Lösung.

Der Service bietet Backup und Recovery auf Laufwerks- und Dateiebene zur Sicherung von Workloads auf mehr als 20 Plattformen. Die KI-basierte Behavioral Engine kann Malware-, Ransomware- und Zero-Day-Angriffe erkennen und stoppen.

Cyber Protect Appliance bietet dem Kunden die Möglichkeit, die identischen Services und Features von Cyber Protect Cloud auf dedizierter Hardware zu nutzen. Die Appliance wird mit diversen Kapazitätsgrössen angeboten und ist optimal auf die Cyber Protect Lösung abgestimmt.

1.1 Service Access Punkt

Die verantwortlichen IT Manager erhalten mittels Cyber Protect Console die komplette Kontrolle über die angebotenen Komponenten.



Die Cyber Protect Console ist über eine reguläre Internet Anbindungen erreichbar.

1.2 Verantwortlichkeiten

Bereitstellung des Service

- Green ist verantwortlich für die Aufschaltung der Cyber Protect Console und stellt über den Partner Acronis den Cloud Storage sowie die Cyber Protect Clients dem Kunden zur Verfügung.
- Green stellt die notwendigen Informationen bezüglich Firewall Regelsets zur Verfügung.
- Der Kunde stellt den Zugriff auf die Cyber Protect Console über das Internet sicher.
- Der Kunde stellt sicher, dass die nötigen Regelsets auf den lokalen Netzwerk Geräten (Firewalls, Router) eingerichtet sind, um die ein- und ausgehenden Datenströme zu ermöglichen.

Betrieb des Service (Appliance)

- Der Kunde muss die korrekte Stromversorgung im eigenen Rack sicherstellen (AC Eingangsspannung 230 V, AC Eingangsfrequenz 50 Hz, Max. AC Eingangsstrom 2A). Die Verantwortung für Ausfallszeiten aufgrund eines Stromausfalls beim Kunden Rack wird explizit ausgeschlossen. Bei einem «Appliance shared oder dedicated Rack» stellt Green die Stromversorgung, die geforderten Umgebungsbedingungen sowie den Zugriffsschutz sicher.
- Der Kunde muss die korrekte Umgebungsbedingungen am Standort sicherstellen (Betriebstemperatur 0° bis 40°C, Betriebsfeuchtigkeit 10 bis 85%, nicht kondensierend, Raumluft weitgehend staubfrei).
- Der Kunde muss die Appliance vor Zugriffen durch unbefugte Dritte schützen. Der physische Zugang zur Appliance darf nur autorisierten Betriebskräften möglich sein.

Betrieb des Cyber Protect Cloud Service

- Green stellt dem Kunden Supportleistungen zur Behebung von Störungen zur Verfügung.
- Der Kunde, sofern er eine Störung feststellt, meldet diese an Green über die unter Abschnitt 3 genannten Kanäle. Im Falle einer notwendigen Störungsbehebung beteiligt sich der Kunde aktiv bei der Fehleranalyse. Für die Kommunikation von Störungen an die Benutzer ist der Kunde verantwortlich.
- Der Kunde muss Green einen verantwortlichen Ansprechpartner nennen, der für den Kunden verbindlich Entscheidungen treffen kann.
- Der Kunde muss Störungen in nachvollziehbarer und detaillierter Form unter Angabe aller für die Ursachenerkennung und -Analyse zweckdienlichen Informationen schriftlich melden.
- Der Kunde muss auf Anfrage von Green einen Protokoll-Trace oder Logfiles von seinen Workloads zur Verfügung stellen, um die Funktionsfähigkeit der Workloads nachzuweisen.
- Der Kunde muss Mitarbeitern der Green Zugang zu seinen Betriebsräumen gewähren, soweit dies für Störungseingrenzung oder –Beseitigung erforderlich ist.
- Green überwacht die bereitgestellte Appliance durch den Business Customer Service (BCS) an 365 Tagen im Jahr (24x7) auf ihre Verfügbarkeit.
- Green installiert die vom Hersteller der Appliance zur Verfügung gestellten, Software Updates und Patches in einem zeitnahen Wartungsfenster (siehe unter Punkt 2.1).
- Anpassungen der Initialkonfiguration, wie zum Beispiel der Änderung von Firewall Regeln, werden nach Prüfung durch das BCS zu Geschäftszeiten ausgeführt. Konfigurationsänderungen ausserhalb der Geschäftszeiten werden gesondert zu den geltenden Stundensätzen verrechnet.
- Green stellt dem Kunden über die Cyber Protect Console Statistiken und Logfiles der eingesetzten Workloads zur Verfügung. Eine Analyse bzw. Interpretation der Logfiles durch Green ist kostenpflichtig.

Beendigung des Service

- Der Kunde muss innerhalb von 30 Tagen nach Vertragsende sämtliche Ausstattung, die von Green zu Erbringung des Services zur Verfügung gestellt wurde, unaufgefordert und in ordnungsgemässem Zustand zurückzugeben.
- 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 verschicken oder sich ggfs. für eine andere Option entscheiden.
- In den folgenden Fällen ist der Kunde schadenersatzpflichtig:
  a. Falls die Appliance abhandengekommen ist oder nicht innerhalb von 30 Kalendertagen nach Vertragsende zurückgegeben wird,
  b. falls die Appliance aus grobfahrlässigem Grund nicht mehr funktionstüchtig ist.
  Sollten die Fälle a. oder b. eintreffen, beträgt die Gebühr mindestens eine Jahresmiete.

1.3 Service Parameter

Es gelten die Service Parameter in der folgenden Tabelle.

1.3.1 Cyber Protect Service

Ausprägungen	Cloud	Appliance
Cloud Speicher (Kapazität)	Unlimitiert	Modellabhängig
Verfügbarkeit	99.9%	99.9%
Lizenzierung Workloads	Pro Device	Pro Device
Lizenzierung Storage	Pro GB	Inklusive
Basic Security (inklusive)	✓	✓
Basic Management (inklusive)	✓	✓
Backup	✓	✓
Advanced Security	✓	✓
Advanced Management	✓	✓

1.3.2 Appliance Hardware

Appliance Modell Nummer	HDD Size	RAW Capacity	Usable Capacity
Modell 15031	4 TB	60 TB	31 TB
Modell 15062	8 TB	120 TB	62 TB
Modell 15078	10 TB	150 TB	78 TB
Modell 15093	12 TB	180 TB	93 TB
Modell 15108	14 TB	210 TB	108 TB
Modell 15124	16 TB	240 TB	124 TB

1.3.3 Appliance Standorte

Die Cyber Protect Appliance kann an folgenden Orten im Green Datacenter aufgestellt werden. Je nach Stellplatz obliegt die sicherstellung der geforderten Betriebsumgebung dem Kunden oder Green.

Standort	Beschreibung	Verantwortlich für Betriebsumgebung
Swiss Cube	Betrieb im eigenen Swiss Cube Rack	Green (shared oder dedicated Rack)
Colocation	Im eigenen Colo-Rack oder Datacenter Cage mit zusätzlichem Switch	Kunde
Shared Rack anderer Brandabschnitt	Rack mit anderen Kunden geteilt, inkl. Strom, Switch und Verbindung	Green (shared oder dedicated Rack)

	zur Kundeninfrastruktur im Green Datacenter	
Dedicated Rack anderer Brandabschnitt	Privates Rack, inkl. Strom, Switch und Verbindung zur Kundeninfrastruktur im Green Datacenter	Green (shared oder dedicated Rack)
Shared Rack georedundant	Rack in einem anderen Datacenter von Green, mit anderen Kunden geteilt, inkl. Strom, Switch und Verbindung (10 Gbit/s) zur Kundeninfrastruktur im Green Datacenter	Green (shared oder dedicated Rack)
Dedicated Rack georedundant	Privates Rack in einem anderen Datacenter von Green, inkl. Strom, Switch und Verbindung zur Kundeninfrastruktur im Green Datacenter	Green (shared oder dedicated Rack)

1.4 Backup Features

1.4.1 Backup und Recovery

Mit dem Backup-Modul können Sie physische und virtuelle Maschinen, Dateien und Datenbanken per Backup sichern und wiederherstellen – und dabei sowohl lokale Storages wie auch einen Cloud Storage als Backup-Ziel verwenden.

1.4.2 Komprimierung und Deduplizierung

Im Cyber Protect Backup-Format (*.tibx) ist automatisch Komprimierung und Deduplizierung aktiviert. Es handelt sich um clientseitige Deduplizierung («In-Archive») mit dem Ziel, dass bereits vorhandene Daten nicht mehr übertragen werden müssen. Je nach Datenstrukturierung kann mit den beiden Verfahren ein vielfaches an Bandbreite und Backupspeicher eingespart werden.

1.4.3 Replikation

Sie können die Backup-Replikation aktivieren, um jedes Backup unmittelbar nach dessen Erstellung am primären Backup-Zielort zu einem zweiten Speicherort kopieren zu lassen, Falls frühere Backups nicht repliziert wurden (weil beispielsweise die Netzwerkverbindung verloren ging), wird die Software auch alle Backups replizieren, die nach der letzten erfolgreichen Replikation erschienen sind. Wenn die Backup-Replikation mitten in einem Prozess unterbrochen wird, werden beim nächsten Replikationsstart die bereits replizierten Daten nicht erneut repliziert, wodurch der Zeitverlust klein gehalten wird.

Replizierte Backups sind unabhängig von den Backups, die am ursprünglichen Speicherort verbleiben (und umgekehrt). Sie können Daten von jedem dieser Backups wiederherstellen, ohne Zugriff auf andere Speicherorte zu haben.

1.4.4 Kontinuierliche Datensicherung (CDP)

Backups werden üblicherweise mit regelmässigen, aber – aus Performance-Gründen – recht langen Zeitintervallen durchgeführt. Wenn das System plötzlich beschädigt wird, gehen die Daten, die in dem Zeitraum zwischen dem letzten (neuesten) Backup und dem Systemausfall geändert wurden, verloren.

Die Funktion Kontinuierliche Datensicherung (CDP) (CDP für die ebenfalls übliche englische Bezeichnung 'Continuous Data Protection') ermöglicht Ihnen, ausgewählte Daten zwischen den geplanten Backups auf kontinuierlicher Basis zu sichern.

- Indem spezifizierte Dateien/Ordner auf Änderungen überwacht werden
- Indem die Dateien von spezifizierten Applikationen auf Änderungen überwacht werden

1.4.5 Forensische Daten

Schadprogramme (wie Computerviren, Malware oder Ransomware) können bösartige Aktivitäten durchführen, wie etwa Daten zu stehlen oder zu verändern. Diese Aktivitäten müssen möglicherweise untersucht werden, was jedoch nur möglich ist, wenn digitale Beweisdaten verfügbar sind. Es kann jedoch vorkommen, dass Teile der digitalen Beweisdaten (wie z.B. bestimmte Dateien oder Aktivitätsspuren) gelöscht werden – oder dass die Maschine, auf der die schädliche Aktivität stattfand, nicht mehr verfügbar ist.

Backups mit forensischen Daten („Forensik-Backups“) ermöglichen Ermittlern, auch solche Laufwerksbereiche zu untersuchen, die normalerweise in einem herkömmlichen Laufwerk-Backup nicht enthalten sind. Die Backup-Option Forensische Daten ermöglicht es Ihnen, folgende digitale Beweisdaten zu sammeln, die dann für forensische Untersuchungen herangezogen werden können: Snapshots von nicht verwendetem Laufwerksspeicherplatz, Speicherabbilder (Memory Dumps) sowie Snapshots von laufenden Prozessen.

Backups mit forensischen Daten werden automatisch digital beglaubigt.

1.4.6 Antimalware-Scan von Backups

Durch die Backup-Scanning-Funktionalität können Sie verhindern, dass infizierte Dateien aus Backups wiederhergestellt werden. Durch Verwendung dieser Funktionalität können Sie überprüfen, ob Ihre Backups sauber sind (also nicht mit Malware infiziert). Die Backup-Scanning-Funktionalität wird nur für Windows-Betriebssysteme unterstützt. Das Backup-Scanning wird vom Cloud Agenten in einer Umgebung außerhalb der entsprechenden Endbenutzer-Maschine durchgeführt, nämlich in der Acronis Cloud.

1.5 Security und Management Features

1.5.1 #CyberFit Score

#CyberFit Score bietet eine Sicherheitsbewertung und einen Scoring-Mechanismus, der die Sicherheitslage eines Rechners bewertet. Er identifiziert Sicherheitslücken in der IT-Umgebung und offene Angriffsvektoren auf Endpunkten und liefert Handlungsempfehlungen für Verbesserungen in Form eines Berichts. Die #CyberFit Score-Funktionalität wird ab Windows 7 (erste Version) und Windows Server 2008 R2 unterstützt.

1.5.2 Antivirus und Antimalware

Das Antivirus & Antimalware Modul kann Ihre Windows-, Linux- und MacOS-Geräte gegen alle aktuellen Malware-Bedrohungen absichern.

- Erkennen von Malware in Dateien – wahlweise im Echtzeit-Modus (Realtime Protection, RTP) oder manuell bei Bedarf ausgeführt (On-Demand-Modus)
- Erkennen von schädlichen Verhaltensmustern in Prozessen (für Windows)
- Blockieren von Zugriffen auf schädliche URLs (für Windows)
- Verschieben von gefährlichen Dateien in eine Quarantäne
- Verwalten einer Positivliste mit vertrauenswürdigen Unternehmensapplikationen

1.5.3 Active Protection

Active Protection überwacht die auf der geschützten Maschine laufenden Prozesse in Echtzeit. Wenn ein fremder Prozess versucht, Dateien auf der Maschine zu verschlüsseln oder eine digitale Crypto-Währung zu berechnen, generiert Active Protection eine Alarmmeldung und führt entsprechende Schutzmassnahmen durch. Active Protection verwendet eine verhaltensbasierte Heuristik, um bösartige Prozesse zu erkennen. Mit diesem Ansatz kann Active Protection auch neue (bisher unbekannte) Malware anhand typischer Verhaltensmuster als Schadsoftware erkennen.

Zusätzlich **verhindert** die Selbstschutzfunktion (Self-Protection), dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie vorhandene Backups, die in lokalen Ordnern gespeichert sind, verändert werden können.

1.5.4 URL Filterung

Malware wird häufig über bösartige oder infizierte Websites mittels der Drive-by Download Methode verbreitet. Mit der URL-Filterung werden Geräte vor Bedrohungen wie Malware und Phishing geschützt, indem Benutzerzugriffe auf bestimmte Websites blockiert werden. Die verwendete URL-Filterungsdatenbank enthält Daten über Websites mit strittigen Informationen über Pandemien, Scam- und Phishing-URLs.

1.5.5 Microsoft Defender Antivirus

Microsoft Defender Antivirus ist eine integrierte Antimalware-Komponente von Microsoft Windows, **die seit** Windows 8 mit dem Betriebssystem ausgeliefert wird.

Das Microsoft Defender Antivirus (WDA)-Modul ermöglicht es, eine WDA-Sicherheitsrichtlinie zu konfigurieren und deren Status über die Cyber Protect Console zu überwachen. Dieses Modul ist auf Maschinen anwendbar, auf denen Microsoft Defender Antivirus installiert ist.

1.5.6 Quarantäne

Die Quarantäne ist ein isolierter Ordner auf dem internen Laufwerk eines Clients oder Server. Dort werden verdächtige Dateien abgelegt. Dieses Vorgehen verhindert die weitere Ausbreitung der Bedrohung. Die Quarantäne ermöglicht es, verdächtige und potenziell gefährliche Dateien auf dem Gerät zu überprüfen und das weitere Vorgehen zu bestimmen.

1.5.7 Schwachstellenbewertung und Patch-Management

Die Schwachstellenbewertung (SB, Englisch auch Vulnerability Assessment oder kurz VA) ist ein Prozess zum Identifizieren, Quantifizieren und Priorisieren Schwachstellen, die in einem untersuchten System gefunden werden. Im Schwachstellenbewertungsmodul können Sie Ihre Maschinen nach Schwachstellen scannen lassen und so überprüfen, ob die Betriebssysteme und installierten Applikationen aktuell sind und ordnungsgemäß funktionieren.

1.5.8 Software- und Hardware-Inventarisierung

Mit der Inventarisierungsfunktion können Sie alle Software- und Hardware Assets anzeigen, die auf Windows- und MacOS-Geräten mit Cyber Protect-Lizenzen verfügbar sind. Die Inventarisierung ermöglicht es:

- IT Assets der Organisation zu ermitteln
- Software- und Hardware-Inventar aller Geräte der Organisation zu durchsuchen
- die Soft- bzw. Hardwarekomponenten auf mehreren Geräten des Unternehmens vergleichen
- detaillierte Informationen über eine Soft- bzw. Hardwarekomponente anzuzeigen

1.5.9 Fernzugriff (RDP- und HTML5-Clients)

Cyber Protect ermöglicht den Remote-Zugriffe auf Maschinen. Sie können sich remote (aus der Ferne) mit Ihren Endbenutzer-Maschinen verbinden und diese verwalten. Mit dem HTML5-Client können Sie in beiden Richtungen Texte über die Zwischenablage mit der Remote-Maschine austauschen (kopieren und einfügen). Mit dem RDP-Client können Sie Texte und Dateien über die Zwischenablage austauschen (kopieren und einfügen).

1.5.10 Remote Wipe

Mit Remote Wipe (Fernlöschung) kann der Administrator oder Gerätebesitzer die Daten auf einem verwalteten Gerät löschen. So wird z.B. bei einem Diebstahl des Geräts jeder unbefugte Zugriff auf sensible Informationen verhindert.

Remote Wipe ist nur für Rechner mit Windows 10 verfügbar.

1.5.11 Monitoring

Das Dashboard enthält eine Reihe benutzerdefinierbarer Widgets, die einen komfortablen Überblick über laufende Aktionen der Cyber Protect Lösung bieten. Die Widgets werden alle fünf Minuten aktualisiert. Der aktuelle Zustand des Dashboards kann in Form einer .pdf- und/oder .xlsx-Datei heruntergeladen oder als E-Mail versendet werden.

2. Service Level Agreement

Die Service-Verfügbarkeit ist pro Service definiert und in der jeweiligen Tabelle ersichtlich. Alle in diesem Dokument beschriebenen Services werden durch Green BCS betrieben und den Green Kundendienst supportet.

2.1 Betriebs- und Supportzeiten

Die Betriebszeiten und Supportzeiten sowie die Störungsannahmezeiten sind in der folgenden Tabelle definiert.

Service Level und Zielwerte	Standard Support	Business Support (24x7)
Betriebszeit	Mo-So 00.00-24.00	Mo-So 00.00-24.00
Wartungsfenster	So 02.00-06.00 Mo 20.00-22.00 oder gemäss vorheriger Ankündigung	So 02.00-06.00 Mo 20.00-22.00 oder gemäss vorheriger Ankündigung
Supportzeit	Mo-Fr 08.00-17.30 ausgenommen an gesetzlichen Feiertagen	Mo-So 00.00-24.00
Störungsannahme	Mo-So 00.00-24.00	Mo-So 00.00-24.00

Support-Tickets können über die folgenden Kanäle eröffnet werden:

- MyGreen Portal: my.greendatacenter.ch
- Per Telefon unter +41 56 460 23 23 während den Kundensupportzeiten
- Formular auf der Webseite: https://www.green.ch/de/kontaktformular

2.2 SLA Verstösse und Gutschriftenregelungen

Kann Green die definierte Verfügbarkeit nicht einhalten, so erkennt der Kunde an und stimmt zu, dass die hier vereinbarten Gutschriften die einzige und ausschliessliche Entschädigung für den Kunden darstellen. Eine Gutschrift wird gewährt, sobald die Serviceverfügbarkeit unterhalb der garantierten Schwellwerte liegt und der Kunde dies mit einem Support-Ticket meldet. Der Ausfall eines Teils eines von einem redundanten System wird nicht als Ausfallzeit betrachtet. Nur ein korrekt eröffnetes Ticket kann für die Berechnung von Ausfallzeiten und Gutschriften herangezogen werden.

Die nachfolgende Tabelle zeigt die Gutschriften (pro Jahr) als Prozentsatz der Basis der monatlich wiederkehrenden Gebühren (MRC). Diese Gutschriften und Entschädigungen verstehen sich als abschliessend. Weitere oder andere Entschädigungen sind ausgeschlossen. Keine Gutschrift oder Zahlung erfolgt aus anderen Gründen oder in einem anderem Umfang als in dem hier angegebenen, einschliesslich – aber nicht beschränkt darauf – Geschäftsverluste auf Seiten des Kunden aufgrund von Ausfallzeiten. Die Gutschrift bezieht sich jeweils ausschliesslich auf den von der Störung betroffenem Service.

Erreichte Verfügbarkeit ohne Redundanz	Erreichte Verfügbarkeit mit Redundanz	Gutschrift
≥ 99.9%	≥ 99.5%	keine Gutschrift
≥ 99.8%	≥ 99.95%	10% des MRC
≥ 99.7%	≥ 99.9%	20% des MRC
≥ 99.5%	≥ 99.8%	30% des MRC
weniger als 99.5%	Weniger als 99.8%	40% des MRC

Der Kunde hat seine Ansprüche bei Green mittels einer Anfrage unter https://contact.green.ch/ geltend zu machen.

Es wird keine SLA-Gutschrift gewährt, wenn der Service Ausfall oder Unterbruch insgesamt oder zum Teil durch eine der folgenden Ursachen bedingt ist:

1) ein Ausfall der Ausstattung in den Räumlichkeiten des Kunden (falls diese nicht im Besitz von Green ist), des Kundenstandortes (etwa durch Stromausfall) oder der Ausstattung eines Lieferanten des Kunden
2) im Fall von Naturkatastrophen, Terrorangriffen oder anderen Force Majeure-Ereignissen
3) ein Ausfall aufgrund von magnetischen / elektromagnetischen Interferenzen oder elektrischen Feldern
4) jede fahrlässige Handlung oder Unterlassung des Kunden (oder von Mitarbeitenden, Vertretern oder Subunternehmern des Kunden), u.a.:
    a) Verzögerungen bei der Lieferung notwendiger Ausstattung durch den Kunden
    b) Versäumnis, Green zwecks Tests ausreichend Zugang zu den Einrichtungen zu gewähren
    c) Versäumnis, den Zugang zu den Räumlichkeiten des Kunden zu gewähren um es Green zu ermöglichen, ihren Verpflichtungen hinsichtlich des Services nachzukommen
    d) Versäumnis, entsprechende Gegenmassnahmen hinsichtlich des Services zu ergreifen, wie von Green empfohlen, oder Hinderung der Anbieterin, diese selbst durchzuführen
    e) Versäumnis, Redundanzen zu nutzen, wie sie vom Service Level geboten werden
    f) Fahrlässigkeit des Kunden oder absichtliches Fehlverhalten, darunter auch das Versäumnis des Kunden, vereinbarte Verfahren zu befolgen
5) wenn der Kunde den Zugang zum Cage verhindert oder verzögert
6) alle geplanten Wartungszeiträume, wenn der Kunde darüber informiert wurde, und Notfallwartungen, die dazu dienen, künftige Ausfallzeiten zu verhindern

Abschaltung oder Aussetzung des Services durch Green, nachdem der Kunde nicht innerhalb von 90 Tagen ab Rechnungsstellungsdatum bezahlt hat, oder wegen anderer hinreichender Gründe.

3. Rechtliche Bestimmungen

3.1 Zustandekommen des Rechtsverhältnisses

Mit dem Abschluss der Bestellung (bei Erhalt einer unterzeichneten Offerte) kommt zwischen Green und dem Kunden ein Rechtsverhältnis zustande. Die Messung der SLA-Parameter erfolgt ab bestätigter Serviceübergabe.

3.2 Einhaltung der örtlichen Gesetze

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

3.3 Beschränkungen

Alle Entschädigungen für Green 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.

3.4 Verwendung von persönlichen Daten

Kunden akzeptieren ausdrücklich die von Green erlassenen Richtlinien zur Verwendung persönlicher Daten. Siehe dazu: https://www.green.ch/de/rechtliches/datenschutz.

3.5 AGB

Die allgemeinen Geschäftsbedingungen der Anbieterin (Allgemeine Geschäftsbedingungen von Green https://www.green.ch/de/rechtliches/agb) 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. 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 vorhandenen 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.

4. Definitionen

Begriff	Definition
Service Level	festgelegte und messbare Kriterien für die Erbringung einer bestimmten Leistungsqualität durch Green
Service Parameter	angestrebte aber nicht verpflichtende Servicemesswerte
Betriebszeit	Die Betriebszeit ist die Zeit, in der das System grundsätzlich zur Verfügung steht. Die geplanten und angekündigten Wartungsfenster sind nicht Teil der Betriebszeit. Die Betriebszeit beträgt minimal 8‘712 Stunden und berechnet sich wie folgt: 1 Jahr 24/7 = 8‘760 h – 48 h Wartungsfenster. Bei redundanter Architektur werden die beiden redundanten Geräte/Einrichtungen zu unterschiedlichen Zeitpunkten gewartet
Supportzeit	Die Zeit in welcher der Kunde einen Kundendienstmitarbeiter oder im Fall von 24x7 Support einen Techniker im Pikettdienst erreichen kann.
Verfügbarkeit	Verfügbarkeit [%] = 100 * ((Betriebszeit - geplante Ausfälle innerhalb der Betriebszeit) / vereinbarte Betriebszeit). Die vereinbarte Betriebszeit enthält nicht die Zeitfenster für geplante Wartungsfenster. Die Verfügbarkeit wird von Green auf der Rechenzentrumsinfrastruktur gewährleistet. Dies beinhaltet folgende Ebenen: Gebäude mit Versorgungsinfrastruktur und Netzwerk. Um die hohen Verfügbarkeit auf der Verbindung zu erreichen, sind auf Endkundenseite die Lösungen ebenfalls entsprechend hochverfügbar zu designen.
Wartungsfenster	Für die Zwecke dieses SLA sind geplante Wartungen nötig, um die Services zu erbringen oder die Infrastruktur zu aktualisieren. Geplante Wartungsfenster werden im Voraus festgelegt und auf status.green.ch angekündigt, sofern mehrere Kunden betroffen sind. Kunden werden zudem mindestens 10 Arbeitstage vor dem geplanten Serviceunterbruch infolge Wartungsarbeiten informiert. Green informiert die vom Kunden schriftlich mitgeteilte technische Kontaktstelle per E-Mail über die geplante Serviceunterbrechung und die Art dieses Unterbruchs. Diese Mitteilung ist für alle von diesem Dokument verfolgten Zwecke gültig, unabhängig davon, dass es dem Kunden und/oder seinen Vertretern nicht möglich war, aus irgendeinem Grund diese Mitteilung zu erhalten, so auch aufgrund von E-Mail Systemproblemen oder -ausfällen oder fehlerhaften Kontaktinformationen des Kunden oder weiteren Gründen.
Notfall-Wartungsfenster	Notfall-Wartungsfenster werden mindestens 48 Stunden im Voraus angekündigt und auf status.green.ch aufgeschaltet, sofern mehrere Kunden davon betroffen sind.
Service Access Punkt	Der Service Access Punkt ist der vertraglich vereinbarte Punkt, an dem ein Service dem Kunden bereitgestellt und überwacht wird, und an dem die erbrachten Service Level ausgewiesen werden.