SD/SLA
Cyber Protect Cloud Cyber Protect Appliance

1. Service Description

In today's business world, data constitute vital, integral factors that are pivotal to the success of each and every business. That lends even greater importance to the security and storage of existing data. Cyber Protect is perfect for small to medium-sized enterprises. It combines highly qualified data backups with additional security options.

The Cyber Protect should be considered a holistic solution for securing your IT infrastructure.

1.1 Core functions

1.1.1 Backup and recovery

Quick, reliable backups for your applications, systems and data to facilitate quick, reliable recoveries – on every device and after every incident.

1.1.2 Security

Comprehensive next-generation malware protection, including AI-based detection of ransomware and crypto-mining attacks.

1.1.3 Cyber Protect Management

A comprehensive, high-performance solution for managing end points through a single user-friendly interface that helps you minimize your IT resources.

1.2 Editions

1.2.1 Cyber Backup

Cyber Backup contains every function you need to back up and restore your data. It does not include any protective features. The Cyber Backup edition includes these features:

- Back up and restore servers, workstations, virtual machines and network drives
- File backup and image backup
- Application backups (except Microsoft SQL and Microsoft Exchange clusters, Oracle DB and SAP HANA)
- Local storage or Acronis cloud storage (located in Switzerland) can be selected as backup destinations.
- Dashboards and reports for monitoring

1.2.2 Cyber Protect

There are three versions of Cyber Protect available that differ with respect to the scope of their security, backup and protect functions.

1.2.3 Essential

The Essential version includes limited backup functions and focuses on the security and protect aspects. It is suitable for protecting thin clients or workstations with low requirements with respect to availability and downtime.

Backup

- Back up and restore servers, workstations, virtual machines
- Only file backups
- Acronis cloud storage (located in Switzerland) is the only backup destination

Security

- Vulnerability assessment
- Patch management
- Anti-malware protection and web protection, exploit prevention, URL filtering
- Ransomware and crypto-mining protection

Protect

- Device management in groups
- Centralized plan management
- Dashboards and reports for monitoring
- HDD health monitoring (limited)
- Remote desktop and remote assistance
- Software and hardware inventory
- Script execution

1.2.4 Standard

The Standard version provides the same functions as the Essential version and supplements these with functions provided under Cyber Backup. The Standard version offers these additional functions:

Backup

- Backup and restore even network drives
- Image backup
- Application backups (except Microsoft SQL and Microsoft Exchange clusters, Oracle DB and SAP HANA)
- Local storage can also be selected as a backup destination
- Dashboards and reports for monitoring

1.2.5 Advanced

Cyber Protect Advanced includes the entire set of features. Compared to the Standard version, it offers the following additional functions:

Backup

- Advanced application backups for Microsoft SQL clusters, Microsoft Exchange clusters, Oracle DB and SAP HANA

Security

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

1.2.6 Included storage

The Essential, Standard and Advanced versions of Cyber Protect include cloud storage for each licensed device. Information regarding the amount of storage space can found on Green's website or on the price list.

The included storage is assigned to each licensed device; it is dedicated storage and cannot be used for other devices. The amount of storage included is not cumulative. Once the included storage is used up, additional cloud storage is used automatically (subject to charge). The customer is responsible for defining appropriate quotas for the purpose of cost control.

Cyber Backup does not have any cloud storage included.

1.2.7 Version upgrades/downgrades

Customers can switch between the Cyber Backup and Cyber Protect versions at any time and even make the switch themselves. Customers can only downgrade to a smaller version if they first deactivate and remove the services used.

Green does not assume responsibility for any loss of function or data that might occur as a result of mistakes made in the process.

1.3 Software licensing

1.3.1 Licensing on a per-device basis

Software is licensed for each device that is backed up. If Acronis cloud storage is used for the backup, additional fees are charged per GB (except for any cloud storage included in the license). No additional fee is charged for local backup storage or storage on the appliance.

1.3.2 Licensing on a GB basis

Licensing is calculated based on the GB of storage used per month. Local storage is invoiced at a reduced price but also on a GB basis. An unlimited number of devices can be backed up. No fees are charged on a per-device basis. Cyber Protect Cloud and Cyber Protect Appliance do not provide for any licensing purely on a GB basis.

1.3.3 Unused subscriptions

Cyber Protect is provided to customers without any basic monthly fees. Green.ch AG reserves the right to terminate any unused subscriptions. Before a step such as this is taken, however, the customer will be notified of it in advance. If the customer does not react to the information, the Cyber Protect portal will be deactivated.

A subscription is considered unused if no device licenses are triggered for a period of at least 3 months or if no storage space is used in the Cyber Protect cloud.

1.4 Storage location

Backup and security functions are always managed via the Cyber Protect cloud portal from Acronis, which is run in the data center of Green AG. Depending on which service is booked, the customer can use the following types of storage:

1.4.1 Local storage (managed by the customer)

The customer runs and manages the data backup hardware in its own network.

1.4.2 Cloud storage (managed by Acronis)

The data are stored in the Acronis cloud (data located in Switzerland).

1.4.3 Appliance (managed by Green)

All data are stored on a dedicated storage appliance.

If the storage location is not managed by Green AG or if the hardware is not located in an infrastructure offered by Green AG, this SLA cannot be applied.

1.4.4 Appliance hardware

An appliance consists of 5 nodes, regardless of the size of the storage provided. Each node is equipped as follows:

- 2 GHz, 16-core processor
- 160 GB RAM
- 5 x 240 GB SSDs (cache)
- Two 1/10 GB RJ45 ports and two 10 GB SFP+ ports

A redundant power supply is used (two power supplies). If the appliance is operated in a Green rack, a redundant connection to two independent power feeds is guaranteed.

1.4.5 Appliance storage sizes

The storage appliance is offered with different storage sizes. Three storage sizes are specified per appliance type.

1. **Raw capacity (RC)**
   Total amount of storage available (gross)
2. **CloudRAID (R1)**
   Data mirrored across 5 nodes
   (system stability = n-2)

Appliance type	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 locations

The customer can place the appliance inside the Green Datacenter infrastructure. Internet access must be guaranteed for the purpose of managing the backups and security functions. The following options are available.

Colocation / cage
The appliance is operated in a colo rack or cage belonging to the customer within a Green data center. The customer manages the infrastructure required for operating the appliance (power, cooling, network, access). The customer must grant Green access to the rack or cage for the purpose of servicing the appliance.

Cube
The appliance is installed and operated in the customer's Swisscube. Green provides the infrastructure for the Cube and therefore for the appliance as well. The features of the Swisscube must be adapted depending on its size or use. An additional switch might be needed, for example, to correctly connect the appliance to the customer's internal network.

Dedicated server rack
The perfect location for the appliance if the customer uses the appliance for backing up a virtual data center or for a dedicated server infrastructure. The infrastructure is provided by Green. The Internet connection required for appliance management is provided either through the VDC firewall or a firewall appliance in a dedicated server rack.

Shared/dedicated rack in another fire zone or data center location
If the customer already operates an IT infrastructure in one of Green's data centers, having data backups performed in another fire zone or even in another data center is advantageous.

Green sets up the infrastructure and the appliance's connection to the customer's location.

If the appliance cannot be operated in a shared rack for reasons related to data compliance, it is possible to install the appliance in a dedicated rack.

1.4.7 Requirements for the customer installation

The appliance can be operated in a colocation setup or in a customer-specific cage at Green's data center. To guarantee the operational reliability of this equipment, the following requirements apply:

Ambient conditions	
Operating temperature	0° to 40° C
Operating humidity	10% to 85%, non-condensing
Ambient air	Largely dust-free

The electrical power available at the site must meet up to the requirements of Green. Green urgently recommends the use of an uninterruptible power supply (USP; available from Green) to minimize downtime. The USP must be equipped such that the power supply to Green's equipment is guaranteed. Downtime that occurs as a result of a power outage at the customer's site is excluded from any agreement in this document.

Permanent power supply	
AC input voltage	230 V
AC input frequency	50 Hz
Max. AC input current	2A (230V)

1.5 Additional information regarding the offer

Additional information about the service (supported workloads or operating systems, prices, features) can be found at the following URL:

URL for:

Technical price/factsheet

2. Service Level Agreement

The successful outsourcing of IT services requires a transparent definition of the customer/supplier relationship. Green AG and the customer shall define the quality of the services to be provided and the obligations on the part of the customer (hereinafter "Service Level") in the subsequent Service Level Agreement ("SLA").

The SLA enables the customer to receive a defined level of quality and, should Green AG fail to provide these services, entitles the customer to a reimbursement of all or part of the monthly fees paid (hereinafter referred to as “Service credit in the event of non-availability”).

2.1 Availability

Green AG enables the availability as specified below of the services mentioned in the offer. The outage of one part of a redundant system shall not be considered downtime. If green.ch is unable to provide the aforementioned availability, the customer hereby acknowledges and agrees that the credits specified in the SLAs shall be the sole, exclusive form of compensation due.

2.1.1 Calculation of availability

Availability=
(operating time - downtime) / operating time * 100

Green AG offers credits as soon as service availability falls below the guaranteed threshold values. This document shows the credits expressed as a percentage of the basic monthly recurring charges (MRC). These credits and compensations shall be considered final. No other or additional compensation shall be granted.

2.2 General measures to ensure the security of ongoing operations

Green AG exclusively provides top-quality, highly secure services in its data centers. The security of customer data and the availability of services are ensured by these and other measures:

- Backbone lines and related equipment is set up redundantly.
- Segmentation of all networks and strict separation of the various data streams
- Network monitoring by our in-house NOC (Network Operations Center)
- Exclusive use of name-brand components
- Data center has a carrier-neutral, redundant IP connection

2.3 Financial reimbursement

If Green AG is unable to fulfill its contractually stipulated obligations, Green shall grant credits in accordance with the sections shown below. Any further claims for damages are explicitly excluded. If the customer wishes to assert any claims against Green, this must be done using the contact form provided at https://contact.green.ch.

2.3.1 Unrecoverable data

The customer is responsible for creating and managing data backups. Green AG assumes no liability for any unrecoverable data that was not created through a managed service provided by Green.

2.3.2 Exclusion of compensation for losses

In no event shall either party be liable to the other party for any special, incidental, indirect or consequential damages (including lost profits or lost data), regardless of whether such damages are based on breach of contract, tort (including negligence), product liability or otherwise, and regardless of whether or not the party was advised of the possibility of such damages.

2.3.3 Insufficient availability

Green AG offers an availability of 99.0% per calendar month.

In the event that no data backup can be created due to service unavailability, the customer may claim a refund of no more than 25% of the monthly fee.

Availability of the service is considered insufficient if the data cannot be backed up for 24 hours because the service is not available.

If a service is unavailable for a certain period of time, no SLA credit will be granted if this is attributable, either in part or in whole, to one of the following causes:

- the malfunction of equipment on the customer's premises (if not owned by Green AG), at the customer's location (e.g. due to a power failure) or equipment belonging to one of the customer's suppliers
- natural catastrophes, terrorist attacks or other force majeure events
- an outage due to magnetic/electromagnetic interference or electrical fields
- any negligent act or failure to act on the part of the customer (or on the part of the customer's staff, representatives or subcontractors), including:
    - delays in the customer's delivery of necessary equipment
    - failure to grant Green access to the installations for testing purposes or to perform repairs
    - failure to grant access to the customer's facilities to enable green to fulfill its service obligations
    - failure to take appropriate countermeasures regarding the faulty services, as recommended by green, or the prevention of green from taking such measures itself or
    - failure to use redundancies as offered by the service level
    - negligence on the part of the customer or willful misconduct, including the customer's failure to follow agreed procedures
- if the customer prevents or delays access to the cage or data
- non-availability due to scheduled maintenance (if the customer has been given prior notice) and emergency maintenance to prevent future downtime or
- deactivation or discontinuation of the service by Green AG if the customer has not paid within 45 days of the date of the bill, or other for other good cause

3. Service management

3.1 Support

Support for all of our services is provided through standard channels:

- Online support: via the ticketing system at https://contact.green.ch
- Live chat: www.green.ch
- The Green AG website: http://www.green.ch/support
- As a customer of Green AG, you can obtain telephone support by calling +41 56 460 23 23 during our office hours of 8 a.m. - 5:30 p.m., Monday - Friday (except prior to and on public holidays).
- Customers with 24/7 coverage should also contact this same number during our office hours.

3.1.1 Extended support

Unless already included in the service contract, the 24/7 Service Desk is available as an additional service subject to charge and can only be contacted outside office hours.

3.2 Incident management

3.2.1 Reporting an outage

Green will AG inform the customer's technical contact either by phone or e-mail (in the case of a written notification, this will be sent to the contact details provided to green.ch).

3.2.2 Incident management procedure

Green AG's philosophy is that customers should receive the very best level of availability and service quality possible, both technically and operationally. Should failures arise, our main objective is to handle the incident swiftly and restore service availability. This approach benefits our customers by limiting the incident's impact on their business activities. Customers must report all incidents and outages affecting "reactively" managed services. Once the outage has been reported, a trouble ticket is opened and analyzed. Services is then restored in accordance with the agreed service level. Incidents and outages affecting "proactively" managed services will be reported by the monitoring system. Once appropriate steps are taken, the customer will be notified accordingly subject to the agreed service level. If the outage affects the customer's business activities, the customer must open a trouble ticket via the appropriate channels.

3.3 Obligations of the Support organization

- Ask for and verify the credentials of the person submitting the request and compare these with the Service Level Agreement in place between the customer and the provider.
- Trigger the incident management process which comprises the following:
  - Receive the request, open a trouble ticket and provide confirmation
  - Prioritize, coordinate and monitor the troubleshooting process with the help of internal and external tools
  - Notify the customer about the steps taken, interim solutions and the solution
  - Notify the customer that service availability has been restored
  - Analyze the underlying cause and recommend the next steps (change management)

In the case of unexpected delays in troubleshooting efforts that lead to a violation of the SLA, the matter is automatically escalated internally. Depending on the type of problem, the first escalation level will be either senior members of our internal staff or sales/subcontractor support. The manager on duty will be called in at this point to ensure compliance with the SLA during the escalation process and that the problem is resolved in a timely manner.

3.3.1 Obligations of the Customer

- The customer shall provide all necessary contact details, including contacts for escalation, for all services provided and shall ensure that they are updated on an ongoing basis in the event of changes.
- The customer shall provide green with a list of all individuals entitled to access support services and keep this list up to date.
- The customer shall implement suitable means of identifying these authorized individuals and keep these updated.

- The customer shall ensure that information related to changes made to the configuration, interfaces, channels, applications and systems of relevance for the purpose of providing joint services are delivered to the provider and kept up to date.
- The customer is responsible for the continuous maintenance of all customer applications. The maintenance of customer applications or customer data is the sole responsibility of the customer.
- Only equipment that is in perfect condition and poses no danger to persons or property may be installed.
- The customer must ensure that green can access equipment managed by green at all times and for any reason. Failure to do so constitutes a breach of the agreement and may result in termination of the contract.
- All activities carried out in cooperation with green.ch employees must be coordinated in advance. This also applies to supplementary service options such as additional accounts or network changes.
- All unauthorized attempts by a customer to access equipment belonging to green.ch, whether physically or electronically, is strictly prohibited. This also applies to CPE (customer premises equipment).

3.4 Amendment procedures

Amendments to the customer agreement will be made in writing unless otherwise agreed. Amendments not documented in writing are invalid. Unless otherwise agreed, the costs incurred in connection with contract management shall be borne by each contracting party itself.

The contracting parties will examine proposals regarding amendments and notify the requesting party in writing of their approval or any amendments desired, as a rule within two weeks following the submission of the proposed amendment. The requested party usually either approves or rejects this or the alternative amendment proposal within another two weeks following submission of the revised amendment proposal.

If one party rejects an amendment proposal for good reason or the other party either does not approve the proposed amendment or fails to do so before the deadline, the agreed scopes of service as well as the terms and conditions shall remain unamended.

4. Other provisions

4.1 Object of the contract, scope of application

This SLA only applies to the offer sent together with the SLA and the service contract concluded on this basis. It shall not affect any other contracts in place between green.ch and the customer. The SLA can only be applied to the Cyber Security solution and its options, but not to other product ranges. If any of these provisions contradict other provisions of this agreement, the agreements in the corresponding service contract take precedence over the provisions of the SLA. The currently valid version of the General Terms and Conditions of Green AG shall also apply.

4.2 Establishment of the legal relationship

A legal relationship is established between Green AG and the customer as soon as the online order placement process has been completed or by way of a quote. Measurement of the SLA parameters begins when the customer successfully logs in to the portal for the first time.

This document constitutes an integral annex to the contract for all orders placed with Green AG, whether online or on the basis of a quote issued.

4.3 Compliance with local legislation

The customer must ensure that no illegal data traffic is sent via Green AG connections. Green AG assumes no liability for this.

4.4 Restrictions

Compensation for Green AG's services is limited to the compensation amounts specified in this document. No credit or payment will be made for reasons or of an amount other than those specified here including, but not limited to, any lost business suffered by the customer as a result of downtimes.

4.5 Use of personal data

Customers expressly accept the guidelines issued by Green governing the use of personal data.

For more information, please refer to: http://www.Green/de-ch/übergreench/agb/datenschutz.aspx

4.6 Amendments

Green AG reserves the right to amend this document occasionally, provided that the customer is informed accordingly in writing before the amendments take effect. If the changes have a material effect on the services, the service fee or other obligations under this contract, the customer may terminate this contract in writing at any time subject to the monthly notice period.

4.7 Insurance

While Green AG systems are insured against appropriate risks, neither the customer data nor the availability of the services provided by the customer to its own customer base are insured. It is the express responsibility of the customer to obtain insurance coverage. No compensation will be granted for the loss of business information or for the impact of any other system failures in excess of the credits explicitly described in this document.

4.8 Termination of services

In the event that a service is terminated, the customer must return all equipment furnished by Green AG for the provision of the service, without being asked to do so and in proper condition, to Green AG within 30 days of the end of the contract. The customer is responsible for all fees and costs associated with the return of this equipment. As an alternative, the customer can also request that the provider send a technician to pick up the equipment (subject to charge), send it by mail or choose another option, where applicable. The customer is liable for bearing the cost of any replacement hardware in the following cases:

If the equipment is lost or not returned within 30 calendar days following the end of the contract.

If the condition of the equipment is such that the provider can no longer use the hardware for another client; this does not include wear and tear over time.

4.9 GTC

The General Terms and Conditions of the provider (General Terms and Conditions of Green AG) form an integral part of the customer agreement. The general terms and conditions of the customer shall not apply. Any provisions to the contrary contained in the customer's documents are not applicable. Cancellations, amendments and supplements to the service agreement and the service contracts must be made in writing. The written form requirement can only be waived in writing. Should individual provisions of this service

agreement or the service contracts or other appendices to the customer agreement prove to be legally invalid or unenforceable, the invalid or unenforceable provision shall be replaced by a valid or enforceable provision that comes closest to the desired effect of the contracting parties at the time the respective provision was agreed and corresponds to the common objectives set out in the preamble to this service agreement. The new provision may not result in any impairment of the relationship between the provider's services and the customer.

GTC of Green Datacenter