Service Level Agreement v3.3

Combell managed hosting

COMBELL nv • Skaldenstraat 121 • B-9042 Ghent • Tel: +32(0)9 218 79 79 • Fax: +32(0)9 270 30 60
www.combell.com • info@combell.com • KBC: 737-0036586-60 • IBAN BE73 7370 0365 8660 • BIC KREDBEBB
VAT: BE 0541.977.701 • Combell is ISO 9001:2000 certified and Microsoft Gold Certified Partner

Table of Content

1 Infrastructure

1.1 Data centres

Combell has several spaces available in different data centres in the Benelux. All these data centres are equipped with: UPS (Uninterruptible Power Supply), air conditioning, fire detection, temperature control and other environmental /security systems. Combell's own network infrastructure is redundant, which in practice means that Combell has installed all systems in duplicate, or even better. So, if one system goes down, another one takes over.

1.2 Power supply

Combell ensures an uninterrupted power supply to the systems located in the data centre. Combell is however not responsible for interruptions caused by (i) equipment or applications that belong to third parties, (ii) actions and neglect by the Customer or third parties, or (iii) force majeure.

Each server is fed by two power circuits (A + B), creating a redundant power supply for the Customer's server(s). Therefore, in the event that one of the power circuits goes down, the servers remain powered by the other one. Moreover, each circuit is connected to a separate electrical power network, each equipped with UPSs (uninterruptible power supplies) and backup battery power. In addition to these redundant power circuits with their backup devices, generators are in place to provide continuous electrical power in the event of prolonged power failures. All backup power supply facilities are being regularly tested by a specialised maintenance team that is thus familiar with the entire procedure, to allow for decisive action to be taken when necessary.

1.3 Security and access control

Advanced security systems monitor the entire data centre 24x7. A closed circuit television system (CCTV) records and archives all activities. Each person accessing the data centre must provide valid identification and is registered when entering and leaving the premises.

1.4 Fire and smoke detection

The data centres are all equipped with smoke and fire detection / repression systems. Throughout each data centre, several detectors and gas dispersion systems are in place. As soon as smoke is detected at two different locations, the alarm will sound and gas is dispersed. This gas will lower the percentage of oxygen in the air to extinguish the fire. It is forbidden to leave flammable material in the data centre. The data centres and Combell will perform regular checks and reserve the right to remove any flammable material (or have it removed) at the Customer's expense.

The data centre has passed stringent fire control audits.

1.5 Active climate control

The air is being cooled through redundant, high-end climate control systems throughout the data centre. Efficient cooling is accomplished by means of the "hot/cold aisle containment" principle, separating warm and cold air are mixed to the least extent possible.

1.6 Network infrastructure

Combell's entire network infrastructure has been designed by certified engineers. Routing is fully redundant and Combell manages its network fully independently.

1.7 Network connectivity

Combell uses several providers for its network connectivity. The backbone networks of those providers are fully redundant; all their nodes are connected to at least two other nodes through separate circuits. This results in a network that will withstand malfunctions.

2 Service Level Packages

With each virtual, dedicated, or cloud server, Combell provides the standard service level ("Basic") as described below. When placing the initial order as well as over the term of the contract, the Customer may purchase a higher Service Level Package at the then-current rates.

In the table below, you will find an overview of the services included with each Service Level Package. The paragraphs following it will provide a more detailed description of each of these services.

The included support minutes apply per SLA sold. *For any minutes used between 22:00 and 09:00 (10:00 PM and 09:00 AM), Combell will charge the double hourly fee.*

SLA	Start	Basic	Plus	Pro	Premium
Basic support	Included 24/7	Included 24/7	Included 24/7	Included 24/7	As agreed
System Support	Not included	30 min Week days 9 AM – 5 PM	60 min Every day 9 AM – 10 PM	120 min Every day 24/24	As agreed
Advanced Support	Optional	Optional	Optional	Optional	As agreed
Recovery waiting time for business critical incidents	Reasonable Effort	Next Business Day	4 h – 3 h (*) – 2 h (**)	2 h – 1.5 h (*) – 1 h (**) – 0.5 h (***)	As agreed
Recovery waiting time for non business critical incidents	Reasonable Effort	5 Business Days	3 Business Days	2 Business Days	As agreed
Communication waiting time for business critical incidents	Reasonable Effort	Next Business Day	4 h – 3 h (*) – 2 h (**)	4 h – 3 h (*) – 2 h (**)	As agreed
Communication waiting time for non business critical incidents	Reasonable Effort	5 Business Days	3 Business Days	Next Business Day	As agreed
Basic Monitoring	Not available	Included, office hours	Included	Included	As agreed
Advanced Monitoring	Optional	Optional, office hours	Optional	Included	As agreed

Performance Monitoring	Optional	Optional	Optional	Included	As agreed
Basic Backup	5 GB	10 GB	25 GB	50 GB	As agreed
Advanced Backup	Not available	Optional	Optional	Optional	As agreed
Firewall	Basic	Advanced	Advanced	Advanced	As agreed
Remote reboot	Optional	Included	Included	Included	As agreed
SSL VPN	Optional	Optional	Optional	2 users	As agreed
Patch Management	Basic	Basic	Basic	Advanced	As agreed
Direct access to Operations	Not available	Not available	Not available	Included	As agreed

(*) If the server is part of a virtualisation platform, under the conditions stated below:

- all data is stored on a shared medium, e.g. a SAN (Storage Area Network),
- each physical machine must have sufficient memory to run the virtual servers of any other node at any given time,
- the platform is composed of at least 2 physical servers.

(**) If the server/service is part of a cluster or farm in which services are automatically taken over by an alternative server/service in the event of a failure. Examples include database clusters, web farms, and firewall clusters, the failover mechanism being managed by Combell.

(***) If the server/service is part of an environment in which services, in the event of a failure, are automatically taken over by an alternative server/service located at another data centre.

2.1 Supported operating systems

The following operating systems are supported as long as the respective suppliers continue to provide OS support and provided that the OS has been installed by Combell:

- Microsoft Windows Server (Standard and Datacenter Editions),
- Debian,
- Redhat (Enterprise Server).

Operating systems past end of life are no longer supported by Combell and the corresponding service levels and compensations are voided.

2.2 Basic Support

Basic Support includes all basic questions related to software and services installed by Combell.

This encompasses the following support requests:

- questions pertaining to domain names, DNS settings, e-mail, and FTP,
- questions related to the use of the customer's control panel,
- help with the publication of a website,
- rebooting a server.

2.3 System Support

System Support includes all activities performed by Combell not included with Basic Support.

This encompasses the following support requests:

- Installation/configuration of specific patches, upgrades, hotfixes, and add-ons on existing software or modules installed by Combell, [1]
- solving malfunctions not caused by Combell that negatively affect the services procured (e.g. a web server, mail server, or database server not responding),
- setting up network equipment (switches, VPN, …) at a Combell data centre,
- performing security audits,
- recovering a backup (data or disaster recovery backup),
- upgrading virtual hardware.

Combell will process any System Support requests not related to incidents that need to be solved urgently, in accordance with the communication waiting time and recovery waiting time for non-business-critical incidents as per the Service Level Package chosen by the Customer.

The hours included with the Service Level Package chosen by the Customer can only be used for services and applications that were installed and configured by Combell and are valid per calendar month. Thus, these cannot be transferred to the next month nor can these be used for installing new components. Man-hours for the latter type of actions will resort under Advanced Support as described in article 2.4. The availability of System Support depends on the Service Level package chosen.

Any support beyond the above-mentioned will resort under Advanced Support.

[1] The term 'patches' does not include distribution updates; this latter category by default resorts under Advanced Support.

2.4 Advanced Support

Advanced Support includes all activities performed by Combell that are not included with Basic Support and System Support. Depending on the SLA Package chosen, a number of hours is included. When exceeding these hours, the then-current rates for Advanced Support will apply.

Advanced Support encompasses, among others, the following support requests:

- Installation or configuration of new software or modules,
- Upgrades of physical hardware,
- Development of any kind of script (e.g. monitor scripts),
- Performing migrations,
- …

Resolving any malfunction in the Services procured is always free of charge, does not resort under System Support nor Advanced Support, with the following exceptions:

- The malfunction is the result of a resource shortage (e.g. when reaching excessively high visitor counts),
- Problems stemming from less-than-optimal code, database queries, or database layouts,
- Any issue related to software that was not installed and configured by Combell,
- Actions or omissions by the customer that adversely affect service delivery.

Advanced Support is a paid service component, this regardless of the Service Level Package chosen by the Customer. To Advanced Support the hourly rates as stated in the Agreement will apply, with the following multipliers:

- Then-current rate for working days (9 AM – 10 PM) 100%
- Then-current rate for working days (10 PM – 9 AM) 200%
- Then-current rate for Saturdays, Sundays and holidays 200%

Advanced Support is always provided according to the Reasonable Effort principle and is subject to the availability of the engineers in charge of these tasks. The widely varying nature of activities means that Combell can't provide guarantees on the communication, restore, and execution time frames. All activities need to be planned in advance.

2.5 Incidents

2.5.1 Business-critical incidents

With business-critical incidents, Combell refers to failures affecting the data centre infrastructure, Combell's network, hardware, and server services purchased (e.g. a web server, mail server or database server not responding) that lead to a demonstrable unavailability of the service purchased by the Customer.

2.5.2 Non-business-critical incidents

With non-business-critical incidents, Combell refers to failures occurring in the data centre infrastructure, Combell's network, hardware, and server services purchased by the Customer that leave the service still available to the Customer. This includes, among other things, all configuration changes.

2.5.3 Recovery Waiting Time

The Recovery Waiting Time is the time frame during which Combell solves or suggests a work-around for the incident. Any time necessary to restore a backup does not count towards Recovery Waiting Time, since this depends on the volume of data to be restored. Within the recovery waiting time, Combell will restore the OS and will initiate the recovery process of any other data, but logically can't provide a hard guarantee as to the duration of the total recovery time.

2.5.4 Communication Waiting Time

The Communication Waiting Time is the time frame during which Combell sends the Customer feedback regarding the incident. Within this waiting time, Combell will notify the Customer about a possible solution or a work-around for the incident.

This period concerns only the communication with the Customer and not the incident or its resolving. Refer to the table in article 2 for more information on the availability of Combell's support per Service Level Package.

2.5.5 Reasonable Effort

Reasonable Effort means that Combell does its best to solve the reported incidents as fast as possible and to promptly send out a communication, yet without providing any guarantees as to the corresponding communication or recovery waiting time.

2.6 Monitoring

2.6.1 Basic Monitoring

Under Basic Monitoring the server is connected to the monitoring infrastructure.

When exceeding a given value or if a business-critical service is not accessible, an SMS message and an e-mail are sent to an on-duty system manager.

Only applications (e.g. web server) installed by Combell will be included in the monitoring system. If the incident reoccurs, a Combell system manager will get in touch with the Customer. If the incident is caused by an application belonging to the Customer, the monitoring will be temporarily deactivated and the Customer will be requested to solve the incident as soon as possible. A maximum of eight checks per server can be carried out per Basic Monitoring package.

Basic Monitoring is activated by Combell upon it receiving the hand-over document (Customer-to-Combell) signed by the Customer.

2.6.2 Advanced Monitoring

Advanced Monitoring includes all options of Basic Monitoring. With Advanced Monitoring, the Customer can add two of its representatives to our monitoring system. These persons will then also be notified by SMS and/or e-mail if one or several services fail. SMS messages can only be delivered in Belgium and the Netherlands.

The addition of mobile numbers in our monitoring system must be requested by the Customer. With Advanced Monitoring, Combell performs checks with shorter intervals than it does under Basic Monitoring.

Upon request, other services can also be monitored (such as a Windows service, an application running on another port, CPU load, the response time of SQL Server, …). Depending on the type of service or application that should be monitored, a one-time development fee may be charged for the development of a personalised script. This is done in consultation with the Customer and falls under Advanced Support. A maximum of fifteen checks per server are included per Advanced Monitoring package.

2.6.3 List of monitor checks (if applicable)

Monitor check	Description	interval (minutes)	
		Basic	*Advanced*
Custom			
DISK	Check free space and inodes on remote system through NRPE	30	10
LOAD	Check load on remote system through NRPE	10	10
MEMUSED	Check used memory on remote system through NRPE	5	5
NTPTIME	Compare time on remote system to an NTP server through NRPE	240	60
RESOLVE	Check if target's DNS config works	60	30
SWAP	Check free swap space on remote system through NRPE	5	5
Webserver			
APPOOL	Check all IIS application pools	5	5
HTTP-IP	Monitor an IP-based HTTP service	5	2
HTTP-HOST	Monitor a name-based HTTP service	5	2
HTTP-Content	Monitor a name-based HTTP service	5	2
HTTPS	Monitor a name-based HTTPS service	5	2
Linux			
SSH	Monitor SSH service	5	5
OPEN	Check percentage of allocated file-handles	60	60
ROMOUNT	Check for read-only mounted file systems through NRPE	30	10
Windows			
RDP	Monitor RDP service (check_x224)	5	5
NTFSHEALTH	Inspect system logs for signs of NTFS corruption	30	10
Database servers			
MySQL	Check mysql query (first field of first row)	10	5
MySQLBackup	Check if automysqlbackup ran OK	60	60
MSSQL	Check mssql create/insert/select/drop functionality	5	2
MSSQLINST	Check MS SQL instances	5	2
SQLBackup	Receive passive SQL backup check results initiated from this host	30	30

2.6.4 Performance Monitoring

The Customer can check the evolution of its resources per server by means of comprehensive performance statistics. The statistics offer a daily, weekly, monthly and yearly overview in the form of graphics available on an online web page. The Customer shall expressly order the activation of Performance Monitoring.

Depending on the applications installed on the Customer's server, the Customer may log disk space usage, usage of physical and virtual memory, CPU usage (per CPU), the number of active processes, IIS data (attempts, connections, requests) and network statistics. Any development costs related to this shall resort under Advanced Support.

2.7 Backup

2.7.1 Basic Backup

Combell makes available an on-site backup space on a central storage environment, according to the volume chosen (e.g. 5 GB, 10 GB, 25 GB, 50 GB…). The Customer itself is responsible for making and restoring backups. This backup space is accessible using FTP and only through Combell's network.

2.7.2 Advanced Backup

Unlike with a Basic Backup, with an Advanced Backup, making and restoring backups is entirely taken care of by Combell. Combell uses specialised software to make a daily backup of the Customer's server. All files (including those of the operating system, of additional installed software and those holding configurations such as write permissions) are saved onto the chosen backup storage system. This depends on the type of backup that is chosen in the contract. The backup schedule is determined and managed by Combell. Backups of the Customer's server are performed each day during night-time unless contractually agreed otherwise.

Since a backup of the Customer's system is made daily, this backup cannot – under normal circumstances – be older than 24 hours. The most the Customer can lose is therefore 24 hours' worth of data.

If the backup of the Customer's server failed, Combell system managers will be notified about this by e-mail in the morning. In such an exceptional case, the backup of the Customer can be at maximum 48 hours old.

The recovery time of the entire system is strongly dependent upon the amount of data and number of files to be restored. Using differential backups, Combell aims to consistently minimise this time frame.

2.7.3 Tape-Based

If tape-based backup is chosen, the Customer automatically benefits from a 60 day retention period.

The daily backup is guaranteed to be stored for 14 days, after which the weekly backup is stored for 60 days. Combell is responsible for maintaining sufficient capacity to be able to make a backup during these days, which is also part of the backup service. The volume of data to be backed up is equal to the regular storage volume.

2.7.4 Disk-Based

If disk-based backup is chosen, Combell suggests a standard 14-day backup plan. The Customer may however deviate from this if it requires such.

In order to be able to guarantee at least one backup, a minimum of 110% of the regular storage space must be made available as backup space.

In principle, 100% extra backup storage must be made available for each daily guaranteed backup version. This applies only in the unlikely case that 100% of the data would daily change. In practice, we observe an average data change ratio of 10% per day. That is why Combell suggests to make space available for 1 weekly full backup (100% of the regular available space) and 6 incremental backups (6 x 10% changes of the space made available daily). After one week, this amounts to 160%.

Although the Customer can determine the frequency and the retention period of its backups itself, Combell advises the Customer to provide backup means for a 2-week period, meaning that 320% of the regular storage space will be required as backup space. This is the only way Combell can guarantee the Customer a retention period of 2 weeks.

2.8 Firewall

2.8.1 Basic Firewall

With the Basic Firewall option, the firewall is simulated on the Customer's server (software firewall). During the initial setup, Combell determines the configuration of this software firewall (Linux web server/database server or Windows web server/database server…). Traffic through the following ports is allowed: POP3 (110), SMTP (25), HTTP (80), FTP (21), Remote Desktop (3389), Plesk (8843), MySQL (3306) and MS SQL (1433). By default, not all ports are opened up. At the Customer's request via e-mail, traffic via some of the abovementioned ports can be authorised.

The Customer is free to have changes made in the configuration without extra cost, provided it can explain why he wants these ports to be open. Combell always reserves the right to refuse certain changes.

2.8.2 Advanced Firewall

Advanced Firewalling applies when servers are connected to Combell's redundant Firewall Infrastructure (hardware firewall cluster). During the initial setup, the configuration of the firewalls is determined. Traffic via the following ports is admissible: POP3 (110), SMTP (25), HTTP (80), FTP (21), Remote Desktop (3389), Plesk (8443), MySQL (3306) and MS SQL (1433). By default, not all ports are opened. Upon the Customer's request via e-mail, traffic via some of the abovementioned ports can be authorised.

The Customer is free to have changes made in the configuration without extra cost, provided that he can explain why he wants these ports to be open. Combell always reserves the right to refuse certain changes. For this, the Customer shall contact Combell. A maximum of fifty firewall rules (objects) can be set per server.

2.9 Remote reboot

With the Remote Reboot function, it is possible to perform a remote "cold reboot" of the Customer's server. This means that the power to the server is interrupted during a few seconds so that the server can reboot. To have a remote reboot performed, the Customer must send its request to support@combell.com in order for Combell to perform a remote reboot

If the remote reboot option is not included in the Service Level package chosen by the Customer, a "remote reboot" will be charged at the then-current rates for Advanced Support.

2.10 SSL VPN

SSL VPN offers a secure tunnel over Internet between the Customer's computer and the server by means of Combell's specific web interface. The Customer receives a user name and a password that may be linked to a specific IP address. As a result the management ports to the Customer's server are accessible only through the SSL VPN gateway.

2.11 Patch Management

2.11.1 Basic Patch Management

In order to increase the security of the Customer's server, Combell will update Windows servers using a central system. The update server performs the security updates of the Customer's Windows operating system. As soon as Microsoft launches updates, this system (WSUS) will download critical updates and subsequently distribute these to the Customer's server. With Linux servers, critical updates are collected directly from the distributor.

Depending on the schedule that Combell defines, updates will be performed at specific points in time. Combell always arranges for updates to be performed at night. Critical updates are installed within the week unless indicated differently by the customer (see Advanced Patch Management). Other updates are all installed within the week. Service packs are always tested in

Combell's test environment prior to their distribution to the server farm. Upon request, the Customer can be notified when updates occur. Other software (such as SQL Server or a mail server) installed by Combell is also updated by Combell. Among other things, installation of security patches and service packs is included by default with every server.

Software updates and upgrades to newer versions. Such upgrades can be performed at the Customer's request and will be charged for at the then-current Advanced Support rates.

2.11.2 Advanced Patch Management

All updates mentioned above under Basic Patch Management are planned and executed in agreement with the Customer. The Customer will indicate which individuals should be contacted in the event of an update.

These individuals are notified at least 48 hours before performing the update and can, if necessary, postpone the update by agreeing to a new installation time with Combell.

The activation of Advanced Patch Management must be expressly requested by the Customer.

2.12 Direct access to Operations

This option gives the Customer the privilege to directly contact Combell's Operations service in the context of all kinds of incidents. Upon delivery the Customer will receive specific contact information directly contact these individuals.

The Customer's server infrastructure is fully described in a personal technical file by Combell's system managers and is followed closely by the Operations service.

3 Availability

3.1 Measuring method

To measure availability, Combell uses the following formula:

Availability = (maximum availability – downtime) / maximum availability x 100%

Maximum availability = period (in minutes) during which the services could have been available at their maximum. This equals 60 minutes x 24 hours x the number of days in the month.

Downtime = period (in minutes) during which the services were not available, not including downtime due to maintenance or changes.

3.2 Availability of data centre and network

All Combell data centres have been outfitted to aim for continuous service delivery. The complete equipment of each data centre to deliver this uptime is described in article 1.1.

- Network availability >= 99,97%
- Power availability >= 99,98%
- Availability of air conditioning >= 99,98%
- Availability of fire detection >= 99,98%
- Air humidity (RH) 35 – 65%
- Temperature 18 – 26°C

Combell ensures that the average latency on its own network shall never exceed 90 ms for its European part and 200 ms for its trans-Atlantic part.

Combell ensures that the average packet loss on Combell's network shall remain under 1.5 % per month. Combell reserves the right to, if necessary, perform emergency maintenance on the network infrastructure if the service delivery is jeopardised.

3.3 Hardware availability

Combell repairs or replaces free of charge all faulty hardware that is topic of the Agreement. Incidents relating to hardware that cause downtime are considered business-critical incidents and are solved accordingly. Combell consistently maintains a supply of spare systems and components to perform the repair as soon as possible.

The Customer itself cannot make changes to its server. Servers are located in a highly secure environment, to which only Combell's representatives have access. Upon request, it is possible for the Customer to visit its server and the local data centre infrastructure.

3.4 Bandwidth availability

Combell ensures that the average bandwidth usage, measured over a 1-week period, shall not exceed 45% of the total available bandwidth in order to guarantee optimal availability and throughput, this including during peak loads.

3.5 Support availability

Our support services can be reached by calling the toll-free numbers 0800 8 5678 (from Belgium) or +31 20 716 88 88 (from the Netherlands) and by sending an e-mail to support@combell.com.

Customers may contact Support as per the following table.

Weekdays:	from 8:00 AM to 12:00 PM
Saturdays:	from 9:00 AM to 12:00 PM
Sundays:	from 10:00 AM to 12:00 PM

Beyond these hours, calls will be answered by our call centre service yet if desired, it will transfer the caller immediately to an on-duty Combell engineer.

4 Installation and delivery

4.1 Delivery of the server(s)

When choosing a custom server (i.e. adapting memory, CPU, etc.), delivery will take at least 10 working days from the date of the order. In this case, Combell is also not responsible for any delays caused by the hardware supplier.

4.2 Software installation

Upon delivery, Combell will install the operating system. Combell can install additional software at the Customer's request, at the then-current rates for Advanced Support.

Software management following delivery (e.g. user creation, new folders, assignment of rights, …) is for the Customer to perform itself unless contractually agreed to the contrary.

After the delivery, the Customer must manage the software himself (e.g. creating users or folders, setting permissions, etc.), unless stated otherwise in the contract. The Customer can also call upon Combell's Advanced Support for such tasks.

5 Abuse of systems

5.1 Access to the systems

Combell reserves the right to examine the Customer's system at any time without prior consent. Such will occur only for checks, maintenance, and patch installation. In this respect Combell takes the necessary technical precautions and will always treat the Customer's server confidentially in accordance with the then-applicable legislation and regulation.

5.2 Abuse

If Combell receives a message reporting possible abuse committed with the Customer's server, Combell maintains the right to immediately block off the server if strong indications exist that the message is founded. Examples of abuse are: sending unsolicited e-mail (spam), or using the Customer's hardware to attack other servers.

In the event that the Customer's server has been hacked, Combell will analyse the log files. If the analysis reveals that the server has been hacked due to an application error (e.g. SQL injection), this will resort under Advanced Support. Combell will delete all infected files or scripts to the extent possible and, if necessary, will advise a system reinstallation.

If network attacks target the Customer's server, Combell reserves the right to, in exceptional cases, temporarily block the Destination IP address to ensure network stability.

Upon identification of abuse, the Customer's liaison will be contacted.

6 Compensation

If the service levels are not met as agreed, the Customer is entitled to claim compensation. This compensation consists of a one-time rebate, to be discounted from the invoice for monthly fees of the services that Combell delivers in relation to the affected system. 'Affected system' refers to the system to which the defect applies, and thus bears no relation to the total monthly sum invoiced.

The liability for, and the compensation paid by, Combell in relation to whichever service level - including those regarding availability and restore times – will under all circumstances remain limited, per claim of range of claims following from the same feat or cause, to the sum of recurring fees (i.e. not including any one-off charges) that relate to the affected system and that have been invoiced to and paid by the Customer over the 3-month period preceding the incident to which the claim applies.

The compensations below are the only compensations that the Customer is entitled to claim if Combell fails to meet the agreed upon service levels. Moreover, these compensations may not be accumulated if these result from the same feat or cause.

6.1 In relation to business-critical incidents

Compensation flowing from the failure to comply with the communication and/or recovery waiting time in case of business-critical incidents

Hours exceeding the target	% rebate
0 – 3 hours	25%
3 – 4 hours	50%
4 – 6 hours	75%
More than 6 hours	100%

Hours exceeding the target will be considered as per article 2 of this document.

6.2 In relation to non-business-critical incidents

Compensation flowing from the failure to comply with the communication and/or recovery waiting time in case of non-business-critical incidents

Days exceeding the target	% rebate
0 – 1 day	25%
1 – 2 days	50%
2 – 3 days	75%
More than 3 days	100%

Days exceeding the target will be considered as per article 2 of this document.

6.3 In case of unavailability of the purchased service

Exceeded % availability of the data centre	% rebate
1 %	25%
2 %	50%
3 %	75%
More than 3 %	100%

The % exceeding the target will be considered as per article 3.2 of this document.

6.4 Version of this document

Combell reserves the right to unilaterally change this agreement to respond to the rapidly evolving technological evolution in which the context of this agreement is set. Changes take effect one month after notice and will be announced in the monthly newsletter. The latest version of this document is always available on the website http://www.combell.com/sla

6.5 Submission of claims

All claims pertaining to the service levels offered by Combell must be duly motivated and sent within a period of fifteen (15) days after the occurrence of the failure, per registered letter, to the following address: Skaldenstraat 121, B-9042 Gent, Belgium.

6.6 Translated document

The content of this document was written in Dutch. If any dispute arises from nuances of meaning resulting from the translation process, the Dutch version will prevail.