INTERCONNECT

SERVICE LEVEL AGREEMENT

Version: 4.6.0
Date: 01-12-2021

TABLE OF CONTENTS

DISCLAIMER

Please note: This is a translation of a Dutch document. Errors and omissions excepted. Legal basis for the contractual relationship is the Dutch original document.

1 ABBREVIATIONS & DEFINITIONS

Capitalized terms used in this Service Level Agreement (SLA) shall have, unless otherwise explicitly specified in the context of this SLA, the following meaning. In this SLA names of services are also capitalized. These are not included in the overview below.

Agreement	The Agreement including appendices between Interconnect and Customer that constitutes the basis for a Service provided by Interconnect.
Authorization List	List of contacts who are authorized by the Customer to access the datacenters of Interconnect, request Smart Hands, request administrative and/or technical changes and/or manage contacts.
Availability	Percentage of total time, measured over a full calendar year, in which the Service is available to the users, excluding Maintenance and Emergency Maintenance. The following formula is used to calculate the Availability: **Availability** = (**U**-**D**) / **U** * 100%, where **U** = total of service hours within the measured period, excluding Maintenance and Emergency Maintenance; **D** = Downtime. Total number of hours the Service was not available as a result of an Outage.
CST	Customer Service Team (Service desk) of Interconnect.
Customer	The legal entity with whom Interconnect has entered into an Agreement (contracting party).
DC1	Interconnect Datacenter in 's-Hertogenbosch.
DC2	Interconnect Datacenter in Eindhoven.
Demarcation Point	The demarcation points of the Service, wherein the guarantees described in this SLA apply.
Downtime	The timeframe, measured and registered by Interconnect, between the Incident Report and the closing of the Incident as reported by Interconnect to the Customer, or the time the Service is available again.
Emergency Maintenance	Performing maintenance to the Infrastructure to correct unforeseen circumstances that are an immediate threat to the continuity and/or security of the Service and/or other Services.
Incident Report	Formal report from an authorized contact of the Customer (by phone/email) or the monitoring system of Interconnect to the CST stating the Service is not working properly.

Infrastructure	The technical infrastructure of Interconnect providing the Service. Including, if applicable, support services of suppliers.
Interconnect	InterConnect Services B.V. registered at the Chamber of Commerce under number 50100572.
Maintenance	Performing maintenance to the Infrastructure with the aim of maintaining the quality of the Interconnect Service or to implement changes to the Service or the Infrastructure.
MyInterconnect	The online customer portal of Interconnect (www.myinterconnect.nl) where the Customer can request information, make changes and submit requests with regard to the Service(s).
Office Hours	Periods in which Interconnect can be reached by phone, as stated on the website of Interconnect. Dutch public holidays and days on which Interconnect has announced to be closed, are not considered Office Hours.
Office Hours CST	Periods in which CST can be reached by phone, as stated in chapter 4.1. Dutch public holidays and days on which Interconnect has announced to be closed, are not considered Office Hours CST.
Outage	There is an Outage if the Service, within the Demarcation Points, is unavailable, unless an exclusion is valid as stated in this SLA.
Resolution Time	See "Downtime".
Response Time	The timeframe between an Incident Report and the moment incident handling starts (registration, first Customer contact and diagnosis start).
Service	The specific Service that Interconnect agrees with the Customer, as stated in the Agreement.
SLA	Service Level Agreement. This document.

2 GENERAL

This Service Level Agreement is an agreement between Interconnect and the Customer, wherein the qualitative and quantitative agreements concerning the delivery and support of the Service(s) are set out.

2.1 SCOPE

This SLA only applies to one or more Service(s), as listed in *Appendix A*, that the Customer purchases based on a written Agreement and to which this SLA is declared to be applicable.

The SLA is valid from the moment Interconnect has confirmed in writing to the Customer that the Service has been delivered.

2.2 CHANGES TO SLA

Interconnect is authorized to make changes to this SLA as deemed necessary. The Customer shall be informed of all amendments at least 30 days before the amendments come into effect.

2.3 TERMS AND EXCLUSIONS

1. The SLA explicitly does not apply to:

    a) other Services by Interconnect that the Customer purchases and on which no SLA is agreed.
    b) hardware repairs on the equipment of the Customer, unless explicitly otherwise agreed.

2. There is no Outage if the Service was unavailable due to:

    a) circumstances that can be attributed to the Customer, including a failure in Customer equipment and software (installed on request of or by the Customer). If it is feasible that a reported Outage is caused by such circumstances, then the Out of Office Hours Service Charge of €275,- per started hour per engineer is applicable.
    b) Maintenance and Emergency Maintenance (see 4.3 – 'Change Management').
    c) a situation where a single component, from a redundant purchased Service or option on a Service, cannot meet the required capacity (e.g. a B power feed where the circuit breaker is tripping because the A feed is down).
    d) causes that Interconnect cannot reasonably influence (including force majeure). This also includes the situation in which the consequences of an incident could have been minimized through the use of another Service or option on a Service, but the Customer did not purchase it at the time of the start of the incident. E.g. a DDOS attack where the option Anti-DDOS has not been purchased.
    e) suspension based on the Agreement.

3. "False" Outages caused by unannounced system administration by, because of or on behalf of the Customer, will be invoiced and can lead to cancellation of this SLA. Therefore maintenance that affects the operation of the Interconnect monitoring system must be communicated forehanded to the CST.

4. The management option "Managed" can only be supplied if Interconnect has an administrative account on the Service. The Customer must ensure that such a login is maintained. The Customer indemnifies Interconnect against any liability that may result from the use of the login, unless this consequence is demonstrably attributable to Interconnect.

5. The SLA on Managed Firewall only applies if the firewall is placed in a datacenter of Interconnect.

6. All measurements performed by Interconnect as a result of this SLA serve as compelling evidence between the parties. Measurements by Interconnect will therefore always prevail.

3 SERVICE DELIVERY AND SERVICE LEVELS

3.1 INTERCONNECT

Interconnect has its own datacenters in 's-Hertogenbosch and Eindhoven. The facilities in the datacenters are fully committed to ensure the reliability of the Services. An extensive overview of the specifications and facilities of the datacenters are included in the relevant product information.

3.2 AVAILABILITY

3.2.1 General

A Service can be available or in Outage. There is an Outage if the Service, within the Demarcation Points, is unavailable. An incident is, in terms of this SLA, not an Outage if there are one or more situations applicable as described in section 2.3 paragraph 2.

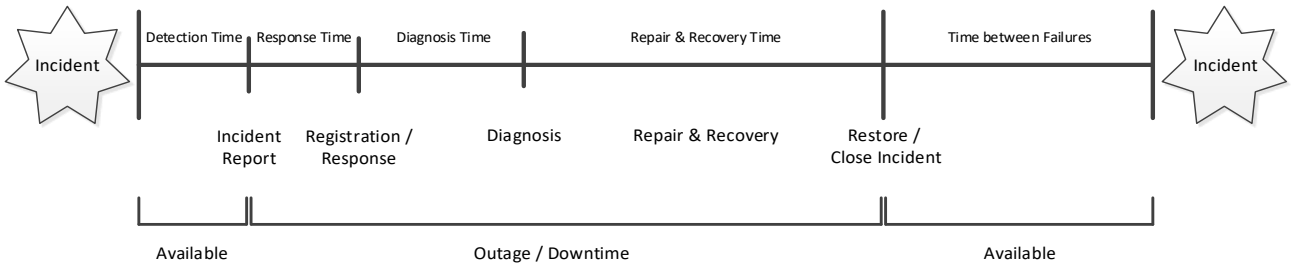

Figure 1. Schematic overview Availability vs. Downtime

For hosting and datacenter Services (see *Appendix A*) Availability also means the Service is accessible (reachable) for the Customer. This guarantee is valid within the enclosed part of the IPv4 / IPv6 network under the direct management of Interconnect, with the exception of Connectivity Services.

In situations where the Availability of Service A depends on Service B, the starting point for the calculation of the Availability of Service A is that Service B was always available.

When calculating the Availability of a Service that was delivered or terminated in the same calendar year, the Service is considered to be available before delivery and/or after termination.

SLA types

Interconnect offers different SLA types concerning the Availability of the Service. The Availability of the Service applies within the Demarcation Points, being the platform that Interconnect deploys to deliver the Service.

SLA type	Availability
Bronze	99 %
Silver	99.6 %
Gold	99.9 %
Platinum	99.95 %

Appendix A states which SLA type is included as standard with a Service and/or can be purchased optionally. The following paragraphs describe different/additional guarantees, Demarcation Points, and preconditions where applicable.

3.2.2 MyInterconnect

The Availability of MyInterconnect (see *Appendix A*) is an operational objective and does not fall under the compensation scheme (see 5 – 'Compensation scheme').

3.2.3 Datacenters Interconnect

Colocation

For colocation Services delivered from the datacenters of Interconnect, the following service levels apply:

Colocation	DC 1 – 's-Hertogenbosch	DC 2 – Eindhoven
IP connectivity	99.9 % (up to and including patch point on patch bay in rack)	99.9 % (up to and including patch point on patch bay in rack)
Power	99.9 % (up to and including busbar)	99.9 % (up to and including tap-off box)

The following values are operational objectives that do not fall under the compensation scheme.

Colocation	DC 1 – 's-Hertogenbosch	DC 2 – Eindhoven
Temperature	99.0 % (16°C-25°C)	99.9 % (18°C-25°C)
Humidity	99.9 % (20%-80%)	99.9 % (20%-80%)

Preconditions / principles

- Failure of a non-redundant network connection qualifies as a class 1 incident (Outage, see 4.2.2 – 'Priority').
- Failure of a non-redundant power feed in DC 1 ('s-Hertogenbosch) qualifies as a class 1 incident (Outage). Failure of a non-redundant power feed in DC 2 (Eindhoven) qualifies as a class 2 incident.
- Failure of both components of a redundant power feed (A+B), Multiple Switch Connect or Multiple Datacenter Connect, qualifies as a class 1 incident (Outage). Failure of a single component qualifies as a class 2 incident.
- The 'temperature' performance concerns the percentage of the total number of temperature measurements that fall within the bandwidth stated in the table above. In DC 1, the exhaust air from the CRAC (cooling) unit is measured. This can differ per unit and depends on the conditions of the return air (to the cooling units). In DC 2 the supply air in the cold corridor is measured.

Private Space

For the Private Space Service, the Platinum SLA type applies if the Customer purchases each power feed redundantly (A+B) and provides each network connection with a Multiple Switch Connect or Multiple Datacenter Connect.

3.2.4 Connectivity

This SLA guarantees the Availability of the connection from the broadband aggregator in the core network of Interconnect up to and including the DSLAM in the local exchange (DSL) or the NTU at the customer location (fiber optic). See the figures below in which these Demarcation Points are shown.

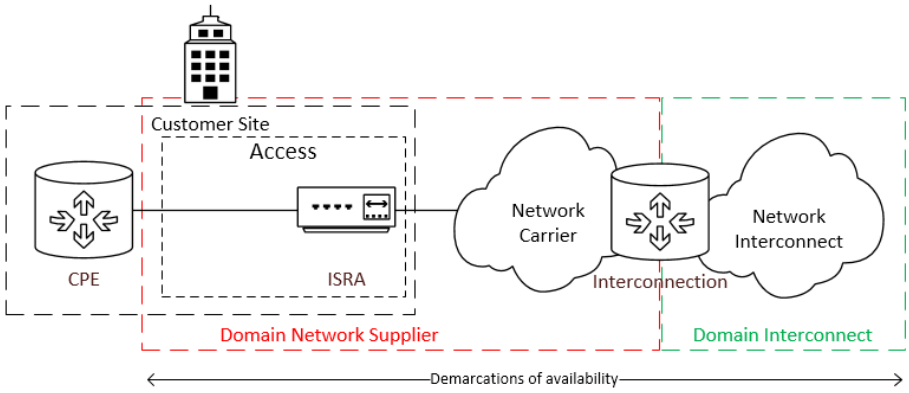

Figure 2. Availability AoDSL / EoDSL

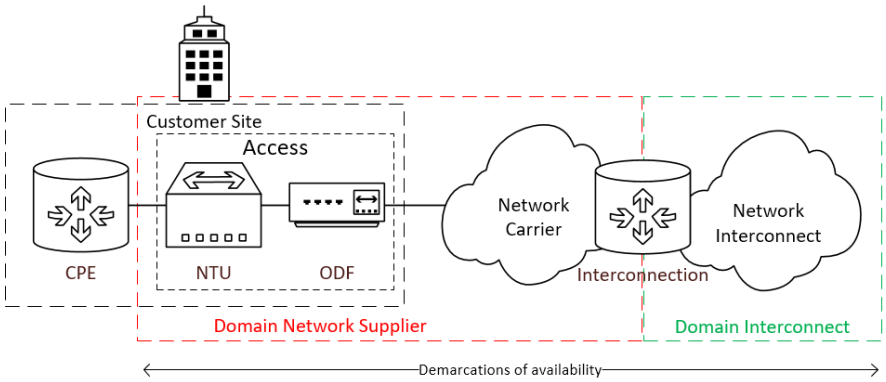

Figure 3. Availability optical fiber

An incident is an Outage if no data transport is possible on the connection and therefore all PVCs / VLANs do not function. This Service involves reactive incident management. The Downtime starts when the Incident Report of the Customer is received by the CST. The Outage is considered to be solved as soon as data transport on the connection is possible again.

Preconditions / principles

- An SLA Gold or Platinum is only possible in combination with a CPE or NTU from and managed by Interconnect. With optical fiber, also access must be purchased from Interconnect.
- An SLA Platinum is only possible with a redundant connection (DSL/DSL based on two different network providers, DSL/optical fiber, optical fiber/optical fiber or a combination of DSL or optical fiber with a radio connection). If one connection is unavailable, it qualifies as a class 2 incident. If both connections are unavailable, it qualifies as a class 1 incident (Outage).

Optical fiber (Dark Fiber)

The 'Dark Fiber' Service (unlit fiber optic connection between two locations) involves reactive incident management. The Downtime starts when the Incident Report from the Customer is received by the CST. The Outage is considered to be solved, as soon as the physical optical fibers are functioning again. An incident is an Outage if one or more physical optical fibers are not functioning.

Preconditions / principles

- Necessary reconstruction of the route and/or renovation of the fiber optic connections are outside the scope of this SLA.
- When an Incident Report regarding an Outage is received, the emergency response team of the contractor will be on-site within 2.5 hours, after the receipt of the report, to begin locating the fiber problem. Once the root-cause is located, repair of the physical optical fiber(s) will be started immediately.
- The contractor shall ensure that the fibers of the broken connection are repaired within a maximum of 12 business hours (the first fibers within 4 hours after arrival and the remaining fibers on average within 8 hours after arrival). Repair of damages in trenchless installations, directional drills, artworks and other situations in which the activities take longer due to force majeure, are not included in the above-mentioned recovery times.

If the above-mentioned recovery times cannot be met due to force majeure, the contractor is obliged to do everything in its power to solve the Outage as soon as possible.

Public Cloud Connect

The SLA on this Service only applies in the event of an Outage on one of the components within the Demarcation Points, shown in the figure below.

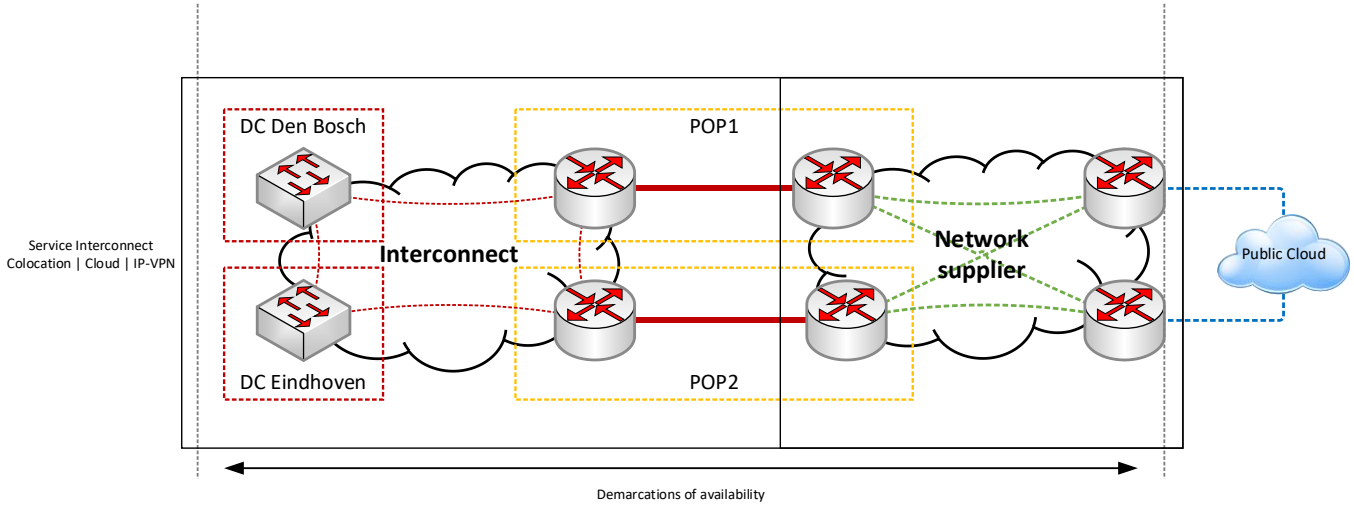

Figure 4. Availability Public Cloud Connect

3.2.5 Cloud

With the Cloud Services, Interconnect guarantees the Availability of the platform that is used to provide the Service. The Service is considered to be available when the platform is available.

Preconditions / principles

- For a multi-site configuration, failure of both sites (locations) qualifies as a class 1 incident (Outage). Failure of one site qualifies as a class 2 incident.

  Non-availability of the Service during the restart time of the VMware HA (High Availability) mechanism does not count as Downtime.

3.2.6 Security

Managed Firewall

For a redundant firewall configuration, an SLA Gold or SLA Platinum applies, depending on the type. This is specified in *Appendix A*.

Preconditions / principles

- Failure of both components of a redundant firewall qualifies as a class 1 incident (Outage).
- Failure of a single component of a redundant firewall qualifies as a class 2 incident.

3.2.7 Options

Options with their own availability guarantee are listed separately in *Appendix A*. The compensation scheme (see 5 – 'Compensation Scheme') applies to the offered availability guarantee of the relevant option if this availability is not achieved.

3.3 BACKUP

Interconnect endeavors to make a daily backup of all Services, if possible, to speed up the recovery during calamities. If digital storage space is a part of the Service and backup of this Service is possible, the Customer data that is stored on the Service will be included in this backup.

Interconnect does not guarantee the availability of backups made by Interconnect. The Customer is responsible for performing and storing backups of its own data.

3.4 PROCEDURES

Interconnect values information security highly and is ISO 27001 certified. The scope of this certification applies to the entire organization.

Interconnect's information security policy is aimed at ensuring the reliability of information systems and minimizing possible damage resulting from security incidents. Interconnect is committed to the objective of continuously measuring and improving information security.

3.4.1 Authorization of contacts

Interconnect follows a strict procedure to prevent individuals, who are not authorized by the Customer, from obtaining sensitive or Customer related information when they contact Interconnect, from implementing changes to the Service and/or gaining access to the datacenter. A contact can have the following permissions:

- Manage contacts
- Datacenter access
- Smart Hands
- Technical changes
- Administrative changes

The Authorization List saved by Interconnect is decisive when determining the authorizations of a contact. The Customer is responsible for the correctness and (periodical) checking of this list. The customer can self-manage contacts and their authorizations via MyInterconnect or request these changes in writing or by e-mail to Interconnect. Changes made on MyInterconnect are active immediately. Changes to the Authorization List requested in writing or by e-mail are only processed during Office Hours.

3.4.2 Access procedure

The datacenters of Interconnect are accessible 24x7. Visitors must be authorized at Interconnect to access the data center. Guests are only allowed access accompanied by an authorized contact.

A visit to the datacenter must be announced by telephone at least 30 minutes in advance by a contact from the Authorization List of the Customer.

Announce datacenter visit
Phone number: + 3173-8800012 / + 3173-8999912 (backup)

All visitors of the datacenter must identify themselves upon arrival with a valid ID to the receptionist or Datacenter Host on duty.

Please note: a copy of an ID or a similar document will not be accepted and access will not be granted on this basis.

All visitors of the datacenters of Interconnect must always comply to the rules as described in "House Rules Datacenters Interconnect".

3.4.3 Reporting and handling of information security incidents

If a significant (information) security incident is detected with (possible) impact on the Service, Interconnect will immediately (without undue delay) report this to the Customer. This also applies when there is a security breach of personal data (data leak) which has or may have adverse consequences for the data subject(s).

If the Customer detects an (information) security incident or security vulnerability, related to the Infrastructure of Interconnect, we request the Customer to report this to the Customer Service Team (see 4.1 – 'Customer Service Team').

4 SERVICE SUPPORT

4.1 CUSTOMER SERVICE TEAM

The Customer Service Team (CST) is the primary technical point of contact for the Customer. It takes care of the acceptance, registration, classification and handling of incidents, service requests and change requests.

Contact details and Office Hours CST

CST:	+3173-8800011
Interconnect Emergency Service (Out of Office Hours Service) (24/7):	+ 3173-8800012 / + 3173-8999912 (backup)
Email:	service@interconnect.nl
Monday - Thursday	08.00 - 19.00
Friday	08.00 - 17.30

4.2 INCIDENT MANAGEMENT

Incidents that occur after delivery of the Service are the responsibility of the CST.

4.2.1 Proactive and reactive

Incident management is carried out in one of the following two ways, depending on the Service (see *Appendix A* – 'Overview Services Interconnect'):

1. Proactive incident management
2. Reactive incident management

Proactive incident management

The Infrastructure of Interconnect is actively monitored by the Interconnect monitoring system. Every 5 minutes measurements are taken on the critical components of the Service, to check on various aspects like Availability and capacity.

Incidents are automatically reported by the system and handled by the CST. All Incident Reports of an Outage will be picked up immediately, both within and outside Office Hours CST.

The Customer will be notified if there is an Outage on the Service.

Reactive incident management

The reactive incident management process is triggered when an Incident Report of the Customer is received by the CST. The CST will register, classify and handle this Incident Report. An Outage can be reported both within and outside Office Hours CST.

4.2.2 Incident Report

Incidents that are detected by the monitoring system of Interconnect are automatically reported to the CST.
Incidents that are detected by the Customer must be reported by email and/or phone to the CST stating the affected Service, description of the incident and the starting time of the incident. In the case of an Outage, the Incident Report must be made by phone.

Outside of Office Hours CST the Interconnect Emergency Service (Out of Office Hours Service) phone number must be used to report an Outage.

Incidents, including Outages, which are detected by the Customer, can only be reported by contacts on the Authorization List of the Customer.

Note:

- The Interconnect Emergency Service (Out of Office Hours Service) phone number is only intended for reporting an Outage of the Service (explicitly not for regular service requests), announcing a datacenter visit (see 3.4.2 – 'Access procedure') or requesting Smart Hands, performed by personnel from Interconnect.
- The Interconnect Emergency Service (Out of Office Hours Service) phone number is only intended for reporting Outages on a Service to which a valid SLA applies. Explicitly not for reporting Outages on a Service to which no SLA applies.
- If the two here above-mentioned conditions are not met or if an Outage is reported outside of Office Hours CST that is not attributable to Interconnect or its suppliers, the Out of Office Hours Service Charge will apply (see 2.3 – 'Terms and Exclusions').

Priority

Each Incident Report is prioritized by the CST as follows:

Priority	Description
Class 1 (high)	The Service is unavailable. Outage.
Class 2 (medium)	The Service can only be used with limited functionality.
Class 3 (low)	The Service shows an inconvenient shortcoming.

The priority can be changed during the Downtime by the CST.

4.2.3 Incident handling

The CST endeavors to process and handle all Incident Reports as soon as possible.
The maximum incident Response Time depends on the priority class as shown in the table below.

Response Time

Priority	Response Time
Class 1 (high)	Directly after Incident Report (<15 minutes).
Class 2 (medium)	Within 4 hours of Incident Report, during Office Hours CST.
Class 3 (low)	At the latest the next business day.

From the moment an Outage is handled, there will be continuous work on the repair and recovery of the Service, unless this does not reasonably shorten the Downtime.

During the Downtime the Customer will be informed about the progress of the repair and recover work. The Customer must cooperate with Interconnect in resolving an Outage, without any cost.

Immediately after an Outage has been resolved, Interconnect will report this to the Customer. On request, Interconnect will provide the Customer with an RFO (Reason for Outage) within 3 working days at the latest.

4.2.4 Escalation

The CST uses functional and hierarchical escalation procedures to minimalize Downtime and give incidents proper attention.

4.3 CHANGE MANAGEMENT

Interconnect may perform Maintenance or Emergency Maintenance to the Service.

4.3.1 Planned Maintenance

If planned Maintenance has (possibly) a significant or major impact on the Service, Interconnect will announce this Maintenance at least 5 working days in advance. The announcement consists of:

- the start time and expected end time of the work;
- the nature of the work;
- the expected non-availability;
- Service(s) affected.

If the Customer wants to object to the planned date/time, then the Customer must report this to the CST within 24 hours after receiving the announcement. Interconnect will take the objection into consideration, but reserves the right to still carry out the work on the planned date and time.

Note: Maintenance will be announced by the Technews mailing list. Upon first request, Customer contacts will be subscribed to this mailing list.

In case of Maintenance with (possible) minor impact on the Service, Interconnect may choose not to announce this, deviate from the announcement period and/or notify the Customer in a different manner.

4.3.2 Emergency Maintenance

In case of Emergency Maintenance, the above-mentioned notice period may be deviated from.

4.3.3 Maintenance window

Maintenance will be performed within the maintenance window as much as possible. This also applies to Emergency Maintenance. If required by the situation, (Emergency) Maintenance can be expedited.

(Possible) impact to the service	Maintenance window
Minor	Monday - Sunday 20.00u – 01.00u (CET)
Significant / major	Monday - Sunday 00.00u – 06.00u (CET)

Note: Maintenance on the datacenter facilities Infrastructure equipment (e.g. power, cooling) will typically be performed during Office Hours.

4.3.4 Change freeze

During the beginning and end of a calendar year, no scheduled Maintenance will be performed on the Service (change freeze). If necessary, Emergency Maintenance will be performed during this period. The exact start and end dates of the change freeze are determined per year.

4.3.5 Black Building Test

Interconnect intends to conduct a Black Building Test (BBT) in the last quarter of each year. The purpose of this test is to test the reliability of the emergency power supplies. During the BBT, the grid power will be switched off entirely on the side of (and by) the grid operator (A- and B-feed). Interconnect's emergency power supplies then take over the power supply to the datacenter.

The BBT is conducted in a controlled and well-prepared situation with all relevant suppliers present.

Interconnect reserves the right to change the schedule of the BBT at any time.

4.4 REPORTING

Interconnect provides the Customer with an online Datacenter Portal where the power usage and data traffic can be viewed of the relevant Services. Login details for this portal are provided with the delivery of the Service.

Interconnect Datacenter Portal
https://dcportal.interconnect.nl

5 COMPENSATION SCHEME

Interconnect has a compensation scheme, as described below, that applies when the service levels guaranteed in this SLA are not met.

5.1 SCOPE

The compensation scheme applies if the Customer, within 3 months after the end of the calendar year, appeals for compensation and makes it plausible that the agreed Availability of the Service was not achieved.

5.2 CREDIT

For each commenced hour that the Service has been unavailable for longer than permitted, in the preceding calendar year, a credit will be issued in accordance with the pro rate cost for one day of the monthly fee. The monthly fee is the subscription fee in one calendar month, excluding additional costs based on subsequent calculation, such as costs for exceeding the maximum permitted data traffic.

The maximum credit amount provided based on this SLA shall never exceed the amount the Customer would have paid Interconnect per month for the Service affected by the Outage, in the event that no credit had been applied.

For bundled Services, which consist of components that are also offered as individual Services by Interconnect, the compensation and the maximum amount of this compensation is based on the relevant part that has not achieved the guaranteed Availability. Example: if with the Private Space Service 1 of 4 rackspaces was unavailable for longer than permitted, the compensation will be calculated based on the monthly amount of the concerning rackspace.

For the Services Rackspace, Private Space and Private Datacenter, a compensation and the maximum amount of this compensation, if the guaranteed Availability of IP connectivity is not achieved, is based on the rackspace(s) in which the relevant network connection has been delivered.

5.2.1 Example

Situation

- A Private Space with 2 rackspaces. Total amount per month: € 1.700,-.
- Customer has an Agreement starting October 1.
- On November 20, 1 rackspace was unavailable for 14 hours, due to failure of both power feeds.
- Based on the applicable Availability percentage of 99.95% on an annual basis (SLA Platinum), the rack space may not be available for a maximum of 4 hours and 23 minutes (4.38 hours) per calendar year.

Calculation of compensation

- Exceeding of maximum agreed Downtime in calendar year: 9.62 hours.
- Rounding up due to crediting per commenced hour (see 5.2) makes 10 hours.
- Pro rate cost 1 rackspace: € 770,-.
- Pro rate cost for a day: 770 / (average number of days in a month per year = 30) = 25.67 euro.
- Compensation over calendar year: 10x25.67 = € **256.70**.

APPENDIX A – OVERVIEW SERVICES INTERCONNECT

Service	Availability				Incident Management
	Bronze	Silver	Gold	Platinum	
General	99 %	99.6 %	99.9 %	99.95 %	
Online Customer portals					
MyInterconnect	●	-	-	-	Proactive
DCPortal	●	-	-	-	Proactive
vCenter	-	-	-	-	Proactive
VMware Cloud Director	●	-	-	-	Proactive
Rancher	●	-	-	-	Proactive
Cloud					
Virtual Private Server (VPS)					
VPS Linux / VPS Windows	-	-	●	-	Proactive
VPS	-	-	●	-	Proactive
Virtual Private Cloud (VPC)					
VPC Single Site	-	-	●	-	Proactive
VPC Multi Site	-	-	-	●	Proactive
Virtual Datacenter					
Virtual Datacenter Single Site	-	-	●	-	Proactive
Virtual Datacenter Multi Site	-	-	-	●	Proactive
Kubernetes Cluster					
Kubernetes Cluster Single Site	-	-	●	-	Proactive
Kubernetes Cluster Multi Site	-	-	-	●	Proactive
Security					
Managed Firewall					
SRX-300	-	●	○	-	Proactive
Redundant SRX-300	-	●	○	-	Proactive
SRX-320	-	-	●	-	Proactive
Redundant SRX-320	-	-	-	●	Proactive
SRX-340	-	-	●	-	Proactive
Redundant SRX-340	-	-	-	●	Proactive
Shared	-	-	●	-	Proactive
Anti-DDOS					
Anti-DDOS proactive	-	-	-	-	Proactive
Anti-DDOS reactive	-	-	-	-	Reactive
Hosting					
Webhosting and e-mail					
“Domeinregistratie” (Plus)	-	-	-	-	
Shared Webhosting					
Standard	-	-	-	-	
Premium	-	-	-	-	
Datacenter	-	-	●	-	Proactive

Service	Availability				Incident Management
	Bronze	Silver	Gold	Platinum	
Connectivity	99 %	99.6 %	99.9 %	99.95 %	
Business DSL					
ADSL	-	○	○	○	Reactive
VDSL	-	○	○	○	Reactive
SDSL	-	○	○	○	Reactive
SDSL.bis	-	-	●	○	Reactive
Optical fiber					
Eurofiber	-	-	●	○	Reactive
KPN (WEAS)	-	-	●	○	Reactive
Tele2	-	-	●	○	Reactive
Ziggo (WEA)	-	-	●	○	Reactive
"Glasvezel Interconnect" (Optical fiber Interconnect)	-	-	●	○	Reactive
"Glasvezel Interconnect" (Optical fiber Interconnect) dark fiber	-	-	-	-	Reactive
Radio					
Tele2 Radio	-	-	●	○	Reactive
Public Cloud Connect					
Public Cloud Connect	-	-	●	-	Proactive
Datacenter					
DC 1 ('s-Hertogenbosch)					
Colocated Server	-	-	●	-	Proactive
Rackspace	-	-	●	-	Proactive
Private Space	-	-	●	○	Proactive
Private Datacenter	-	-	●	-	Proactive
DC 2 (Eindhoven)					
Colocated Server	-	-	●	-	Proactive
Rackspace	-	-	●	-	Proactive
Private Space	-	-	●	○	Proactive
Private Datacenter	-	-	●	-	Proactive
Options					
Managed Storage					
Back-up Storage	-	-	●	-	Proactive

- = Availability guarantee not possible.
○ = Availability guarantee optional.
● = Availability guarantee included as standard.