INTERCONNECT

SERVICE LEVEL AGREEMENT

Version: 5.2.0
Date: 01-03-2025

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, or one of Interconnect's partners.
Customer	The legal entity with whom Interconnect has entered into an Agreement (contracting party).
DC2	Interconnect Datacenter in Eindhoven., Park Forum 1041.
DC3	Interconnect Datacenter in 's-Hertogenbosch, Het Sterrenbeeld 55.
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 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	Interconnects customer portals where the Customer can view information, make changes and submit requests with regard to the Service(s).
Namespace	An environment where resources are isolated and organised within a cluster.
Office Hours	Periods in which Interconnect can be reached by phone, as stated on the website of Interconnect. Dutch official public holidays (with the exception of Good Friday en Liberation Day) and days on which Interconnect has announced to be closed, are not considered Office Hours.
CST Office Hours	Periods in which CST can be reached by phone, as stated in chapter 4.1. Dutch official public holidays (with the exception of Good Friday en Liberation Day) and days on which Interconnect has announced to be closed, are not considered Office Hours.
Outage	Unavailability of a Service within the Demarcation Points with the exception of an exclusion as stated in this SLA.
Response Time	The time between an Incident Report and the moment incident handling starts (registration, first Customer contact and diagnosis start).
Service	The specific Service as agreed by Interconnect with the Customer, as stated in the Agreement.
Support Charge	The rate charged for troubleshooting outages beyond Interconnect's responsibility.
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*, purchased by the Customer based on a written Agreement and to which this SLA is declared applicable.

The SLA is effective from the moment Interconnect confirms the Customer delivery of the Service in writing,

2.2 CHANGES TO THIS SLA

Interconnect is authorized to make changes to this SLA as necessary. The Customer is 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 provided by Interconnect purchased by the Customer where no SLA is agreed.
   b) hardware repairs to customer equipment , unless explicitly otherwise agreed.

2. There is no Outage if the Service was unavailable due to:
   a) Conditions that can be attributed to the Customer, including a failure in Customer's equipment and software installed on request of or by the Customer. In case a reported Outage is caused by such conditions, the Out of Office Hours Service Charge per started hour per engineer is applicable, plus additional startingrate. (see Appendix B – Interconnect Rate Overview).
   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, through no fault of Interconnect cannot meet the required capacity (e.g. B power feed where the circuit breaker is tripping because A feed is down).
   d) causes outside Interconnects reasonable 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 done 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 in advance to CST.

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

5. The SLA on Managed Firewall only applies if the firewall is installed and located in one of Interconnect's Datacenters.

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

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 equipped 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.

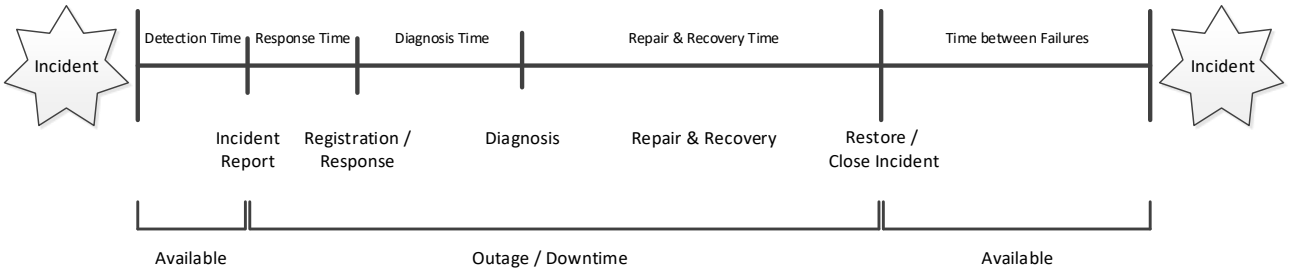

Figure 1. Schematic overview Availability vs. Downtime

For Colocation 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 managed by 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 during a calendar year, the Service is considered to be available before delivery and/or after termination.

SLA types

Interconnect offers different SLA types covering the Availability of the Service. The Availability of the Service applies within the Demarcation Points, consisting of the platform deployed by Interconnect in order to provide the Service.

SLA type	Availability
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 sections describe different/additional guarantees, Demarcation Points, and preconditions.

3.2.2 Portals Interconnect

The Availability of the Interconnect Portals(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 Interconnect's datacenters the following service levels apply:

Colocation	DC2 – Eindhoven	DC3 – 's-Hertogenbosch
IP connectivity	99.9 % (up to and including patch point in rack)	99.9 % (up to and including patch point in rack)
Power	99.9 % (up to and including tap-off box)	99.9 % (up to and including tap-off box)

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

Colocation	DC2 – Eindhoven	DC3 – 's-Hertogenbosch
Temperature	99.9 % (24°C-32°C)	99.9 % (24°C-32°C)
Humidity	99.9 % (20%-80%)	99.9 % (20%-80%)

Preconditions/principles DC2

- A failure of a non-redundant network connection in DC2 qualifies as class 1 incident (Outage, see 4.2.2 – 'Priority').
- In case of failure of both components of a Switchport redundancy configuration – single site, a Switchport redundancy configuration - dual site, a Multiple Switch Connect or a Multiple Datacenter Connect in DC2, qualifies as a class 1 incident (Outage). Failure of a single component qualifies as a class 2 incident.
- Failure of a non-redundant power feed in DC2 is a class 2 incident. Failure of both components of a redundant power feed (A+B) qualifies as a class 1 incident (Outage).
- The 'temperature' performance concerns the average temperature of the total number of temperature measurements that fall within the bandwidth stated in the table above. In DC2 the supply air in the cold corridor is measured.

Preconditions/principles DC3

- An incident in DC3 is a class 1 incident (Outage) if no data transport is possible on a single switchport or two redundant switchports (Outage, see 4.2.2 – 'Priority').
- Failure of a non-redundant power feed DC3 is a class 2 incident. Failure of both components of a redundant power feed (A+B) qualifies as a class 1 incident (Outage).
- The 'temperature' performance concerns the average temperature of the total number of temperature measurements that fall within the bandwidth stated in the table above. In DC3 the supply air in the cold corridor is measured.
- The Demarcation Point of a peering/transit-location is the patch point in the rack.

Private Space

The SLA type Platinum applies to the Private Space Service if the Customer purchases redundant power feeds (A+B) and provides each network connection with a Multiple Switch Connect or Multiple Datacenter Connect.

Datacenter Connectivity

The Datacenter Connectivity Service is subject to the Platinum SLA type when the connection is purchased redundantly.

3.2.4 Connectivity

This SLA guarantees the Availability of the connection from the broadband aggregator in the Interconnect core-network up to and including the DSLAM at the local exchange (DSL) or the NTU at the customer location (fiber optic). For Demarcation Points see figures 2 and 3 below.

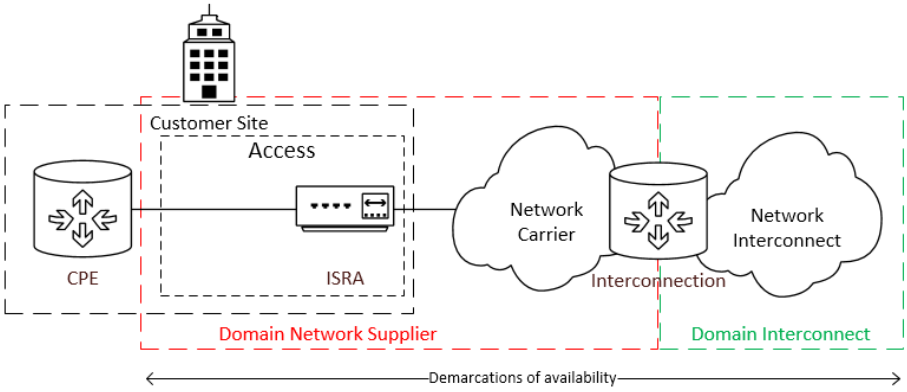

Figure 2. Availability xDSL

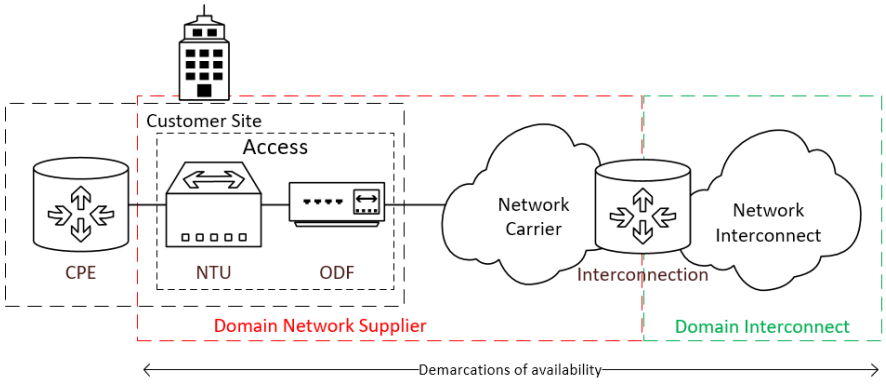

Figure 3. Availability optical fiber

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 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 provided and managed by Interconnect. With optical fiber, also access must be purchased from Interconnect.

- An SLA Platinum is only possible with a redundant connection (optical fiber/optical fiber or optical fiber/xDSL). If one connection is unavailable, it qualifies as class 2 incident. If both connections are unavailable, it qualifies as 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 at the moment the Incident Report from the Customer is received by CST. The Outage is considered resolved, 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 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 as a result of jacking, directional drilling, damage to artworks or other situations where, due to force majeure, the work takes longer, are not included in the above mentioned repair 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.

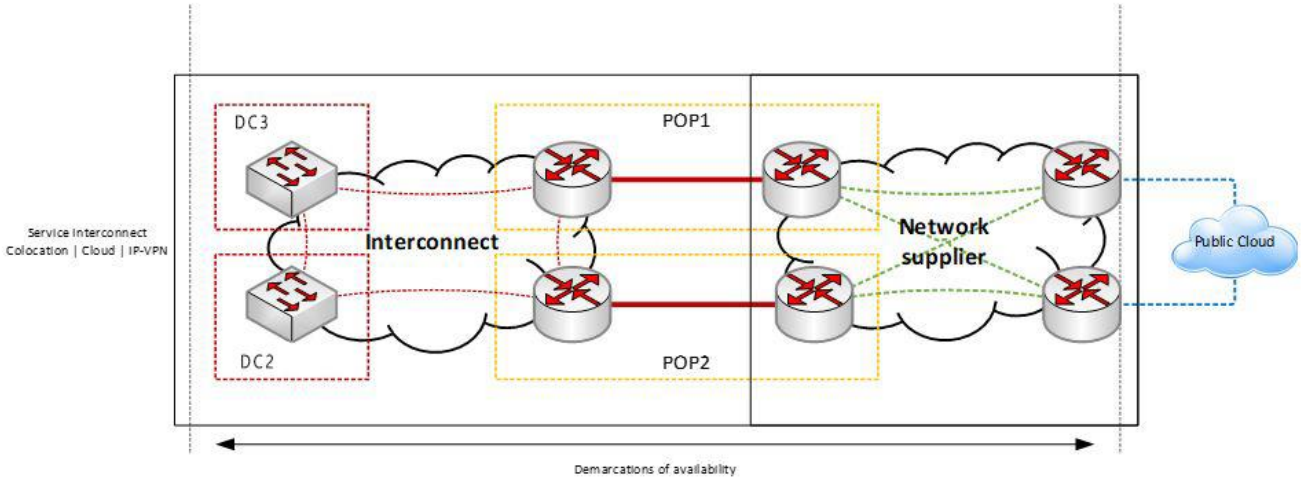

Figure 4. Availability Public Cloud Connect

3.2.5 Cloud

3.2.5.1 (Dedicated) Virtual Private Cloud (VPC) and (Dedicated) Virtual Datacenter (VDC)

Interconnect guarantees the Availability of the platform deployed to provide these Cloud Services. The Service is considered available if the platform is available.
The (Dedicated) Virtual Private Cloud (VPC) and (Dedicated) Virtual Datacenter (VDC) services are subject to SLA type Platinum when it concerns a multi-site environment. Single-site environments are subject to SLA type Gold.

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.
- On the Dedicated variant of the VPC and VDC Service single site, the availability guarantee applies as long as at least the N+1 server rule regarding redundancy is applied by the Customer. This indicates that one server from the dedicated pool of servers is set up as a failover server. This server cannot be used for the load on the cluster.
- On the Dedicated variant of the VPC and VDC Service multi-site, the availability guarantee applies as long as at least the 2N server rule regarding redundancy is applied by the Customer. This indicates that the secondary site handles as many servers as the primary site. The secondary site serves as a fallback for failover and cannot be used for load on the cluster.

3.2.5.2 Kubernetes Cluster Single Site

Interconnect guarantees with the Kubernetes Service the availability of the platform deployed to provide the Service. The Service is considered available if the platform is available.
The Kubernetes Cluster Single Site service is subject to SLA type Gold.

Preconditions/Principles

- Downtime in case of hardware failure is minimized by VMware High Availability.
  Note: However, it is important the customer's application is suitable for restarting nodes.
- Non-availability of the Service during the restart time of the VMware HA (High Availability) mechanism, does not count as Downtime.

3.2.5.3 Managed Kubernetes

With the Managed Kubernetes Service, Interconnect guarantees the availability of the platform deployed to provide the Service. The Service is considered available if the platform is available.
The Managed Kubernetes Service is subject to SLA type Platinum only when the 24/7 disaster recovery support service (“24/7 calamiteiten support service”) has been purchased.

Preconditions/principles

- In case of a failure, the Control Plane node or Worker node may be restarted. For this requirement it is necessary the Customer's application is suitable of restarting the nodes.
- To resolve issues with (customer) applications, Customer is required to provide 24/7 capacity/support.
- Applications requiring 24/7 support need to be self-healing and redundant.
- To qualify for the 24/7 disaster recovery support service ("24/7 calamiteiten support service"), the entire Kubernetes platform must be unavailable.
- The availability guarantee only applies if the 24/7 disaster recovery support service ("24/7 calamiteiten support service") has been purchased.

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

3.3 BACKUP

Interconnect endeavors to make a daily backup of all Services if possible, in order to speed up the recovery process in case of (disaster recovery) 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 gives no guarantee regarding the availability and integrity of backups made by Interconnect for disaster recovery purposes. The Customer is responsible for performing, storing (safely), verifying and validating the backup of its own data.

Only for Services for which backup is one of the primary purposes, the following applies:

- For unmanaged backup Services, the Customer sets the frequency, size and other parameters of the backup at its own discretion. Interconnect provides the Customer with an Online Customer Portal, in which the Customer has to verify the presence and content of the backup. Interconnect bears no responsibility except for provisioning of the Online Client Portal and the storage purchased by the Customer, unless and as applicable an explicit advice has been given in this regard, which has been strictly followed.
- With managed backup Services Interconnect sets the desired frequency, size and other parameters of the backup at Customer's request. Interconnect provides an Online Client Portal to the Customer in which the Customer has to verify the content of the backup. Interconnect checks at least monthly for the presence of the backups in accordance with the set parameters.

3.4 PROCEDURES

Interconnect highly values information security. Interconnect's information security policy is aimed at ensuring the reliability of information systems and to minimize any damage arising from security incidents. Interconnect is committed to the objective of measuring and improving information security on a continual basis.

3.4.1 Contact authorization

Interconnect follows a strict procedure to prevent individuals, 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:

MyInterconnect
Manage your contacts
Datacenter Access
Remote/Smart hands
Technical Changes
Administrative changes
View Contracts
Manage datacenter appointments
MyInterconnect Access
Support Portal Access
Cloud Director Access

The Authorization List stored by Interconnect is leading in determining the authorizations of a contact. The Customer is responsible for the correctness and (periodic) check of this list. The customer manages contacts and their authorizations through MyInterconnect or requests these changes in writing or by e-mail to Interconnect. Changes through MyInterconnect are effective immediately. Changes to the Authorization List requested in writing or by e-mail will only be processed during Office Hours.

3.4.2 Access procedure

Interconnect's datacenters are accessible 24x7. Visitors must be authorized by Customer at Interconnect to access the datacenter. Unauthorized visitors are only allowed access when accompanied by an authorized contact.

A visit to the datacenter must be announced by telephone at least 30 minutes in advance by telephone by a contact on Customers Authorization List. Depending on the authorization, a visit to the datacenter can be registered directly through the MyInterconnect portal by an authorized contact.

Announce datacenter visit
Phone number: + 31 73-8800012 / + 31 73-8999912 (backup)

Every visitor of the datacenter has to identify on arrival with a valid ID-document to the receptionist or Datacenter Host on duty.

Please note: a copy of an ID-document or a similar document will not be accepted and no access will be granted on this basis. Copies are not be accepted and access will not be granted without original documents.

Visitors of Interconnect's datacenters must always comply with the rules as described in "House Rules Datacenters Interconnect".

3.4.3 Reporting and handling of information security incidents

When 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).

When the Customer detects an (information) security incident or security vulnerability, related to Interconnect's Infrastructure, we request the Customer to report this to CST (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. They take care of the acceptance, registration, classification and handling of incidents, service requests and change requests.

Contact details and CST Office Hours

CST:	+31 73-8800011
Interconnect Emergency Service (Out of Office Hours Service) (24/7):	+ 31 73-8800012 / + 31 73-8999912 (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 CST.

4.2.1 Proactive and reactive

Incident management is performed in either one of the following two procedures, 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 performed on the critical components of the Service, to check various aspects like Availability and capacity.

Incidents are automatically reported by the system and processed by CST both inside and outside CST Office Hours.

The Customer will be notified if there is a Service Outage.

Reactive incident management

The reactive incident management process is triggered when CST receives a Customer's Incident Report. CST will register, classify and handle this Incident Report. An Outage can be reported both within and outside CST Office Hours.

4.2.2 Incident Report

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

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

Incidents, including Outages, detected by the Customer, can only be reported by the contacts on Customer's Authorization List.

Note:

- The Interconnect emergency service phone number (Out of Office Hours Service) is only intended for reporting an Outage of the Service, announcing a datacenter visit (see 3.4.2 – 'Access procedure') or requesting Smart Hands, performed by Interconnect Staff. This number is explicitly not intended for regular service requests.
- 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 without applicable SLA.
- If the two conditions mentioned above are not met or if outside CST Office Hours an Outage is reported that is not due to Interconnect or its supplier(s), the Failure Rate (see 2.3 - 'Conditions and exclusions') applies, plus additional startingrate. (see Appendix B – Interconnect Rate Overview).

Priority

Each Incident Report is prioritized by 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 CST.

4.2.3 Incident handling

CST endeavors to process and handle all Incident Reports as soon as possible.
The maximum incident Response Time depends on the given 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 CST Office Hours.
Class 3 (low)	Ultimately the next business day.

From the moment an Outage is handled, Interconnect will continuously work to repair and recover the Service, unless this does not reasonably shorten the Downtime.

During the Downtime the Customer will be informed periodically regarding the progress of the repair and recovery. 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. At Customers request, Interconnect will provide the Customer with an RFO (Reason for Outage) within 3 working days.

4.2.4 Escalation

CST uses functional and hierarchical escalation procedures to ensure minimal Downtime and to be able to give incidents proper attention.

4.3 CHANGE MANAGEMENT

Interconnect is allowed to perform Maintenance or Emergency Maintenance to the Service.

4.3.1 Planned Maintenance

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

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

In case the Customer wants to object to the planned date/time, then the Customer must report this to CST within 24 hours after receiving the announcement. Interconnect will take Customers objection into consideration, yet 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, authorized 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, Interconnect can decide to differ from the above mentioned announcement period.

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 Interconnect's Datacenters base facilities (e.g. power, cooling) will usualy be performed during Office Hours.
- Maintenance for Managed Kubernetes services without planned downtime, is typically performed during Office Hours.

4.3.4 Change- / Planned maintenance freeze

During the beginning and end of a calendar year, no scheduled Maintenance will be performed on Services (change freeze). 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 DC2 in the first quarter of each year, and in DC3 in the third quarter. 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 at 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 an online Datacenter Portal where, depending on the Service, the power usage and/or data traffic can be viewed. 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. This scheme is applicable when the service levels guaranteed in this SLA are not met.

5.1 SCOPE

The compensation scheme applies if the Customer appeals for compensation within 3 months after the end of the calendar year 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 is limited to 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 consisting components also offered as individual Services by Interconnect the compensation and the maximum amount of this compensation is based on the relevant part which 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.

In case the guaranteed Availability of IP connectivity is not achieved for the Services "Rackspace", "Private Space" or "Private Datacenter", and "Datacenter Connectivity" the compensation and the maximum amount of this compensation 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 – INTERCONNECT SERVICE OVERVIEW

Service	Availability			Incident Management
	Silver	Gold	Platinum	
General	**99.6%**	**99.9%**	**99.95%**	
Online customer portals				
MyInterconnect	●	-	-	Proactive
DCPortal	●	-	-	Proactive
vCenter	-	-	-	Proactive
VMware Cloud Director	●	-	-	Proactive
Rancher	●	-	-	Proactive
Support Portal	●	-	-	Proactive
Cloud				
Virtual Private Server (VPS)				
VPS Linux / VPS Windows / VPS	-	●	-	Proactive
(Dedicated) Virtual Private Cloud (VPC)				
VPC Single Site	-	●	-	Proactive
VPC Multi Site	-	-	●	Proactive
(Dedicated) Virtual Datacenter (VDC)				
Virtual Datacenter Single Site	-	●	-	Proactive
Virtual Datacenter Multi Site	-	-	●	Proactive
Kubernetes				
Kubernetes Cluster Single Site	-	●	-	Proactive
Managed Kubernetes	-	-	○	Proactive
Storage				
Object Storage	-	-	-	Reactive
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
Backup				
Microsoft 365 Backup	-	-	-	Reactive

Service	Availability			Incident Management
	Silver	Gold	Platinum	
Connectivity	**99.6%**	**99.9%**	**99.95%**	
Business DSL				
ADSL	○	○	○	Reactive
VDSL	○	○	○	Reactive
SDSL.bis	-	●	○	Reactive
Optical fiber				
Optical fiber – 3rd party networks	-	●	○	Reactive
Optical fiber – 3rd party networks (dark fiber / FTTH)	-	-	-	Reactive
"Glasvezel Interconnect" (Optical fiber Interconnect)	-	●	○	Reactive
"Glasvezel Interconnect (dark fiber)" (Optical fiber Interconnect) dark fiber	-	-	-	Reactive
Public Cloud Connect				
Public Cloud Connect	-	●	-	Proactive
Colocation				
DC2 (Eindhoven)				
Colocated Server	-	●	-	Proactive
Rackspace	-	●	-	Proactive
Private Space	-	●	○	Proactive
Private Datacenter	-	●	-	Proactive
Colocation Housing	-	-	●	Proactive
Datacenter Connectivity	-	●	○	Proactive
DC3 ('s-Hertogenbosch)				
Colocation Housing	-	●	-	Proactive
Datacenter Connectivity	-	●	○	Proactive
Other				
Domains				
"Domeinregistratie (Plus)" Domain registration (Plus)	-	-	-	Reactive

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

APPENDIX B – INTERCONNECT RATE OVERVIEW

Sort	Rateclass	Start rate	Hourrate **
CST/DCE/DCB	A		€ 110
Projectmanagement	B		€ 145
Engineering and audits	C		€ 185
RFC Low	K		€ 185
RFC High	L		€ 275
Failure rate	M	€ 275	€ 275

Interconnect rate overview: reference date 13.2.2025 *.

*These rates may be revised as described in Article 11.3 of Interconnect's general terms and conditions.
**Per hour started