Bilag 12.c Co-location

Dynamic purchasing system

02.22 It-drift

Version 1.0

The State and Municipalities' Purchasing Service A/S
The assembly hall | Pakkerivej 6, 2500 Valby
Telephone +45 33 42 70 00 | CVR 17472437

Contents

1 Introduction

This appendix contains the Customer's requirements for the Co-Location that the Supplier must deliver under the Supply Contract, including with a view to complying with the Service objectives set out in Appendix 8 (Service Objectives) for the Supplier's delivery of operations.

In its delivery of Co-Location to the Customer, the Supplier must comply with and adapt its solution according to the Customer's requirement specification and set-up, cf. appendix 3 (Customer's IT environment).

This appendix sets out the requirements for placing the Customer's own IT equipment in the Supplier's data centers as well as the Supplier's operation of the Customer's data centers.

2 General requirements for Co-Location

The supplier must deliver Co-Location as regulated in this Annex 12.c (Co-Location). Co-Location means Services in relation to physical data center facilities as well as associated service, advisory and security services, such as the provision of physical security, perimeter security, physical access control and monitoring. When delivering Co-Location, the Supplier must handle all underlying operation and maintenance of fixed installations that enable the Customer to operate, maintain and support its own data center solution in the Supplier's data center facilities through the provision of housing Services, including for example physical floor space, racks, cages, premises, power and cooling where the Customer can install his own IT equipment.

K-1 General requirements for Co-Location

The Supplier must deliver Co-Location under the Delivery Contract via the data centers described in Annex 12.c.i (Supplier's solution description). The supplier must:

a. handle all Operational Processes that are relevant in connection with Co-Location, cf. appendix 4.c (Operational Processes)

b. ensure monitoring of all Co-Location, including compliance with all KPIs related to Co-Location. As part of the monitoring, the Supplier must, among other things, but not exclusively:

i. create alarms based on the underlying suppliers' and/or manufacturers' best practice

ii. set up other alarms so that the Supplier can proactively carry out mitigating actions as well as other alarms that may be necessary to meet the Customer's requirements for the Supplier's delivery of Services and reporting under the Supply Contract.

c. provide the necessary assistance to the Customer and the Customer's Other Suppliers, e.g. in connection with Root Cause Analyses, including Root Cause Analyzes in relation to security incidents related to the Supplier's own equipment (e.g. failure of power supply, failure of UPS, breakdown in cooling, burglary and access by unauthorized persons).

K-2 The supplier's advice

The Supplier must advise the Customer within Co-Location, including how the Customer can optimize its Co-Location with regard to operational reliability, performance and price, e.g. optimal placement of equipment in rack cabinets in relation to e.g. current load and expedient utilization of the ongoing development of data center technology.

K-3 The supplier's certifications

The supplier must be ISO/IEC 27001 certified or equivalent, or comply with the rules and guidelines of the ISO/IEC 27001 standard.

EK-1 The supplier's certifications

The Supplier must document its current ISO/IEC 27001 certification or equivalent, or document how the Supplier ensures compliance and compliance with the rules and guidelines in the ISO/IEC 27001 standard.

The supplier must also document the offered data center's compliance with the tier III standard, or higher, as specified by the Uptime Institute or similar organization.

In connection with the evaluation of the Supplier's response, it is positively weighted if:

- **The supplier is ISO/IEC 27001 certified or equivalent, cf. K-3.**
- **The Supplier can in other ways document how the Supplier ensures compliance with the rules and guidelines in the ISO/IEC 27001 standard, cf. K-3.**
- **The supplier has a Tier III certification for the data center offered, cf. K-5**
- **The supplier can otherwise document Tier III compliance for the data center offered, cf. K-5.**

The Customer will make an assessment of the Supplier's response in connection with the evaluation of Annex 12.c (Co-Location). The assessment is made in relation to the sub-criterion relating to Quality.

It is recommended that the Supplier limit its response to 5 Pages.

The supplier must insert its response to the evaluation requirement in appendix 12.c.i (Description of the supplier's solution).

K-4 Provisioning and decommissioning of the Customer's IT equipment

The supplier must ensure provisioning and decommissioning of the Customer's IT equipment, including racks and floor space as described in K-11 and K-12.

K-5 Supplier's data centers

The supplier must provide Co-Location equivalent to the tier III standard or higher as specified by the Uptime Institute or equivalent organization. This implies that the data center's infrastructure components must be able to be maintained simultaneously and that the Supplier's Co-Location must contain:

1. Redundant and independent power supply (UPS), automatic transfer switches (ATS) and battery to ensure uninterrupted transition to secondary emergency power in case of power loss, interruptions and peak load periods. The UPS system must be sized to be able to supply the data center's total consumption for the necessary period until emergency generator power is phased in.

2. Redundant emergency power generator such as oil/diesel generator for power generation as well as fuel storage and refueling facilities. The emergency power generators must be able to take over the load of the data center from the UPS before it runs out of power, incl. an appropriate margin of safety. The emergency power generators must be equipped with flicker-free feedback to the power from the data center's power grid company. The emergency power generator system must be sized to be able to supply the data center's total consumption.

3. Replenishment agreement with fuel supplier so that the emergency power generators can run continuously until power from the data center's utility company is re-established.

4. Redundant and independent separate plug entry for all essential external supply sources, including power cables (with separate electrical panels and fuses), network cables and water pipes into the data center.

5. Redundant cooling, humidity control and heat rejection equipment for rooms and spaces.

6. Fire protection, including installations for fire fighting and ensuring that fire fighting equipment does not damage the data center's other installations, infrastructure or network.

7. Water protection, including protection against water ingress and flooding.

8. Redundant internal distribution routes for the above, e.g. power cables (mains), network cables and water pipes.

K-6 Redundant Data Centers

EXPIRES

EK-2 The supplier's data centers

The supplier must describe the data center the supplier offers the customer.
The supplier's description must cover at least:
-Tier certification or equivalent data center certification, cf. K-5
-Geographical location (address)
-Perimeter security
- Shell protection
- Access control
-Cabling (the data center's routing paths)
-Water, fire and electricity protection
-Power supply and construction under the floor
-Cooling (what types of cooling solutions are offered)
-Facilities (warehouse, unpacking area, common living room, cleaning, etc.)
- Offered data center space (shutdown, installation floor, climate control, guideways, lighting, outlets, etc.)
- Option for extended protection of specially secured environments
- Possibility of expansion

In connection with the evaluation of the Supplier's response, it is positively weighted if:

- **The Supplier can make a data center with a tier III certification (or higher) or equivalent available to the Customer.**
- **The supplier's data center has a high level of security**
- **The supplier's data center is able to ensure a high degree of redundancy in the infrastructure**
- **The supplier's data center offers high delivery reliability**
- **The supplier's data center offers good facilities for the customer's employees**
- **The customer can continuously monitor power consumption at a detailed level**
- **The supplier's data center offers the possibility of high power loading of rack cabinets**

The Customer will make an assessment of the Supplier's response in connection with the evaluation of Annex 12.c (Co-Location). The assessment is made in relation to the sub-criterion relating to Quality.

It is recommended that the Supplier limit its response to 8 Pages.

The supplier must insert its response to the evaluation requirement in appendix 12.c.i (Description of the supplier's solution).

K-7 Data center access

The supplier must secure and at all times be able to document a complete audit trail in relation to all virtual and physical access to the data center.

The Supplier must ensure and facilitate that the Customer's own technicians, the Customer's Other Suppliers and auditor(s) can access the Supplier's data centers and network installations 24/7/365 to the extent that the Customer may need this. The customer must approve all access following the foregoing.

K-8 Datacenter governance

The supplier must ensure that the allocated employees, who must access the data centers in which the Customer receives Co-Location, have the necessary training, qualifications, authority permits, knowledge of installations and knowledge of the Customer's cooperation organization, to deliver safe and stable operation.

The Customer must approve the Supplier's allocated employees before the allocated employees begin operation, maintenance and support tasks for the Customer.

When entering into the Supply Contract, the Customer states its conditions for the Supplier's access. The customer cannot refuse his approval without a valid reason. Factual reason can e.g. be if the Supplier's employees do not obtain the necessary security approval to be able to perform work for the Customer.

K-9 Data Center Maintenance

The supplier must coordinate data center maintenance taking into account the Customer's conditions, so that the Customer is as little affected by downtime as possible. The Supplier must obtain the Customer's approval prior to commencing all maintenance work, regardless of whether it is planned, preventive or unplanned maintenance.

The supplier's maintenance obligations consist of, among other things, of providing monitoring and proactive intervention related to the Customer's IT equipment when the IT equipment shows initial signs of failure.

K-10 Data Center Security

The supplier must immediately inform the customer in the event of a security breach, if the customer's data is potentially or currently put at risk. If the security breach is caused by the Supplier, the Supplier must immediately and without undue delay implement its action plan for this.

K-11 Floor space

The Supplier must, at the Customer's request, make available floor space, including the possibility of dedicated and private locked rooms and cages for servers, in the Supplier's data centre. The customer must be able to set up their own IT equipment, such as rack cabinets and cubes, on the floor space.

In this connection, the supplier must ensure that all necessary cabling as well as fixed installations and network connections are available to the customer for setting up the customer's own IT equipment. The supplier must, among other things, but not exclusively provide:

a. Redundant power sources.

b. Redundant network connections and accesses.

c. Cooling, water and fire protection.

d. Availability and option to purchase additional floor space to meet the Customer's needs.

K-12 Racks

The Supplier must provide rack cabinets, including dedicated and private rack cabinets, in connection with the Customer's placement of IT equipment in the Supplier's data centers. The supplier must, among other things, but not exclusively ensure that the following are made available:

a. Redundant power sources.

b. Redundant network connections and accesses.

c. Cooling, water and fire protection.

d. Redundant Power Distribution Unit (PDU).

e. 19" locked rack cabinet with space for a minimum of 42U.

f. Availability and option to purchase additional racks to meet the Customer's needs.

K-13 Power

In connection with the Customer's purchase of floor space or racks, the Supplier must supply climate-friendly power according to consumption for the Customer's IT equipment in the Supplier's data centres. The power must be from renewable energy sources such as water, wind and solar energy. The supplier's purchase of climate-friendly electricity must comply with the requirements set out in Appendix 22 (Social responsibility, work clause and student places).

K-14 Other Requirements

No own requirements

3 Green Requirements

K-15 Basic requirement: The ratio between renewable energy and the total energy consumption (REF)

The supplier must document how large a proportion of the total power consumption used in fulfilling the supply contract originates from renewable energy sources.

As documentation for fulfilling the requirement, the supplier must present a statement of the percentage of the total power consumption that comes from renewable energy sources, prepared as a ratio between renewable energy and the total power consumption (REF).

REF must be calculated according to: EN 50600-4-38 but only calculated in relation to power consumption for the data center(s) and where renewable energy sources are defined according to directive 2009/28/EC9.

Documentation: (see above method)

- Calculation of REF with associated reference to the documentation below:
- Copy of electricity bill(s) showing the total electricity consumption.
- Copy of the purchase of green electricity and/or production of renewable energy, which demonstrates the total access to electricity from renewable energy sources and which complies with Directive 2009/28/EC9.

The supplier must submit documentation for the above requirements once a year at the Customer's request and no later than 20 Working Days thereafter.

K-16 Basic requirements: Data center design

The supplier must confirm and document that the supplier works for an effective data center design that contributes to high energy efficiency. 'Effective' must be understood in accordance with the guidelines for Airflow management as described in the EU's Code of Conduct section 5.1.1, 5.1.2, 5.1.3, 5.1.4 and 5.1.5 as well as the guidelines for 'Cooling management' as described in the EU Code of Conduct section 5.2.2, 5.2.3, 5.2.4, 5.2.5 and 5.2.8.

The supplier must, at the customer's request, as documentation for fulfillment of the requirement, send e.g. images, data center design sketches or descriptions, which show that the above guidelines have been complied with and are continuously monitored. If there is a difference in design at different locations or areas of the locations, this must be stated in the description. It must thus be made visible whether the customer is placed in an area or in several data centers that are more or less energy efficient than others.

The supplier must submit documentation for the above requirements once a year at the Customer's request and no later than 20 Working Days thereafter.

K-17 Green light: Use of refrigerants with low greenhouse gas warming potential (GWP)

The supplier must not use refrigerants with a GWP of more than 675.

The supplier must, as documentation for the fulfillment of the requirement, submit an overview of the GWP for the refrigerants used, which are part of the refrigeration systems used for the fulfillment of the Supply Contract.

The supplier must submit documentation for the above requirements once a year at the Customer's request and no later than 20 Working Days thereafter.

K-18 Green light: Proper disposal of used batteries from UPS systems

The supplier must describe the implemented solution/agreement for the correct disposal and possible recycling of end-of-life batteries from UPS systems that have been used in the fulfillment of the Supply Contract.

The supplier must, as documentation for the fulfillment of the requirement, describe the process for returns to the manufacturer, seller or other relevant third party, as well as a contract or other agreement as documentation for the return scheme." Disposal, reuse and recycling must be in full compliance with the requirements of Article 8 and Annexes VII and VIII of the (recast) WEEE Directive 2012/19/EU.

The supplier must, as documentation for the fulfillment of the requirement, describe the process for returns to the manufacturer, seller or other relevant third party, as well as a contract or other agreement as documentation for the return scheme.

The supplier must submit documentation for the above requirements once a year at the Customer's request and no later than 20 Working Days thereafter.

K-19 Green light: Data center efficiency

The supplier must demonstrate DCiE for the data center or for each of the data centers used to fulfill the Supply Contract.

The supplier must provide documentation for DCiE for the data center or for each of the data centers used to fulfill the Supply Contract. The supplier must, as documentation for the fulfillment of the requirement, present the DCiE for the data center or for each of the data centers used to fulfill the Supply Contract.

The documentation of DCiE must follow the EU Code of Conduct, section 9.3.1, that is:

- DCiE = (IT equipment power consumption / Total data center power consumption) x 100%
- DCiE = 1/PUE (1 divided by PUE)

For DCiE, the efficiency scale below has been defined.

PUE	DCiE	Level of Efficiency
3.0	33%	Very Inefficient

2.5	40%	Inefficient
2.0	50%	Average
1.5	67%	Efficient
1.2	83%	Very Efficient

Once a year, at the Customer's request, and no later than 20 Working Days thereafter, the Supplier must submit the DCiE or updated DCiE for the data centers that are used to fulfill the Delivery Contact as documentation for the above requirements.

K-20 Red light: Minimizing the content of harmful substances

EXPIRES

K-21 Other Requirements

K-21.K-1 Power usage effectiveness (PUE)

The supplier must continuously measure the data center's PUE, cf. K-19. The PUE of the data center must not exceed 1.3.

PUE is logged and reported to the Customer in the monthly status report.

4 Other Requirements

K-22 Other Requirements

K-22.K-1 Geographical location of the data center

The data center will be operated by staff from the Customer's address at Lautruphøj 2 in Ballerup. In order to limit the transport time for the Customer's personnel between the Customer's address and the new data center, the new data center must be located at an address within a radius of no more than 30 km from the Customer's address.

Furthermore, for security reasons, the new data center must not be located at an address in Glostrup Municipality.

K-22.K-2 Perimeter security

The data center building must be secured with an outdoor perimeter fence at a minimum height of 2.2 metres.

K-22.K-3 Shell protection

At a minimum, the data center building must be secured against physical access corresponding to the AIA catalogue's security level 50-S or equivalent.

Larger openings in the interfaces to the secured area must be equipped with doors, windows or members that are Insurance & Pension-registered according to EN 1627, RC4 or equivalent or with gates according to SSF 1074, class 32 (RED class) or equivalent cf. www.sikringsguiden.dk – or be reinforced with fuses that are classified accordingly.

K-22.K-4 Building-in-building

The data center must be designed according to the building-within-a-building principle, with its own walls and its own roof, independent of the shell protection. The customer's data center outer walls must not adjoin or be the shell fuse's outer walls.

K-22.K-5 Access control

The data center must have:

- Physically manned access control 24/7/365.
- Access control system at all entrances to the data center with personal access control that ensures physical access to buildings, premises and spaces, including the customer's data center through closed and locked doors and gates.
- Access log showing the name and time of personnel who have gained access to the Customer's data centre. The access log must be available to the Customer.
- Dedicated emergency response in case of emergencies.

K-22.K-6 Supervision

The data center must have 24/7/365 video surveillance, including monitoring of outdoor areas, entrances, doors, gates, corridors/walkways, rooms and spaces using a data center monitoring, alerting and fault management system. The video surveillance must be saved for a minimum of 30 days.

If the Customer so wishes, the Supplier must establish video surveillance of the Customer's data center. The video surveillance must be made available to the Customer on request.

K-22.K-7 Reaction in case of alarm

In the event of a security breach or potential breach of security, the Supplier must immediately and without delay alert the Customer or an authorized customer representative.

The total reaction time from alarm release to local alarm disconnection or equivalent must not exceed 20 minutes - cf. Insurance & Pension's guidance on Reaction to an alarm from an AIA facility.

K-22.K-8 Access card

The Supplier must, as part of Transition Ind, create access rights in the Supplier's access solution and issue physical access cards (permanent cards) to 20 people in the Customer's staff to the Customer's data centre.

K-22.K-9 Access rights portal

The supplier must make a web-based portal available to the customer, where the customer can order/update/change/withdraw access to the customer's data center.

K-22.K-10 Card readers

All card readers used for the Customer's access/areas are logged. The access is reported to the Customer in the monthly status report.

K-22.K-11 Key boxes

The supplier must establish two key boxes with separate codings. An external key box that only gives access to the Customer's data center and, if applicable, other rooms as well as an interior key box that gives access to the Customer's secured access to the room. Key boxes outside the data center must be electronically locked for reasons of access control and logging. The internal key box(es) must be located one per cube and at the end closest to the entrance to the data center.

The number of keys in the individual cube must reflect the number of rack cabinets.

K-22.K-12 The data center's guideways

The supplier's data center must be equipped with redundant routing paths to the Customer's data center, including routing paths for power and network/internet connection.

The redundant guideways must be clearly separated. For example the redundant routing paths can go from opposite sides of the Supplier's data center building to the equivalent in the Customer's data center premises.

K-22.K-13 Leadways to networks

The redundant routing paths for the network connection from the data center's meet-me room (the physical connection point between the Customer's network provider's network and the data center's internal network) to the Customer's data center must be implemented as 2 times 24 pairs of single-mode fiber cable per routing path.

K-22.K-14 Protection against penetrating water

The data center must be secured against ingress of water. This can e.g. happen in the form of closing off all cable/installation penetrations that break through the data center's climate shell.

The data center must also be able to withstand a 100-year event related to rainfall. The supplier must be able to document measures taken to withstand such an incident.

Possibly water intrusion incidents that have occurred must be logged and reported to the Customer in the monthly status report.

K-22.K-15 Detection of leaks

The data center must be equipped with a system for detecting leaks on the roof, under the raised floors and in refrigerant piping. The supplier must be able to document an emergency plan for handling leaks. Possibly leaks must trigger an alarm with the Supplier and the Customer.

Possibly leakage incidents that have occurred must be logged and reported to the Customer in the monthly status report.

K-22.K-16 Fire detection

The data center must be equipped with a Very Early Smoke Detection Apparatus (VESDA) system or similar type of fire detection.

K-22.K-17 Firefighting

The data center must be equipped with an active fire extinguishing system that uses inert (non-reactive) gas as extinguishing agent. The extinguishing agent must be discharged during constant gas discharge, i.e. the system must use Constant Discharge Technology (CDT). The system's extinguishing nozzles must be equipped with silencers.

The extinguishing system must be approved by an authority-approved body and the approval must be valid for the entire contract period.

In the event of extinguishing gas being released in the data center, a human fire guard must be deployed during the period until automatic fire fighting is re-established.

The supplier must be able to document an emergency plan for handling fire. A fire that occurs must trigger an alarm with external fire emergency services, the Supplier and the Customer.

Possibly fires that occur must be logged and reported to the Customer in the monthly status report.

K-22.K-18 Protection against power failure

The data center must be equipped with protection against power failure, cf. requirement K-5.

The supplier must be able to document an emergency plan for handling power failures. A power failure must trigger an alarm with the Supplier and the Customer.

Possibly power failures that have occurred must be logged and reported to the Customer in the monthly status report.

K-22.K-19 Fuel readiness with filling agreement

The Supplier must have a valid and active filling agreement with the fuel supplier/s regarding "infinite" supply of fuel for the Supplier's emergency power generators, so that the emergency power generators can run continuously until the power from the data center's power grid company is re-established in the Customer's data center, cf. K-5.

K-22.K-20 Storage room

The supplier must make a separate storage room available to the customer for receiving and storing equipment until it can be set up in the customer's data center.

The warehouse must be dedicated to the Customer, locked and monitored.

The storage room must have a minimum area of 12 m² and a ceiling height of 2.4 m.

K-22.K-21 Receiving equipment

The supplier must receive equipment that has been sent to the Customer's data center and place it in the Customer's storage room.

K-22.K-22 Unpacking area

The supplier must make a separate or common unpacking area available to the customer for unpacking equipment outside the warehouse and the customer's data center.

The unpacking area must have a minimum area of 6 m² and a ceiling height of 2.4 m.

K-22.K-23 Loan of rolling table and similar

The supplier must, if such equipment is available, give the customer access to the loan of a rolling table for the transport of equipment from the unpacking area to the customer's data centre.

K-22.K-24 Common living room

The supplier must make a separate or shared living room, with toilet and dining facilities, available to the customer.

Dining facilities must contain a kitchenette or similar with access to electricity, toilet, water, coffee, tea, dining table and chairs. The supplier must provide wi-fi in the living room.

K-22.K-25 Access to temporary dedicated room

Upon request, the customer must be able to make available a temporary room dedicated to the customer's staff for crisis management or the like with 4 hours' notice. The room must have room for a minimum of six people and have the possibility to set up conference equipment and be equipped with wi-fi.

K-22.K-26 Cleaning

The supplier is in charge of cleaning the data centre, including the Customer's data centre.

Personnel who carry out cleaning must comply with safety requirements cf. appendix 14 (Security), K-37.

Cleaning must be logged (who, when and extent) and reported to the Customer in the monthly status report.

K-22.K-27 24-hour shift

The supplier's data center must have a 24-hour guard that the customer can contact 365/24/7 if necessary, e.g. for questions regarding data center availability.

The 24-hour service is not a service desk that the customer does not need.

K-22.K-28 Closure

The customer's data center must be isolated so that only the customer has access to the customer's IT equipment in the data center.

If there are openings in the room facing other customers' data centers, the openings must be secured with an attached fine-mesh grid, which also applies under the floor, where the grid is at least at safety level with Troax safe UX 550 grid fence.

K-22.K-29 Capacity

The customer's data center must have an area of approx. 260 m² and a ceiling height (from floor tiles to ceiling) of at least approx. 3.75 m and could accommodate the following equipment:

- 90 rack cabinets
- 3 patch network racks ((dimensions: 100 cm in width and 60 cm in depth) placed against the walls of the data center so that they are not placed where the rack cabinets are located.)

K-22.K-30 Raised installation floor

The installation floor of the data center, on which the rack cabinets are installed, must be raised above the raw concrete floor of the data center and have a clearance of at least 100 cm.

The raised floor must have a bearing capacity of at least 1400 kg/m2 for fire cabinets and 1200 kg/m2 for the rest.

The basic structure of the floor must be grounded to the data center's overall grounding system.

In the case of cubes, cooling is blown in from below through perforated floor tiles that maintain the same load-bearing capacity as specified above. Perforated floor tiles are ordered in collaboration with the Supplier, so that the cooling performance can be optimised.

K-22.K-31 Cooling and humidity

The data center must be equipped with a climate control system so that temperature and humidity can be controlled. Cooled air must be blown into the cold aisle of the cubes from the floor, via perforated floor tiles.

The data center's climate control system must maintain the following climate intervals:

- The cubes must maintain a temperature of 22-25 °C, measured in the cold center aisle of the cube.
- The cubes must have a relative humidity of 30-60%, measured in the cold center aisle of the cube.

If the temperature in the cold aisle of the cubes exceeds 25.5 °C, the exceedance must trigger an alarm at the Supplier and the Customer.

The ongoing measurements of temperature and humidity must be logged and reported to the Customer in the monthly status report.

K-22.K-32 Guideways

The supplier must establish routing paths for cabling to the cubes' rack cabinets after clarification with the customer. The guideways are established via grid trays strung over the cubes. The grid trays must have a firm base of e.g. clear plexiglass. The guide ways must have a width of at least 300 mm.

Guideways must be established over each of the cube's rows of rack cabinets. A guideway must also be established across between the cube's rack rows, with spaces not exceeding 3.6 metres.

For all branches, it is ensured that the cables do not exceed their maximum bending radius, e.g. by using "waterfall".

Setting up guide ways (wire grid trays) must follow the instructions from the relevant supplier/manufacturer.

K-22.K-33 Lighting

The supplier must establish lighting everywhere in the Customer's data center with an illumination intensity of at least 300 lux in the data center's cold and warm corridors. All floor areas and rack cabinet sides must be lit to ensure a good working environment. There must be no floor areas or rack cabinet sides left in darkness or shadow.

K-22.K-34 Wi-Fi

The customer must be able to set up their own WiFi (wireless data network) access point in the customer's data center.

K-22.K-35 Outlet

The supplier must establish 10 grounded outlets/sockets with 230 volt alternating current in the Customer's data center. The sockets must be distributed evenly over the data centre.

K-22.K-36 Measurement of power consumption

The customer wants to be able to continuously monitor power consumption, both for reasons of consumption, but also to be able to see the load on the individual rack cabinets and PDUs, for reasons of optimal placement of equipment. The supplier must therefore continuously measure the power consumption (kWh) in the customer's data centre. It must be possible to monitor power consumption both for the data center as a whole, for each of the data center's 3 phases, for the data center's rack cabinets and for the rack cabinets' associated PDUs

The ongoing measurements must be logged and reported to the Customer in the monthly status report.

K-22.K-37 Number of rack cabinets

The supplier must acquire and install 90 rack cabinets in the Customer's data center.

K-22.K-38 Rack cabinet specifications

The rack cabinets established by the Supplier must meet the following specifications:

- Width (EIA standard): 19”
- Width: 800 mm
- Depth: 1200 mm
- Height: approx. 2000 mm
- Space capacity: minimum 42 rack units (U)
- Carrying capacity: minimum 1200 kg

K-22.K-39 The design of the rack cabinets

The rack cabinets established by the Supplier must have:

- Light colors (white, glacier white or light gray)
- Removable side panels.
- Perforated front door with minimum 80% opening
- Perforated double door (French doors) on the back with minimum 75% opening
- Cover plate at the bottom of the rack front to protect against short-circuiting of cooling air
- It must be possible to install blanking plates (on click) for unused U capacity
- Adjustable 19” mounting at the front and back for later installation of servers
- It must be possible to lead cables from the ceiling's cable trays down through two openings in the top of the rack cabinet and further down through the right and left sides of the rack cabinet. The openings in the top of the rack cabinet must be covered with "brooms", so that outflow of cold air is reduced as much as possible.
- Each rack cabinet must have its own ground. An earthing kit must be supplied for the sides, door and doors of the rack cabinet.

K-22.K-40 The hinges of the rack cabinets

In order to secure escape routes, the front doors of the rack cabinets (in the cold part of the cube) must be hinged so that escape to the right or left from the center of the cube can take place unimpeded. That is if a front door is open and blocks the escape route, this must be easily closed by hand on the way out of the cube.

This means that from the center of the cube, the front doors must be right-hinged on one side (and left-hinged on the opposite side), which ensures an unobstructed escape route to the left. The same must apply to the other half of the cube, where the front doors must be left-hinged on one side (and right-hinged on the opposite side), which ensures an unobstructed escape route to the right.

K-22.K-41 Rack cabinet accessories

Rack cabinet accessories

All rack cabinets must be supplied with the following accessories:

- 4 wheels and 4 adjustable still legs that can fix and lock the rack cabinets when they are put in place
- Patch cable holders (finger system) in the sides, both front and back at full rack height with outlets per U for vertical routing of patch cables in rack cabinets
- Air dam kit between 19” mounting and side panel so that cold air passes through the equipment and warm air does not recirculate around the equipment
- Clamping bracket for joining several rack cabinets.

K-22.K-42 Locking the rack cabinets

The rack cabinets established by the Supplier must be lockable. Unique key access must be provided for each rack cabinet, as well as a suspended key cabinet for each cube in the Customer's data center, where access is by key card. Alternatively, an electronic locking system operated with an access card can be established by agreement with the Customer.

K-22.K-43 The rack cabinets' power supply

Each rack cabinet must, on the back and on each side, be supplied with 2 redundant vertical rack PDUs (Power Distribution Unit) in full height.

The customer's data center must be able to supply grounded 3-phase 400 volt AC, 32 amps, 50 Hz to each PDU in a rack cabinet.

Each PDU must therefore be able to be loaded with an output of up to 22 kW. However, an average load of 8 kW per PDU is expected at normal load.

However, selected rack cabinets must be able to be loaded with a higher power of up to 66 kW (3 * 22 kW), when installing additional PDUs (66 kW rack cabinets must be supplied with 6 PDUs, 3 PDUs for the supply of 3 * 22 kW power and 3 PDUs to maintain redundancy). Alternatively, the 66 kW load can be distributed over 3 rack cabinets with a load of 22 kW in each rack cabinet.

In the clarification phase, the Supplier must come up with a proposal for the selection of PDUs. The final decision is made in collaboration with the Customer.

K-22.K-44 Number of cubes

The supplier must establish the number of cubes in the Customer's data center which ensures optimal utilization of the data center's area and optimizes the requirements for cooling and power supply.

K-22.K-45 Design of the cubes

The cubes established by the Supplier must have:

- Plate enclosure that closes off between cold and hot areas in the rows of rack cabinets
- Take in clear and self-supporting non-flammable plastic material (alternatively made of glass material)
- Self-closing double sliding doors, made in plate casing, at the ends of each cube

K-22.K-46 Specifications of the cubes

The supplier must organize the data center's rack cabinets into cubes, so that the customer's data center is used optimally in terms of space utilization as well as power consumption and cooling.

There must be a space of two floor tiles between a cube's rows of rack cabinets.

K-22.K-47 Unlocking the cubes

The cubes established by the Supplier must be lockable. Unique key access must be provided to each cube in the Customer's data center. Alternatively, an electronic locking system operated with an access card can be established by agreement with the Customer.

K-22.EK-1 The supplier's offered data center premises

The supplier must document the offered data center in a dimension-fixed and editable Microsoft Visio drawing, with an indication of the scale ratio used, so that the Customer can detail the location of equipment in the offered data center.

The drawing must contain at least:

- Floor tiles
- Rack cabinets
- Cube placements
- Guideways over cubes, and from external rooms

- Cooling units
- Bearing concrete columns

In connection with the evaluation of the Supplier's response, it is positively weighted if:

- The data center offers efficient use of the room
- The data center optimizes the number of cubes
- The routes to the data center are clearly separated.

The Customer will make an assessment of the Supplier's response in connection with the evaluation of Annex 12.c (Co-Location). The assessment is made in relation to the sub-criterion relating to Quality.

The supplier must insert its response to the evaluation requirement in a separate appendix 12.c.ii (Supplier's solution description – Drawing of data center premises).

K-22.K-48 Ownership of established rack cabinets and cubes

The supplier must, as part of Transition Ind, purchase and establish the rack cabinets and cubes requested in this appendix. After the transition day, ownership of the purchased and established rack cabinets and cubes passes to the Customer.