Customer Guide to the *DATA*ONE Datacenter

User guide for
Private Suite or Colocation Customer

Version 1.0
July 2012

CONTENTS

1   Welcome

Thank you for choosing *DATA*ONE housing services. To simplify your move to our facility and ensure security of all personnel and equipment, this guide is provided to explain our Colocation and Private Suite requirements in accordance with the Service Level Agreement which is part of your signed contract. If you have questions or concerns, do not hesitate to call your Service Manager.

2 Getting started

2.1 Contacting us

*DATA*ONE
Bruynvisweg 11
1531 AX Wormer
Netherlands

Support e-mail: support@dataone.nl
Security e-mail: security@dataone.nl

Phone: +3175711 2156 (24/7)

2.2 Obtaining Security Access to the Facility

After your final walkthrough and approval of the *DATA*ONE facility Guide, you will be able to obtain security badges that will give you access to the facility.

You shall determine at least one Primary Badge Administrator for your company and a maximum of two Secondary Badge Administrators. The Primary Badge Administrator is responsible for all (security) contacts between *DATA*ONE and the client. The secondary Badge Administrator will be in charge when the Primary Badge Administrator is not available. The Primary Badge Administrator will always be informed about any issue.

1.   The Badge Administrators are the single point of contact for all security issues.

2.   Every call from a Badge Administrator for security-related requests shall be sent to our email address: security@dataone.nl. Calls received by *DATA*ONE from those individuals within your company who are not authorized Badge Administrators will be referred back to your company's authorized Badge Administrator with their request. Only Badge administrators will be allowed to:

- Request additional badges
- Change the status of a badge
- Enquire on security issues
- Allow visitors in the Private Suite or Colocation Room

3.   Your Service Manager will walk you through the process for each of your employees and/or vendors to obtain their badges. The Badge Administrator shall communicate the content of this document to their authorized employees/vendors. For security purposes, please be prudent about the number of badges you distribute to your employees. The Service Manager will need to determine the following information in order to process your badge request:

- Date and time that access is needed (At least 24 hours advance notice is required for scheduling purposes).
- Name of the person(s) needing access as well as their associated company name
- Whether access is "Permanent" (1 year) or "Temporary" (24 hours,etc)

4.   When your employees or vendors visit the facility for the first time, they will be required to show Government-issued photo I.D., Passport or Drivers License. Thereafter, they will have their pictures taken.

5. At least one operations staff member will be available to process badge requests during office hours from 9.00 through 16.00 local time.

6. Please notify your Service Manager as soon as possible when any employee or vendor is no longer allowed to enter the Private Suite or Colocation Room by email.

7. Your employees and vendors with valid access badges have unescorted access to your Private Suite or Colocation Room, 24/7, unless otherwise agreed.

8. Anyone without a valid access badge that requires access can be accommodated as follows:

   - They must be announced at Security in advance and must be escorted by a badge holder or the Datacenter Security Engineer.

Permanent badges are valid for 12 months. However the first time until January 1st of the next year. Each company's Badge Administrator is responsible for revalidating badges prior to the expiration date. You will be notified 60 days prior to the expiration date to revalidate the employees with badges. Badges without revalidation authorization by the 12-month anniversary date will automatically expire and will require manual re-activation by the Security Engineer.

---

3 *DATA*ONE Policies

3.1 Security Standards

- *DATA*ONE facilities are monitored 24/ 7
- *DATA*ONE will provide and maintain in working condition card readers(s) and/or other access devices) as selected by *DATA*ONE for access the Private Suite or Colocation room.
- Under no circumstances may you "prop open" doors or otherwise bypass the security measures and devices *DATA*ONE has imposed for access to the *DATA*ONE Facilities.
    - No "tailgating" is allowed – each individual who enters the facility must use a valid access badge or must be escorted by a valid badge holder.
    - No propping or holding open doors is allowed.
- *DATA*ONE will provide a locking device on Customers Private Suite or Colocation Room, which Customer shall be solely responsible for locking and/or activating such device. In the event that unauthorized parties gain access to the Private Suite or Colocation Room through access cards, keys or other access devices provided to Customer, Customer is responsible for any damaged caused by such parties.
- You will be responsible for the cost of replacing any security devices lost or stolen after delivery thereof to Customer.
- In the event you have reason to believe that an unauthorized party has gained access to your Private Suite or Colocation Room, *DATA*ONE will, at your written request which should not be made later than 7 days after the suspected time of breach, make video surveillance tapes of the Private Suite doors or corridors leading to your Private Suite / Colocation room available to you for viewing in the presence of a *DATA*ONE employee.
- In addition to the previous point, *DATA*ONE will provide you with a copy of the access logs for doors or building, as applicable, upon prior written request.
- You will be responsible for securing doors/gates to the Private Suite or Colocation Room.
- All Access Controlled Doors are monitored by *DATA*ONE.
- It is not allowed to take any pictures inside the building, except of your own equipment.
- Any cameras, or visual monitoring devices mounted inside private Suites or Colocation Rooms may only be used to monitor access and egress at the immediate location of the exterior door of the suite.
    - If it is determined that the field of the monitoring device exceeds the immediate area of the door, and is capable of viewing activities other than access and egress from the room, the device will have to be removed, or modified, at the Customer's expense.
    - Viewing of work areas located in *DATA*ONE, common areas, or any other areas it NOT permitted.
    - The field of view of any visual monitoring devices is subjected to review by *DATA*ONE Security at any time.

3.2 Evacuation Policy

Safety First
- *DATA*ONE cares about and is committed to safety. Therefore, anyone accessing the facility must comply with the evacuation policies.

Emergency Planning
- Contact the *DATA*ONE Operational personnel for any questions about site-specific evacuation procedures, routes and meeting points.
- If you have any questions regarding security or want to report a security related issue, please contact your Service Manager.

Communications During an Emergency
- Customers should listen for any announcements and follow instructions.
- Customers should evacuate immediately if they hear or see any alarms.

Access Management
- In all circumstances, *DATA*ONE, at its sole discretion, reserves the right to make the final determination about when it is safe to re-access the facility.
- *DATA*ONE will work with the appropriate local authorities or public service provider in this process.

Liability Disclaimer
- Any individual(s) refusing to leave the facility remains in the facility at their own risk.
- *DATA*ONE shall not be liable in any way for anyone who refuses to adhere to *DATA*ONE's evacuation policy.

3.3 Proof of Insurance

As required by *DATA*ONE Terms and Conditions for housing service, you must procure and maintain the following minimum insurance coverage

- Worker's compensation in compliance with all applicable laws and statues.
- Employer's Liability with limits of at least €500,000 for each accident.
- Commercial general liability with combined single limits of at least €1,000,000 each occurrence.
- "All Risk" Property insurance covering all of the Customer's personal property located in the Private Suite or Colocation Room.

In addition:

- All policies shall provide that your insures waive all rights of subrogation against *DATA*ONE.
- Customer shall furnish *DATA*ONE with certificates of insurance prior to using the space or storing equipment in the Private Suite or Colocation Room.
- Certificates shall contain a statement that the insurance coverage shall not be materially changed or cancelled without at least thirty (30) days prior written notice to *DATA*ONE.
- Your contractors are required to maintain the same types, amounts, and coverage extensions before entering the Private Suite of Colocation Room.

3.4 Maintenance and Environmental Monitoring

*DATA*ONE Maintenance responsibilities include:

- Cleaning services to service areas and corridors around Private Suites and Colocation Rooms
- Cleaning services of Colocation Rooms. Private Suites are optional on clients request
- Environmental systems maintenance
- Power plant maintenance
- Other actions that are reasonably required to maintain the colocation area.

Your maintenance responsibilities include:

- Maintaining the private suite space and/or collocation space in an hazard-free and safe condition
- Returning the private suite and/or collocation space to *DATA*ONE at the expiration of the Service Term set forth in the Customers contract in the same condition (reasonable wear and tear excepted), except as expressly started in your Customer contract.

3.5 Refuse Removal

- Large equipment boxes should be placed in the appropriate bin as dictated by *DATA*ONE personnel.
- Removing refuse is the sole responsibility of the Customer and *DATA*ONE expects Customer to maintain cleanliness and order in the Private Suite of Colocation Room.
- In terms of large suites of cabinet build-outs, Customers must arrange for their own skip or find the means to transport refuse out when no space is available for a dumpster(s).

3.6 Private Suite or Colocation Room Use

- No food, alcohol, smoking or drinks are allowed at the facilities (i.e. in the Private Suite, Colocation Rooms or the corridors).
- It is only allowed to use the space for placement and maintenance of telecommunications or computer equipment.
- Placement of equipment with antenna must be agreed with *DATA*ONE prior to deployment.
- You are not allowed to use photo or video cameras at the facilities without prior written consent from *DATA*ONE.
- **DATAONE may also terminate your use of the colocation space if you or any of your agents, suppliers or Customers are found in the Private Suite or Colocation Rooms with firearms, illegal drugs, alcohol, or are found engaging in any criminal activity, eavesdropping, illegal intelligence gathering, hacking, spamming or related activities.**
- **Persons found engaging in prohibited activities or possession of the aforementioned prohibited items, will be immediately escorted from the building/facilities.**
- Security doors and fire exits must not be left open and/or blocked under any circumstances.
- To avoid risk of fire, manuals and documents must be stored away from live equipment. No other combustible materials or any kind are allowed in the Private Suite or Colocation Rooms.

3.7 Workspace Areas and Break Room

- *DATA*ONE offers on temporary basis workspaces for Customers to use on a first come, first-served basis.
- Customers must adhere to the following guidelines.

    1. Computers are not provided and so Customers must bring their own systems.
    2. The areas are available for Customer use; but Customers are not permitted to drill, solder, or saw in these areas.
    3. These areas do not come with lockable cabinets, faxing, photocopying, or secretarial support.

- *DATA*ONE offers a break room on the first floor. This is the only area where you are allowed to consume food and drinks. No alcohol is allowed in the whole building.
- Please use these areas and room with consideration to others. You must clean them after use.

3.8 Smoking

Smoking is not allowed inside the whole building. If you want to smoke, please go outside the building (offsite).

3.9 Access Hours

- You may enter your equipment at any time (24/7 access) with a valid badge access. Delivery and removal of equipment through the loading bay is possible during office hours. Outside these hours you will need to ask for access at least 24 hours in advance. Cost will be charged.
- However, other areas inside the facilities such as storage areas, etc. are not accessible outside the office hours.
- All visitors must be issued a visitor badge and escorted at all times while inside the facility.

3.10 Bringing your Equipment to the *DATA*ONE Facility

Storing equipment

In the event that storage is needed for equipment (including prior to your space being accepted), *DATA*ONE offers colocation equipment storage if available. Follow these steps:

1. Schedule the delivery of the equipment at the loading bay by contacting *DATA*ONE at least one business day prior to delivery.
2. The loading bay is available from 8:00 to 17:00, Monday through Friday *except public holidays).
3. Please liaise with *DATA*ONE staff to determine the correct goods paths from the storage space to the destination room.
4. When we receive your equipment it will be inventorised, and stored in a secured location free of charge for maximum 10 days.
5. If you do not retrieve stored equipment within the 10-day interval, *DATA*ONE may have to return your equipment at your expense. *DATA*ONE will give you three days prior notice, if equipment needs to be returned.
6. If you need the equipment stored longer than 10 days, contact your *DATA*ONE Service Manager as soon as possible so that special arrangements can be made.

> Storage of equipment is subject to space availability.

Installing your equipment

- We can provide a work area for temporary use. You must vacate the workspace at the end of each day, and must dispose of your office refuse in designated areas before departing.
- In Colocation Rooms you are not allowed to run cable in *DATA*ONE signal and power trays.
- Return chairs to the desks before you leave the facility.
- You are not allowed to move floor tiles or attempt to penetrate the tile under cabinet(s). In a Private Suite this is not applicable.
- You should secure your own equipment before and during installation.
- We recommend that you only check out the equipment from the storage you can install in one day.
- Please notify your Service Manager if your equipment needs to be secured overnight.
- It is your responsibility to provide all installation materials for your equipment and to include items such as fuses, wire, tie wraps, labels, etc.

> *DATA*ONE is not responsible for any equipment or other personal property left in the facility.

3.11 Services from Others

- *DATA*ONE is a carrier neutral Datacenter Facility, if you would like to interconnect with any other service provider available in the facility, you as the Customer will need to provide the following information:

  - Circuit Information.
  - Design layout records to enable *DATA*ONE to make the cross-connection.
  - Prices of cross-connection are available through your *DATA*ONE Service Manager

3.12 *DATA*ONE Access to Suite or Colocation

From time to time *DATA*ONE staff may need access to a clients area so they can carry out joint periodic inspections, routine maintenance, surveys, audits and/or other standard operational work. When this is necessary, *DATA*ONE staff will give reasonable advance notice.

On some occasions *DATA*ONE staff may need immediate access to a clients area, for instance to repair a fault in an emergency, or for security reasons. When this is necessary, *DATA*ONE staff will report you they have entered your area within a reasonable time of completing their work.