

MasterDC Brno Data Center Rules and Regulations

OF MASTERDC S.R.O.

Data Center Address: Cejl 20, 602 00 Brno

1. Introductory Provisions

- 1.1. MasterDC Brno Data Center Rules and Regulations (hereinafter referred to as the „Rules and Regulations“ or the „Rules“) regulate the conditions for the movement of individuals and operation in the premises of the Data Centre operated by MasterDC s.r.o. (hereinafter referred to as the „Provider“) at Cejl 20, 602 00 Brno on the 6th and 7th floors.
- 1.2. For the purpose of these Rules, the Customer is a person or entity that has a Telecommunications Services Agreement concluded with the Provider.
- 1.3. A Visitor, for the purpose of these Rules, is either a person designated by the Customer and included in the List of Authorized Persons or a person who accompanies an authorized person.
- 1.4. Contacts to the staff of the Provider's Operations Centre:
telephone: +420 515 919 805, email: support@master.cz.

2. List of Areas Open to Visitors

- 2.1. The Data Centre open to Visitors comprises:
 - housing rooms on the 6th floor, including administration offices for customers
 - housing rooms on the 7th floor, including administration offices for customers

3. Rules for the Authorization of Persons

- 3.1. Access rights for individuals to the Technical Equipment are granted and administered by the Customer in the customer information system (admin.masterdc.com) within the “Users management” module, specifically in the “Access to DC” section. This section records the first and last names, as well as identity card or passport numbers, of persons authorized by the Customer (hereinafter referred to as the “Authorized Persons”). The Customer is obliged to keep these records up to date. For each

Authorized Person, the Customer may also specify whether the person is or is not authorized to enter the Data Center premises accompanied by another person. For persons accompanying Authorized Persons, personal data, including identity card or passport numbers, shall be recorded by the Provider's Operations Centre staff at the time of authorization.

- 3.2. Only Authorized Persons with valid authorization in the "Access to DC" section, or persons accompanying them (see clause 3.1), are permitted to access the Data Center. Any breach of these rules may result in termination of the contract by the Provider.
- 3.3. The Customer is obliged to ensure that all persons granted access to the Data Center are familiar with these Rules and Regulations. The Customer shall be liable for their actions and behavior, or for any damage they may cause

4. Access to the Data Center

- 4.1. The Data Center is open to Visitors nonstop (24 hours a day, 7 days a week, 365 days a year).
- 4.2. Visitors must first report to the reception of Kovoterm, Cejl 20.
- 4.3. When entering the Data Center, Visitors are required to authorize themselves. As part of this process, the Provider's Operations Centre staff verify the data from ID cards or passports against the information recorded in the customer administration system in the „Users management“ module, specifically in the „Access to DC“ section. For persons accompanying the Authorized Persons, these details are recorded at the time of authorization.
- 4.4. If a Visitor does not have valid authorization in the "Access to DC" section or is not accompanying an Authorized Person who is permitted to enter the Data Center accompanied by another person, the Visitor will not be allowed to enter the Data Center.
- 4.5. After authorization, the staff of the Control Center will admit the Visitor to the housing area reserved to them. If the equipment is locked in a lockable box or rack and the Visitor lacks the assigned keys, the Visitor is required to contact the staff of the Provider's Control Center by telephone, and their technology will be made available to them on request after re-verification of their authorization to access.
- 4.6. Before entering the premises of the Data Center, the Visitor is obligated to put on protective shoe cover which is available in the access room or at the entrance to the Data Center.

- 4.7. In areas where Technical Equipment is placed, the Visitor can perform only activities to which they are authorized under the Agreement.
- 4.8. A Visitor's movement within the Data Center is monitored by cameras operated by the Provider's staff. By entering a visibly marked video surveillance zone, the Visitor automatically consents to the recording of their image and activities by the Provider. Taking photographs or making video recordings by Visitors is prohibited without the Provider's prior written consent.
- 4.9. In the event that the Visitor wants to take away their Technical Equipment, they are required to report this fact in advance to the staff of the Control Center who will ensure that a Technical Equipment Taking Out Report is drawn up.
- 4.10. The Visitor is authorized to access their Technical Equipment in the Data Center or take away their Technical Equipment from the Data Center only if all their obligations towards the Provider have been settled.
- 4.11. It is prohibited to leave any Technical Equipment in the common area of the Data Center. The Visitor is obligated to dispose of any waste from assembly material (scraps of wire, packaging, etc.) in the respective containers.
- 4.12. It is prohibited to enter the Data Center with food, beverages, animals, bulky luggage or with weapons, flammables, explosives or other dangerous objects and substances.
- 4.13. Any person whom the Provider suspects to be under the influence of alcohol or other intoxicating substances shall not be admitted into the Data Center.
- 4.14. Smoking and use of open fire is strictly prohibited throughout the entire premises – the Kovoterm building.
- 4.15. The premises of the Data Center are fitted with an inert gas fire suppression system. If activated gratuitously, compensation for damages will be claimed from the Customer.
- 4.16. The Visitor may remain in the premises of the Data Center only for the time necessary to perform the work to which the Visitor is authorized under the Agreement.
- 4.17. The Visitor is obligated to notify the staff of the Control Center of their departure from the Data Center.
- 4.18. In accordance with the Agreement, the Customer has the right to a remote restart of their device on request by telephone, after proper authorization (with a password), or directly from their account in the customer information system. The restart is normally performed by interrupting power supply to the Server. At the express request of the Customer, the Reset button can be used. Unless the Server controls are adequately accessible and clearly marked, the reset will not be performed.
- 4.19. Other rights and obligations of the Customer are defined in the Agreement and all its parts.

5. Use of Shared Resources

- 5.1. In the Data Center, Customers have at their disposal at least one movable monitor and keyboard (console), and in the administration room there is a stable monitor and keyboard. Measuring instruments and other devices necessary for maintenance service can be connected only to dedicated electric sockets separate from the main backed up power circuits.
- 5.2. A console forms an inseparable set of equipment, and it is prohibited to move the accessories between individual consoles.
- 5.3. In case of failure of the given equipment the Customer is obligated to immediately inform the staff of the Provider's Control Center.
- 5.4. All Visitors to the Data Center are entitled to use the shared resources.
- 5.5. Should the Customer need to perform time-consuming modifications to their equipment directly in the Data Center, it is necessary to notify the Provider one working day in advance. In this case, the Provider shall provide a monitor and keyboard for their use only.
- 5.6. You can use a public Wi-Fi network to connect your laptop in the Data Centre (SSID: "MAI-PUBLIC", password "MasterDCWiFi") or the installed Ethernet wall sockets.

6. Rules for Placing Customer Servers

- 6.1. The Customer can place their Server only after signing the Agreement and reporting the installation to an authorized employee of the Provider.
- 6.2. The Server must be placed in a location that has been assigned to the Server by an employee of the Provider. Any change of location is possible only after prior written (including email or SMS) agreement with the Provider.
- 6.3. Server must be labelled visibly with a tag. The Customer will receive the tag during the installation of the Server. In the event that the Customer does not receive the tag, or if it is damaged, the Customer shall label the server with the assigned IP address. The Customer shall then notify the Provider of this fact in writing.
- 6.4. The Visitor is allowed to install new Technical Equipment in shared rack cabinets or shelves only after prior agreement with the employee designated by the Provider.
- 6.5. It is strictly forbidden to install cabling outside the technological space defined by the Agreement.
- 6.6. Technical Equipment (placed in shared rack cabinets or shelves) are subject to the Provider's control measurement before their new installation or change of hardware. If

limit values determined by the standard ČSN 331600 ed.2 are exceeded, Revision Report will be required from the Customer.

7. Network Security

- 7.1. In shared segments on their Servers the Customer is allowed to use only the IP address space assigned by the Provider's personnel. It is not permissible to use any other IP addresses, network masks or private IP ranges. Any changes to the Ethernet segment are being recorded and archived.
- 7.2. Violation of this rule will result in deactivation of the corresponding port on the switch of the Provider.
- 7.3. The Provider is entitled to immediately disconnect a Server threatening the Provider's infrastructure by its behavior (there is a zero tolerance approach to DOS attacks in particular), spamming or seeking to discredit others.
- 7.4. It is not allowed to launch a DHCP server or IPv6 RA in shared segments.
- 7.5. For the purpose of managing their equipment, the Customer can install their own Wi-Fi access point after the approval of the competent employee of the Provider. This access point may not be publicly available and must not interfere with the Provider's Wi-Fi zone.
- 7.6. It is prohibited to use the assigned address space outside the processing area of the Provider, except exceptions approved in writing.

8. Final Provisions

- 8.1. By entering the premises of MasterDC Data Center, the Visitor is bound by these Rules and Regulations.
- 8.2. These Rules and Regulations can be amended by the Provider. The current version of the Rules is also available at the entrance to the Data Center.
- 8.3. These Rules and Regulations come into force on 1st June 2026.