Master DC Prague Data Centre Rules and Regulations

of Master Internet, s.r.o.

Data Centre Address: Kodanska 46, Prague 10, 100 10

1. Introductory Provisions

1.1. Master DC Prague Data Centre 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 Master Internet, s.r.o. (hereinafter referred to as the "Provider") at Kodanska 46, 110 10 Prague 10 on the 1st floor.

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. Rules for the Authorization of Persons

2.1. "List of Authorized Persons" is a list containing the names and numbers of identity cards or passports of persons who were appointed by the Customer to access the Technical Equipment. The Customer is obligated to keep this List up to date. For each of the Authorized Person Customer can specify whether a person is or is not entitled to enter the premises of the data center with another people. For persons accompanying the Authorized Persons, personal data, including the number of the identity card or passport, will be registered by the staff of the Control Center at the time of authorization.

2.2. Only persons included in the List of Authorized Persons or persons accompanying them (see point 2.1.) shall have access to Data Centre; any violation of these Rules may result in the withdrawal from the Agreement on the part of the Provider.

2.3. The Customer is obligated to acquaint all persons who were provided access to the Data Centre with these Rules and Regulations. The Customer shall be liable for their actions and behavior, or for any damage they may cause.

3. Access to the Data Centre

3.1. The Data Centre is open to visitors nonstop (24 hours a day, 7 days a week, 365 days a year).

3.2. When entering the Data Centre, Visitors are required to authorize themselves. Employees of the Control Center check the data from ID cards or passports with the List of Authorized Persons. For persons accompanying the Authorized Persons, they record this data at the time of authorization.

3.3. If a Visitor is not on the List of Authorized Persons, or does not accompany the Authorized Person who may enter the data center with another person, they will be denied access to the Data Centre.

3.4. After authorization, the staff of the Control Centre will admit the Visitor to the housing area reserved to them.

3.5. Before entering the premises of the Data Centre, the Visitor is obligated to put on protective shoe cover which is available in the access room or at the entrance to the Data Centre.

3.6. In areas where Technical Equipment is placed, the Visitor can perform only activities to which they are authorized under the Agreement.

3.7. The movement of Visitors in the Data Centre is monitored by cameras that monitor the Provider's employees. By entering a visibly marked video capture zone, the Visitor automatically agrees with collecting the video of his person and acts by the Provider. Without the prior written consent of the Provider, photography or video recording by Visitors is prohibited.

3.8. 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 Centre who will ensure that a Technical Equipment Taking Out Report is drawn up.

3.9. The Visitor is authorized to access their Technical Equipment in the Data Centre or take away their Technical Equipment from the Data Centre only if all their obligations towards the Provider have been settled.

3.10. It is prohibited to leave any Technical Equipment in the common area of the Data Centre. The Visitor is obligated to dispose of any waste from assembly material (scraps of wire, packaging, etc.) in the respective containers.

3.11. It is prohibited to enter the Data Centre with food, beverages, animals, bulky luggage or with weapons, flammables, explosives or other dangerous objects and substances.

3.12. Any person whom the Provider suspects to be under the influence of alcohol or other intoxicating substances shall not be admitted into the Data Centre.

3.13. Smoking and use of open fire is strictly prohibited throughout the entire premises – building 4D.

3.14. The premises of the Data Centre are fitted with an inert gas fire suppression system. If activated gratuitously, compensation for damages will be claimed from the Customer.

3.15. The Visitor may remain in the premises of the Data Centre only for the time necessary to perform the work to which the Visitor is authorized under the Agreement.

3.16. The Visitor is obligated to notify the staff of the Control Centre of their departure from the Data Centre.

3.17. 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.

3.18. Other rights and obligations of the Customer are defined in the Agreement and all its parts.

4. Use of Shared Resources

4.1. In the Data Centre, 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.

4.2. A console forms an inseparable set of equipment, and it is prohibited to move the accessories between individual consoles.

4.3. In case of failure of the given equipment the Customer is obligated to immediately inform the staff of the Provider's Control Centre.

4.4. All Visitors to the Data Centre are entitled to use the shared resources.

4.5. Should the Customer need to perform time-consuming modifications to their equipment directly in the Data Centre, 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.

4.6. You can use a public Wi-Fi network to connect your laptop in the Data Centre (SSID: “MAI-PUBLIC”, password "MasterDCWiFi").

5. Rules for Placing Client Servers

5.1. The Customer can place their Server only after signing the Agreement and reporting the installation to an authorized employee of the Provider.

5.2. 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.

5.3. 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 Client does not receive the tag, or if it is damaged, the Client shall label the server with the assigned IP address. The Client shall then notify the Provider of this fact in writing.

5.4. 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.

5.5. It is strictly forbidden to install cabling outside the technological space defined by the Agreement.

5.6. 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 Client.

6. Network Security

6.1. 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.

6.2. Violation of this rule will result in deactivation of the corresponding port on the switch of the Provider.

6.3. 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.

6.4. It is not allowed to launch a DHCP server or IPv6 RA in shared segments.

6.5. 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.

6.6. It is prohibited to use the assigned address space outside the processing area of the Provider, except exceptions approved in writing.

7. Final Provisions

7.1. By entering the premises of Master DC Data Centre, the Visitor is bound by these Rules and Regulations.

7.2. 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 Centre.

7.3. These Rules and Regulations come into force on 9th September 2020.