DATA CENTER OPERATING RULES

Article 1
Introduction

(1) The Operating Rules are binding on all persons who enter the premises of the Data Center or move within these premises, and these persons are obliged to comply with the Operating Rules. The Customer is obliged to familiarize the employees of the Customer or a Third Party with the Operating Rules.

(2) The purpose of the Operating Rules is, in particular, to protect the data and equipment of Customers, Third Parties and the Provider by controlling physical access to areas where data and equipment are stored.

Article 2
Terminology

The following capitalized terms, when used in the Operating Rules, shall have the meaning assigned to them below.

Access List of Authorized Persons	shall mean a list containing the data of Authorized Persons specified by the Provider. Both the Provider and the Customer are obliged to keep this list up to date.
Authorized Person	shall mean a person (an employee of the Customer, Third Party or Provider, or another person who provides services to them) who has been authorized, as specified by Article 3 of the Operating Rules, and placed by the Provider, for example on the Customer's instruction, on the Access List of Authorized Persons.
BIO	shall mean a scan of the palm vein pattern. Wherever BIO is stated in the Operating Rules, the rule relating to BIO shall only apply if BIO is installed in the respective Data Center.
Customer	shall mean a party who is in a contractual relationship with the Provider, whereas the Provider is entitled to allow the Customer (based on such contractual relationship) to place the Customer's and/or Third Party's equipment in the Data Center and/or to provide the Customer or Third Party with services related to the supplies under mutually concluded contracts.
Data Center	shall mean the Provider’s relevant data center.
Data Room	shall mean a defined space in the Data Center marked as a data room, with secured access, in which, in particular, the equipment of the Customer or Third Parties is located.
Operating Rules	shall mean these operating rules issued by the Provider and laying down binding rules, conditions, procedures and behavior related to the operation and protection of the Data Center, and regulating the rules on access, conditions for entry or movement within the premises of the Data Center.
Provider	shall mean CETIN a.s., having its registered office at Českomoravská 2510/19, Libeň, Postcode: 190 00, Prague 9, ID No. (IČO): 04084063, Tax ID No. (DIČ): CZ04084063, registered in the commercial register administered by Municipal Court in Prague, Section B, Insert 20623.

Security Monitoring Service	shall mean a monitoring service ensuring continuous security surveillance of the Data Center, in particular checking the authorization to access the Data Center, authorizing persons as stated in Article 3 of the Operating Rules, material, ensuring the overall physical security of the Data Center, etc.
Technical Monitoring Service	shall mean the Provider's monitoring service ensuring continuous operation of Data Center equipment, receipt of requests from the Customer and/or Third Parties and dealing with requests in cooperation with Customers, Third Parties and its own specialized departments.
Third Party	shall mean a party who is in a contractual relationship with the Customer. Employees of the Third Party may be authorized by the Provider based on the Customer's request.
Visitor	shall mean any person to whom the Provider grants a one-time authorization, as stated in Article 3 of the Operating Rules, and who is allowed by the Provider to enter the Data Center; a Visitor may be, for example, an employee of the Provider or a contractual partner of the Provider different from the Customer (a supplier), an employee of the Customer, an employee of a Third Party, of the company, or a person providing a one-time service to one of the above-mentioned parties.

Article 3
Authorization for the Provider's Employees, Customers, Third Parties and Visitors

(1) Within the authorization process, contactless access cards are issued and activated, a PIN is generated and/or BIO is obtained, for Authorized persons in order to enable their access the Data Center. Persons are authorized based on the Customer's request. Authorized persons are obliged to immediately report the loss or theft of the contactless access card to the Security Monitoring Service, which will block, replace the access card, or generate a new PIN.

(2) Visitors are always checked in and granted a one-time authorization upon presentation of an identity card, passport or confirmation of permanent residence in the Czech Republic, including the acquisition of BIO, by the Security Monitoring Service.

(3) A person who does not present its personal documents (ID card, passport or conformation of permanent residence in the Czech Republic), even at the request of the Security Monitoring Service, will not be allowed to enter the Data Center.

(4) The Customer is obliged to notify the Provider immediately in electronic form (e.g. via e-mail or access security system to the relevant contacts listed below) that a particular Authorized Person of the Customer or a Third Party should no longer be allowed to access the Data Center. Based on the Customer's instruction, the relevant Authorized Person will be removed from the Access List of Authorized Persons. The Provider is entitled to remove the Authorized Person from the Access List of Authorized Persons.

Article 4
Access to the Data Center

(1) Only Authorized Persons and Visitors may access the Data Center.

(2) The Data Center is accessible for Authorized Persons and Visitors 24 hours a day, 7 days a week.

Authorized Persons

(3) Authorized Persons equipped with contactless access cards and PIN enter the Data Center building after authentication and entering the PIN in the entrance reader in front of the Data Center entrance door.

(4) Authorized Persons must first report to the Technical Monitoring Service and provide the reason for their visit to the Data Center before starting any work in the Data Center. An exception to the rule stated in the previous sentence applies only to persons who have a permanent place of work in the Data Center, i.e. they have the right to use the office space under a contract entered into with the Provider.

(5) Authorized Persons equipped with contactless entry cards, PIN and, if applicable, BIO, enter through the entry filter (turnstile entry system/rotary turnstile), if installed in the Data Center, and only with any hand luggage that allows smooth passage through the turnstile system (with size corresponding to, for example, a backpack or bag for a 15.6" diagonal laptop) so as not to damage the interior of the entry filter. Baggage larger than hand luggage is checked in by the Security Monitoring Service. The Security Monitoring Service may prohibit entry through the entry filter with oversized luggage, material, or equipment.

(6) After authentication has been successfully carried out, Authorized Persons are allowed to access other areas of the Data Center. The other areas of the Data Center contain other security devices that allow access to individual rooms and the Data Rooms. Authorized Persons or Visitors may be asked at any time by the Security Monitoring Service to present personal documents to check their identity. Without successful authentication, all other entry filters are inactive.

(7) Before an Authorized Person leaves the Data Center, an employee of the Provider is entitled to visually inspect the condition of the premises in the Data Center, which this Authorized Person entered before leaving. If the Provider's employee decides to carry out this inspection, he/she shall immediately inform the relevant Authorized Person who is obliged to wait until the inspection has been carried out, or a record of the findings has been made, before leaving the Data Center. If the inspection reveals any damage to the Data Center premises, which the Authorized Person entered, to the equipment located there, or violation of the provisions of these Operating Rules by the Authorized Person, the Provider's employee shall make a written record of this, a copy of which will be provided to the Authorized Person and to the Customer. The Authorized Person present in the Data Center is obliged to follow the instructions of the Provider's employees, in particular, regarding cleanliness and order in the premises of the Data Center.

(8) In the event of a malfunction of the access card, PIN or BIO, Authorized Persons will be admitted to the Data Center upon presentation of an identity card, passport or confirmation of permanent residence in the Czech Republic to the Security Monitoring Service and after a subsequent check whether these persons are on the Access List of Authorized Persons. Then Authorized Persons will be let into the Data Center building behind the entry filter, where they will be received by a representative of the Technical Monitoring Service and accompanied to the area in question.

Visitors

(9) Visitors may enter the Data Center provided that an electronic request for entry in accordance with the template of the written notification of a visit to the Data Center (see the attachment to the Operating Rules entitled “Template of the Written Notification of a Visit to the Data Center”) was sent to and approved by the Provider in advance. The request shall be submitted by the Customer always at least 48 hours in advance to the Technical Monitoring Service. The Provider shall decide on the request within 24 hours of its receipt. If the request is sent to the Technical Monitoring Service less than 48 hours in advance, entry shall be subject to approval by the Data Center Administrator or the Data Center Operations Manager. After having received consent to enter the Data Center, the Visitor will be checked in by the Security Monitoring Service. The purpose of this measure is to prevent a large number of people being present in the Data Center. The obligation to make a prior request according to the first sentence of this paragraph does not apply to the Provider's employees.

(10) Visitors shall report their arrival to the Security Monitoring Service using the entrance communication terminal or the doorbell located in front of the entrance to the Data Center.

(11) The Security Monitoring Service will provide Visitors with everything necessary to enter the Data Center following the identity check and their registration in the Provider's access system – i.e. issuance of temporary visitor contactless access cards for temporary access, and possibly PIN or BIO.

(12) If a visit is not announced in advance to the Technical Monitoring Service and subsequently confirmed, the Security Monitoring Service will not allow such person to enter the Data Center.

(13) Visitors then proceed in the same way as Authorized Persons equipped with contactless access cards, except that upon leaving the Data Center, Visitors must return their contactless access cards to the Security Monitoring Service. To enter the Data Rooms, Visitors must be accompanied by an Authorized Person or an Authorized Person of the Provider, if requested in advance in the request for access. BIO will be automatically terminated at the next 00:00 o'clock, or according to the expected departure (depending on the work performed) communicated to the Technical Monitoring Service in the notification sent according to paragraph (9) above.

Keybox

(14) The Customer can rent an unattended keybox in the Data Center - a box for storing keys to equipment ("**Keybox**"). Access to the relevant Keybox is only possible with a contactless access card. Access to the Keybox is continuously monitored and the usage of the Keybox is recorded.

Joint Provisions

(15) In the event of a threat to the life or health of persons present in the Data Center and in order to eliminate such a threat and mitigate the risks, the Provider is entitled to close (disallow access to) the Data Center premises or, as appropriate, request that persons leave these premises immediately or enforce such departure. The Provider is also entitled to take appropriate action in order to protect the health of the persons present within the premises of the Data Center (e.g. measuring body temperature) and to require such persons to declare their stay in high-risk areas (e.g. in connection with an epidemiological situation).

Article 5
Moving around the Data Center

(1) All personnel of the Customer or Third Parties can move or stay in the Data Center only in the manner and for the time strictly necessary to perform work on the equipment they are authorized to handle or to carry out other activities under contracts with the Provider or the Customer if these are not in conflict with the contract between the Customer and the Provider.

(2) Each person present at the Data Center must carry an access card attached visibly to its clothes.

(3) In the event of adverse conditions (e.g. rain, snow) outside the Data Center, all persons are obliged to use protective footwear/shoe covers, if available.

(4) Within the Data Room in which the Provider provides services to the Customer in order for the Customer to further provide these services to one Third Party, the Authorized Person of such Third Party may move or stay at this Data Room without being accompanied by the Customer's Authorized Person.

(5) Within the Data Room in which the Provider provides services to the Customer in order for the Customer to further provide these services to two or more Third Parties, the Authorized Persons of the Third Parties may move or stay at this Data Room only when accompanied by an Authorized Person of the relevant Customer. However, if the Customer submits to the Provider an electronic request that a certain Authorized Person of a Third Party shall be allowed to move or stay within a designated Data Room unaccompanied by the Customer's Authorized Person, and the Provider approves such request, the Third Party's Authorized Person specified in the Customer's request will be allowed to do so. If the Provider does not approve such a request, Provider shall inform the Customer of such non-approval without undue delay, stating the reason for such non-approval.

(6) Visitors may move or stay within the premises of the Data Center and Data Rooms only if accompanied by the relevant Authorized Persons and in accordance with the instructions given by the Provider's employees and according to the Operating Rules. Authorized persons bear full liability for all activities or behavior of Visitors accompanied by them, as well as for any harm or damage caused by them.

(7) The movement of all persons present in the Data Center is subject to camera surveillance which is monitored by the Provider's employees. The surveillance recordings are stored by the Provider, as the administrator of the camera surveillance system, for a period of 30 (thirty) calendar days.

(8) Authorized Persons of the Customer or Third Parties or Visitors must refrain from manipulating with the raised (doubled) floor of the Data Center premises, i.e. to open it or enter the space in the raised (doubled) floor, and in particular they must not interfere in any way with the systems installed in the Data Center premises (cabling, power supply, etc.) or in any way manipulate with or disrupt or influence other equipment of the Provider, other Customers or Third Parties without an express instruction from the Provider.

(9) Authorized Persons of the Customer or Authorized Persons of a Third Party may operate connections between individual racks within one Data Room provided that connections are placed in cable trays that are exclusively dedicated to this Customer or this Third Party or above individual racks, and also provided that such Authorized Persons of the Customer or of the Third Party have the necessary qualifications required for such activity. Every day after the work has been ended, the Authorized Persons shall report the performance of such work to the Technical Monitoring Service and they shall carry out a joint inspection of the area.

(10) Items that are not necessary to perform the work which the Customer's Authorized Persons and Third Party’s Authorized Persons are authorized to carry out must be deposited in the area designated by the Provider.

(11) The entry and movement of persons under the age of 15 is prohibited in the entire Data Center building. It is forbidden to enter any part of the building with animals or with weapons, flammables, explosives or other dangerous objects or substances. It is forbidden to enter the premises of the Data Room or other technological rooms with food or drinks.

(12) Smoking as well as the handling of naked flame is prohibited in the entire Data Center building.

(13) Taking photos, making video recordings or other recordings without the prior written or electronic consent of the Provider is prohibited in the entire building of the Data Center. The resulting recording must be submitted to and approved by the Provider.

(14) Any persons entering the Data Center who the Security Monitoring Service staff reasonably believe are under the influence of alcohol, drugs or other intoxicating substances will not be admitted to the Data Center premises. The non-admission of these persons to the Data Center must always be recorded in the Provider’s daily Security HELP report.

(15) Any persons present in the Data Center who the Security Monitoring Service staff reasonably believe are under the influence of alcohol, drugs or other intoxicating substances will be ordered to leave the Data Center premises. The expulsion of these persons from the Data Center premises must always be recorded in the Provider’s daily Security HELP report.

(16) Any persons present in the Data Center must not in any way endanger or disrupt the operation of the equipment located in the Data Center or in the Data Room(s).

Article 6
Occupational Safety and Health and Fire Safety

(1) The Customer is obliged to demonstrably familiarize the employees of the Customer and the Third Party with the fire and safety regulations provided to the Customer by the Provider in advance, as well as with the regulations arising from the contractual relationship between the Provider and the Customer, and the employees of the Customer and Third Parties are obliged to comply with the instructions set out in these fire and safety regulations, the regulations arising

from the contractual relationship between the Provider and the Customer, and the Operating Rules.

(2) The Provider is not liable for any injury, harm or other damage to the health of Authorized Persons of the Customer or Third Parties or Visitors present in the Data Center, which result from (i) their failure to comply with generally applicable and effective regulations or, as appropriate, rules on safe conduct, (ii) their violation of laws or other regulations aimed at ensuring occupational safety and health (OSH), (iii) the Operating Rules, (iv) the fire and safety regulations, which were provided to the Customer by the Provider, or (v) other rules or regulations that persons present in the Data Center are obliged to adhere to. Furthermore, the Provider is not liable if such injury, harm, or other damage to health occurs as a result of these persons consuming alcoholic beverages or addictive substances.

(3) All persons present in the Data Center are obliged to report to the Technical Monitoring Service staff or the Provider's representative any deficiencies or defects found by them at the workplace, or the performance of any activities or work that could endanger occupational safety or health and, to the extent possible, actively participate in the rectification thereof. Furthermore, all persons present in the Data Center are obliged to immediately notify the Provider's employees of any injury they suffer, if their health condition allows it, or any injury to another person which they have witnessed, and to actively cooperate in investigating its causes.

Article 7
Installing and Uninstalling Equipment

(1) Delivery of any equipment, its installation or a change in the installation or uninstallation of any equipment of the Customer or a Third Party must be notified by such Customer to the Technical Monitoring Service in advance, together with the date of implementation.

(2) If it is not urgent necessary maintenance work, the Customer is obliged to notify the Technical Monitoring Service of the intention of performing activities stated in the previous paragraph, in electronic form, at least 3 (three) business days in advance and if a larger number of devices is to be installed (i.e. devices with total power input of at least 10 kW), the Customer is obliged to notify and consult such intention with the Provider’s relevant employees at least 3 (three) calendar weeks in advance. This rule shall also apply in a situation where it is necessary to take away or remove equipment from the Data Center. The Technical Monitoring Service must process the request and respond electronically to the Customer within 24 (twenty-four) hours. If it is not possible to comply with the date requested by the Customer, the Customer shall agree with the Provider on another suitable date.

(3) The Customer is obliged to provide the Provider with the exact technical parameters of the equipment installed, such as electrical power input, dimensions and weight of the equipment, thermal output of the equipment, required air flow, and - last but not least - a unique identifier of the equipment (type and serial number), unless otherwise agreed in writing between the Provider and the Customer in a specific case.

(4) Requirements for increased electrical power input of the power supply or any other special requirements shall be stated by the Customer in sufficient time in advance to allow for the relevant adjustments to be made before the equipment is installed. Subsequent power supply adjustments are usually made when the equipment is turned on, unless it is necessary in a specific case to make such an adjustment when the equipment is turned off, in which case the Customer runs the risk of outage and shall bear sole and full liability for the outage.

(5) Floor Management or, in other words, the rules for the placement of the Customer's or Third Party's equipment, is within the competence of the Provider's employees, whereas in areas that are intended for exclusive use by the Customer or Third Parties, the Customer or the Third Party is obliged to consult the Provider about the Floor Management in advance and agree on it with the Provider; shared competence between the Customer and the Provider is possible solely on the basis of a written agreement between the Customer and the Provider contained in a contract the subject of which is the provision of Data Center services by the Provider to the Customer. The placement of the Customer's equipment in the Data Rooms within the Data Center is always subject to prior approval of the Provider, unless otherwise expressly stated in writing in the contract between the Provider and the Customer.

(6) The Security Monitoring Service staff shall ensure the drafting, signing and handing over of written reports on the receipt/issuance of equipment/material of the Customer or a Third Party (see the template in the Operating Rules). The written report shall contain the signatures of representatives of the Security Monitoring Service and the Technical Monitoring Service and a representative of the Customer or Third Party. The record-keeping regarding the written report may be regulated by the relevant regulations or an internal guideline, as well as by the Operating Rules. The Provider may grant any exceptions to this provision based on a written agreement with the Customer.

(7) Any movement of material or equipment belonging to the Customer or a Third Party (delivery, removal) is subject to approval by the Technical Monitoring Service and shall take place in a designated area (unpacking room), unless expressly agreed otherwise between the Provider and the Customer.

(8) It is forbidden to unpack equipment in the Data Rooms. Equipment may only be unpacked in a designated area (unpacking room), unless expressly agreed otherwise between the Provider and the Customer. All packaging and waste materials must be (i) removed by the Customer or Third Party on the respective business day or, at the latest, the next business day, or (ii) in the case of municipal-like waste disposed of by the Customer or Third Party in waste containers according to the type of waste (unsorted, paper and cardboard, plastic).

Article 8
Use of Shared Assets

(1) In the Data Center, Authorized Persons or Visitors are allowed to use a monitor, keyboard, mouse and a basic set of tools and screws on the mobile cart ("**Shared Assets**"). The Shared Assets that can be borrowed are primarily located in the Technical Monitoring Service room.

(2) All Authorized Persons or Visitors are allowed to use the Shared Assets.

(3) If the Shared Assets are needed by other Authorized Persons or Visitors and the Shared Assets have already been used for a continuous period of more than 30 (thirty) minutes, the right to use the Shared Assets immediately passes to other Authorized Persons or Visitors in the queue.

(4) If Authorized Persons or Visitors need to carry out longer-lasting work on the Customer's or Third Party's equipment directly in the premises of the Data Center, they shall notify the Provider's employees or the continuous Technical Monitoring Service of such work at least 3 (three) business days in advance. In such a case, the Provider shall provide such Authorized Persons or Visitors with a monitor, keyboard and mouse for their use only.

(5) The Provider's employees are entitled to order the transfer of the Customer's equipment for modifications to a room designated by the Provider for remote installation and configuration of the equipment, if available.

Article 9
Personal Data Processing

The conditions for processing personal data in connection with the entry and movement of Authorized Persons or Visitors in the Data Center and/or the provision of services that are directly related to supplies under mutually concluded contracts, including the scope of the data subject's special rights, are set out in the Privacy Policy available at https://www.cetin.cz/zasady-ochrany-osobnich-udaju.

Article 10
Contacts:

Data Center - DC Chodov:

Name:	Phone	E-mail
Technical Monitoring Service	+420 725 135 576	dc.chodov@cetin.cz
Security Monitoring Service	+420 606 395 939	FO_AB.Chodov@cetin.cz
Termination of access to the Data Center	+420 601 102 773	jan.simonovsky@cetin.cz

Data Center - DC JZM:

Name:	Phone	E-mail
Technical Monitoring Service	+420 702 225 887	dc.jzm@cetin.cz
Security Monitoring Service	+420 702 275 255	jzm.foab@cetin.cz
Termination of access to the Data Center	+420 601 102 773	jan.simonovsky@cetin.cz

Article 11
Annexes:

- Template of the written notification of a visit to the Data Center
- Template of the written report on receipt/issuance of equipment/material in the Data Center

Article 12
Final Provisions

(1) The Provider is entitled to change and/or adjust the Operating Rules. All modifications to the Operating Rules will be announced by the Provider 1 (one) month before the change takes effect, in a suitable form, for example by notification on the Provider's website, a notice in the Data Center premises, or by using another suitable method. The currently valid and effective Operating Rules are available in the entrance area of the Data Center.

(2) The Operating Rules shall enter into force and effect on 1.1.2024.

Annexes

Template of the written notification of a visit to the Data Center

Request for permission for a Visitor to enter and drive in: DC XXX

Date, time of probable entry and duration of stay in the DC	Day month year, hour:minute o'clock, approximately X hrs
Reason	XXX
Organization/company/	XXX
Requested area/site	Example: Data Room No. X/ Room No. X

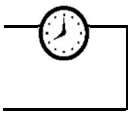
First name, Last name	Date of birth	ID card number	Company		
Pavel Novák	1.1.2020	XXXXXXXX	XXX		
Petr Novák	2.1.2020	XXXXXXXX	XXX		
Authorized contact person for confirmation of access:			**Jan Novák**	Phone number: XXXXXX XXX	E-mail: XXX@XXX.XX

Vehicle make	License plate	Vehicle make	License plate
Škoda Octavia	XXX		

Place and date of writing the request form: Prague, XX.XX.XXX

First name and last name of the requesting person of the Authorized person Jan Novák

Template of the written report on receipt/issuance of equipment/material in the Data Center

Incoming	Outgoing			

Name of equipment	Serial number (if identifiable)	Quantity	Name or personal number	Name of the Customer/company	Date	Signature

Reviewed by:
Date:
Signature: