

## JSC BALTNETOS KOMUNIKACIJOS

### RULES FOR THE PROVISION OF THE SERVER COLOCATION SERVICE

#### 1. DEFINITIONS

##### 1.1 Data centre (DC)

The Baltmeta-owned, specially equipped facilities located at 160c Liepkalnio Str., Vilnius.

##### 1.2 Tier 3 DC

The data centre located at 160c Liepkalnio Str., Vilnius that complies with the Tier 3 data centre requirements as specified in the TIA-942 standard.

##### 1.3 Colocation

Placing the Client's IT hardware in Baltmeta's data centre, which includes providing Internet access and ensuring cooling and power supply.

##### 1.4 UPS

An uninterruptible power supply device.

##### 1.5 PDU

A power distribution unit mounted in a server rack.

##### 1.6 The Client's authorised representative

An employee of the Client or other company (who installs, integrates, and/or maintains the hardware) whom, in accordance with this agreement, the Client grants the full right to manage the Client-owned IT hardware.

##### 1.7 Third parties

Any other representatives of the Client who are not listed in this agreement.

##### 1.8 Dedicated rack

A server rack rented and used by a single client only.

##### 1.9 Shared rack

A server rack used by multiple clients who rent different parts of it.

#### 2. ACCESS TO THE DATA CENTRE AND THE CLIENT'S RESPONSIBILITIES

##### 2.1 The Client's authorised representatives

Only the persons listed in this agreement may access the Client's hardware placed in the DC. By signing this agreement, those persons undertake to follow the set procedure during their visits to the DC.

In the event that the Client terminates its cooperation with the responsible person, which includes but is not limited to terminating his/her employment contract, the Client shall inform the Baltmeta about this as soon as possible. Otherwise, Baltmeta shall not be liable for any damage incurred by the Client in relation to the responsible person.

In the event that a third party arrives together with the responsible persons to visit the DC, the Client shall be fully liable for all actions of the third party and their consequences.

##### 2.2 Registration

The Client must register for access to the DC in one of the following ways:

- by sending an email to patekimas@balt.net;
- by making a phone call to +370 700 800 88;
- by filling out a registration form in the Client Area.

A request for registration shall be accepted only if it comes from an email address or a phone number included in the contact information of the listed responsible persons. A request for registration must be submitted at least 24 hours prior to the visit.

During registration, the Client must specify the purpose of the visit (for example, new hardware installation, part replacement, hardware unmounting, etc.).

##### 2.3 Urgent access

The Client may gain urgent access in the event of a failure of the Client's IT hardware. In this case, the Client must register by making a phone call to +370 700 800 88.

While new hardware is being mounted or unmounted, the Client may not gain urgent access to the DC.

#### **2.4 On arrival**

Having arrived at the DC's premises, the Client's authorised representative shall talk to the security post via a remote communication device. The representative shall communicate to the security officer the purpose of the visit and which persons (and of which company) have arrived.

If the security officer has no information about the visit, the gates shall not be opened.

Having entered the premises, the car shall be left in the guest parking area. It shall be prohibited to attempt to enter any other areas.

#### **2.5 Documents produced on arrival**

Where the Client's representative arrives at the DC for the first time, his/her biometric data shall be added to the database, using an electronic fingerprint reader. Where the representative arrives for the first time, he/she must also produce a photo identity document.

On any subsequent visit, a security officer shall ask the representative to scan his/her fingerprints. No identity document shall be required.

#### **2.6 Access control cards and passwords**

Provided that the Client's representative is registered, a security officer shall issue him/her an access card; when leaving the DC's premises, the representative must return the card to the security service.

The card shall be non-transferable and may be used only by the person whom it was issued to.

#### **2.7 The Client's representatives' work at the DC**

In the event that the physical work on the Client's server is expected to last for over 1 (one) hour, the Client must remove the server from the server colocation room and move it to the server workroom, continuing the work there.

#### **2.8 Prohibited behaviour and liability for it**

At the DC, the Client may not carry out works that are not related to the Client's hardware (cable switching, the introduction of alternative power sources, etc.).

At the DC, it shall be strictly prohibited to take photos, use video-recording equipment and attempt to establish an unauthorised connection with infrastructure hardware and other clients' hardware.

The Client shall compensate Baltmeta for all loss that Baltmeta incurs due to the Client's representative performing a prohibited action. The Client shall also satisfy all claims made by third parties.

#### **2.9 Unsuitable hardware**

In the event that it becomes established that the hardware provided by the Client may pose a threat to the stable operation of the DC infrastructure or of other IT hardware, such hardware shall not be mounted and shall be returned to the Client.

### **3. DC INFRASTRUCTURE**

#### **3.1 Climate-controlled environment**

In the server colocation room, a temperature of 22–27 °C shall be maintained. The measured temperature shall be that of the air stream delivered to the servers. The hourly temperature fluctuations shall not exceed 5 °C. A relative humidity of 44–55% shall be maintained in the server room.

#### **3.2 Electric power**

In order to ensure the constant supply of electric power, Baltmeta installed a redundant system of service entry equipment, UPSes, and PDUs. The constant power supply shall only be guaranteed provided the Client's IT hardware is connected to the power grid using 2 or more power sockets.

#### **3.3 Fire protection**

At the DC, fire shall be extinguished using inert gases.

In the event of a fire at the DC during the Client's visit, the Client must follow the instructions issued by Baltmeta's responsible persons and leave the premises through the exits shown on the fire escape maps.

#### **3.4 Racks**

The DC shall be equipped with AR3140 server racks. Dimensions: height 42U, width 750 mm and depth 1070 mm. The Client

shall be prohibited from placing its own racks.

### 3.5 Network

In order to ensure a high availability of Internet connection, Baltmeta installed redundant computer networks and switching/routing hardware.

The availability of Internet connection shall only be guaranteed provided the Client's IT hardware is connected to the network using 2 or more ports of the switching hardware.

## 4. TECHNICAL MAINTENANCE

### 4.1 Accepting and returning hardware

The Client's IT hardware shall be accepted at 160c Liepkalnio Str., Vilnius.

Upon acceptance, a certificate of acceptance shall be signed. The certificate shall include the value of the hardware. The value of the hardware shall be required for the purpose of insuring the hardware against any damage that it may suffer from fire or water and against other physical damage. In order to determine the value of the hardware, the Client must provide a contract of sale or any other document that would allow an objective assessment of the value of the hardware.

When any hardware is being taken away, it shall be recorded in the hardware register and a certificate of acceptance shall be signed. After the certificate has been signed, any claims related to the hardware being faulty or malfunctioning shall not be accepted.

### 4.2 Storing hardware

For storing the Client's IT hardware or its components, the Client may rent the open or closed racks located in the warehouse. Where a closed rack is rented, the key shall be kept at the security post.

For storing new hardware that is to be installed, but for a period of time not longer than 1 week, the Client may use, free of charge, the open racks located in the warehouse.

### 4.3 Unpacking hardware

Hardware may be unpacked only in the server unpacking workroom. It shall be prohibited to unpack hardware in the server room. In the event that various installation materials, cables, discs, etc., need to be carried to the server room, the plastic box located in the server unpacking workroom must be used.

For transporting heavy hardware, the Client may use a pallet truck.

### 4.4 Installing hardware

Where a shared rack is rented, the servers shall be mounted by Baltmeta's engineers.

Where a dedicated rack is rented and if not agreed otherwise, the hardware shall be mounted by the Client's authorised representatives.

The Client must ensure that all the hardware being installed be equipped with mounting rails. Before the mounting rails are not installed, the Company shall not proceed with mounting the Client's hardware. If the Client wishes so, the mounting rails may be purchased from the Company for an agreed price.

Any new hardware must be installed in such a way that it can be uninstalled without disrupting the operation of other servers. Cables must be laid in such a way that they do not obstruct access to a server's or a switch's ports.

### 4.5 Remote Hands

The Remote Hands service (ordered separately) shall include restarting the Client's IT hardware, monitoring visual alerts from the IT hardware, modifying the network topology, and hot-swapping server components. The service shall not include any parts or materials.

The service shall concern carrying out concrete works ordered by the Client (for example, replacing disks or changing the network configuration). Baltmeta shall not be liable for any consequences that may arise as a result of the actions mentioned above (for example, the Client provides an unsuitable disk, which, after having been used to replace another disk, causes a disruption in the smooth operation of the system).

## 5. SLA

### 5.1 Availability

The total availability of the DC infrastructure shall be defined as a combination of the availabilities of the infrastructure components, i.e. 1) the local and international Internet connection infrastructure; 2) the electric power supply infrastructure and 3) the temperature control infrastructure.

The availability of local Internet connection shall be verified by sending the *ping* command to the following addresses: delfi.lt, plus.lt and skelbiu.lt. If all the above-mentioned addresses do not respond, local Internet connection shall be deemed

unavailable. The availability of international Internet connection shall be verified analogously, by sending the *ping* command to the following addresses: [bbc.co.uk](http://bbc.co.uk), [yahoo.com](http://yahoo.com) and [google.com](http://google.com).

When the temperature of the air stream delivered to the servers exceeds 30 °C, that point in time shall be deemed the start of the period of malfunction of the DC infrastructure.

When both PDUs mounted in the server rack fail, that shall be deemed a disruption to the power supply. Where the Client's IT hardware is connected to only one PDU and that PDU fails during service provision, that shall not be deemed a service provision disruption.

The total availability shall be calculated as the minimum of the three infrastructure component availabilities.

The monthly availability of the Tier 3 DC shall be 99.982%, i.e. 8 min of unavailability per month.

## 5.2 Reliability

For the Tier 3 DC, the maximum allowed monthly number of failures shall be 1.

## 5.3 Failure registration time

Failures can be registered 24 hours a day by making a phone call to +370 700 800 88 or sending an email to [pagalba@balt.net](mailto:pagalba@balt.net).

## 5.4 Response time

The response time to a request for change or information shall be 4 h. Requests for change or information shall be completed on business days from 8:00AM to 5:00PM.

The incident response time shall be 15 min.

## 5.5 Monitoring

Where a dedicated rack is rented, the Client shall be granted 1) the right to manage power sockets, 2) access to Internet load graphs and 3) access to data on the air stream delivered to the servers.

Where a shared rack is rented, the Client shall be granted 1) the right to manage power sockets (restart only) and 2) access to Internet load graphs.

## 5.6 Compensation

In the case of the Tier 3 DC, in the event that there is a month when downtime exceeds 8 min, the Client shall receive a compensation in the amount of 10% of the monthly fee per half-hour of downtime.

In the event that repeated service provision disruptions occur, the Client shall receive an additional compensation for each disruption from the second one on, in the amount of 20% of the monthly fee.

The compensations shall be cumulative.

The maximum total compensation shall not exceed 100% of the monthly fee paid for the rental of server racks, Internet connection for the servers, electric power and cooling.

The compensation shall be provided in the form of a discount on the monthly fee for the current month.

## 5.7 Hardware insurance

All hardware provided by the Client shall be insured by an insurance company against fire, water and physical damage. In the event of an incident, the damage shall be compensated for based on the market value of the hardware. The insurance shall not cover the value of data.

The hardware shall be insured only if the Client provides, upon the installation of the hardware, documents that prove the value of the hardware.