BEYOND.PL SP. Z O. O.

ul. Adama Kręglewskiego 11

61-248 Poznań

Poland

# IDW-05 – BEYOND.PL DATA CENTER 2 CAMPUS POLICY

| | |
|---|---|
| Document indication: | IDW-05 |
| Version: | 06 |
| Date of issue: | 2024-03-29 |
| Created by: | Dariusz Sobkowiak |
| Approved by: | The Board |
| Confidentiality level: | Internal Unclassified |

## CHANGELOG

| Date | Version | Created by | Change description |
|---|---|---|---|
| 2017-11-22 | 02 | Dariusz Sobkowiak | Changes related to modifications in P-30 PERSONAL SECURITY CHECK procedure. |
| 2018-11-27 | 03 | Dariusz Sobkowiak | Changes related to address. |
| 2019-03-12 | 04 | Dariusz Sobkowiak | Title change, modifications in the content. |
| 2019-08-09 | 05 | Aleksandra Urbanowicz | Implementing Personal Data Processing Information Clause – point 4.4. |
| 2024-03-29 | 06 | Dariusz Sobkowiak | Update Facility Team and Security Team contact information. Removal of the phrase CBTI from the content. |
| | | | |
| | | | |

# Contents

# 1. Goal of the Procedure, Range, Users

This document contains information about the location of Beyond.pl Data Center 2 Campus, its equipment, the configuration of its security systems, the organization of its operations and the rules for using its services.

Without the written consent of Beyond.pl, the document may not, in whole or in part, be copied or used for purposes other than those for which it was provided.

The users of this document are all Beyond.pl employees and external entities (including contractors, subcontractors, organizational units, individuals or legal entities), depending on the need arising from the tasks performed for or on behalf of Beyond.pl.

# 2. Definitions

For the purposes of this policy, the following terms and definitions apply:

**Beyond.pl Data Center 2 Campus** - a facility located at 11 and 11A Adama Kręglewskiego Street in Poznań City in Poland, consisting of an Office Building, Data Center 2 Building (Technology Building with Logistics Module) and outdoor areas within the fence;

**Data Center 2** - Technical Building with the Logistics Module, necessary technical infrastracture (i.e. guaranteed power supply installations, cooling systems, labs) and the Logistic Module, in which warehouses, Data Center 2 Service Management Center and social-living spaces are located;

**Logistic Module** - Data Center 2 area adapted for storage and unloading;

**Administrator** - administrator of Data Center 2 Campus – the company Beyond.pl Sp. z o.o., registered in Poznań, ul. Adama Kręglewskiego 11, entered in the Register of Entrepreneurs of the National Court Register under KRS 0000237620;

**ZOT -** Campus technical maintenance team;

**Service -** entity providing supplies, performing finishing works, repairs, or maintenance at Campus premises.

**Guest -** a person present on the Campus and invited by an employee of the Administrator;

**Customer -** entity using Data Center 2 services to the extent specified in the Agreement;

**Agreement -** agreement between the Administrator and the Customer, defining specific terms of reference for the services provided;

**Colocation Space -** Cage, Server Rack, rack space, or any other combination and number of the above specified in the Order;

**Warehouse -** warehouse space at the Logistics Module specified in an Order or an Agreement;

**Infrastructure -** Administrator’s equipment and accessories used to perform Services;

# 3. Description of the Data Center at the Information Technology Research Center

This chapter includes a description of Beyond.pl Data Center 2 Campus.

## 3.1. Location and Equipment

Campus is located at ul. Adama Kręglewskiego 11 in Poznań, Poland. The facility consists of the following buildings:

- **technical building (Data Center 2)** including the data server module, necessary technical infrastructure (i.e. guaranteed power supply installations, cooling systems, labs) and the the Logistic Module, in which warehouses, Data Center 2 Service Management Center and social-living spaces are located,
- **office building** for staff with rest and refreshment facilities, classrooms and conference rooms, one underground and two overhead technical passages, which are an integral part of the office building and connect it with the technical building.

## 3.2. Zone Description

### *3.2.1. General Information*

Data Center 2 (Technical Building and Logistics Module) architecture reflects the needs of customers for easy access to their space and complete physical security.

Data Center 2 - access points:

- personnel entrance (main entrance), located next to the security post in the logistics module,
- technical entrances (unloading ramps) equipped with lifts, enabling deliveries,
- two entrances leading from the office building - aboveground connectors,
- underground passage leading from the office building - underground connector,
- technological entrances, enabling ongoing maintenance of technological equipment.

### *3.2.2. Security Zones*

For security reasons, the campus area, together with its immediate surroundings, has been divided into zones with different levels of security and zones requiring different levels of access privileges. The facility is protected 24/7 by security personnel equipped with direct coercive measures, carrying out a strict set of security procedures.

#### *3.2.2.1. Outdoor Area*

The outdoor area includes: all outdoor areas adjacent to the technical building (Data Center 2) and the office building. Access to the area is restricted by a double fence (steel mesh fence 290 cm high with steel posts on the outside, concrete walls 25 cm thick and 200 cm to 400 cm high from the plot level on the outside and a section of the wall). The outdoor area is covered by video surveillance. The area is regularly patrolled by security personnel.

#### *3.2.2.2. Parking Area*

Parking area is located within the outdoor area and includes parking space and a bicycle

shelter next to the office building, and parking places between the office building and the data center building. Car park can be accessed by staff and Guests/Customers/Maintenance Services that have an appointment.

#### *3.2.2.3. Hospitality Area*

The hospitality area covers social-living spaces, lobby in the office building and the logistics module, as well as the visitor route. Guests don't need an activated access card to access the hospitality area, however, they must sign the Statement of Understanding of Data Center Policy, attached as the F-39 form to this document. The entry and exit of Guests is assigned to dedicated member of staff. Before you access the hospitality area, you must go through a security check. All Guests must present their identity document to Security personnel. Following successful identity verification, Security personnel issues a badge and hands over the Guest to a member of staff.

In the event that a Guest is accompanied by a member of staff towards the offices, the visitor route or directly into the Data Center 2, they are required to go through a security check according to **the P-30 Personal Security Check - Metal Detection and Baggage Screening.**

The procedure for handling guests is described in detail for Beyond.pl employees in document **P-19 - Handling guests and tours.**

#### *3.2.2.4. Access zone for external service companies*

This zone includes a room or group of rooms, together with the route leading to them, for which deliveries, repair or maintenance work is carried out. Access to a service area requires prior notification in the form of a completed Work Permit Application, a sample of which is form F-38 of these regulations. A dedicated access card for the area is activated for the service area. Service work may take place only in the presence of a ZOT employee. Entrance to the service area is preceded by an inspection at the Security post. The serviceman is required to show to Security an identity document and the contents of his luggage. After positive verification of identity, and as far as the service application indicates, Security will issue an access card and badge.

When ordered by Security, the serviceman is required to submit to inspection in accordance with **P-30 Personal Security Check - Metal Detection and Baggage Screening** and **P-31 - Vehicle Security Check**.

**Detailed rules for reporting service visits are described in sec. 3.4.3 below.**

#### *3.2.2.5. Loading/Unloading Area*

Access to this area requires prior notification in accordance with the guidelines contained in para. 8 in **IDW - 06 Infrastructure Service Policy Beyond.pl** (applicable to Customers) or in the form of a completed Work Permit Application, a specimen of which is Form **F-38** of these Regulations (applicable to Services).

Access to the loading/unloading area does not require activation of the access card, unless the information in Form F-38 state the contrary. Unloading work may take place only in the presence of personnel and at least one Security Officer. Entry to the loading/unloading area shall be preceded by a check at the Security post. The serviceman is obliged to show an identity

document to Security and allow inspection of the vehicle and baggage being brought in. Upon positive verification of identity, Security shall issue a badge and allow entry to the loading/unloading zone.

Collection and supply handling is detailed in the procedure:
***P-20 - Collection and Supply Handling (Logistics) - Personnel.***
***P-21 - Collection and Supply Handling (Logistics) - Customers and Maintenance Services.***

#### *3.2.2.6. Customer Access Zone*

Customer Access Zone includes: guest area, perimeter corridors and collocation and/or storage space specified in the contract/order. Work in IT chambers may take place only in the presence of a Beyond.pl employee. Entry to the Customer's access area is preceded by a check at the Security desk. After positive verification of identity, Security issues an ID badge, transfers the Client's Representative to the custody of the facility staff, and allows entry.

Upon Security's request, the Customer is required to undergo **P-30 Personal Security Check - Metal Detection and Baggage Screening**.
Customer area rules are detailed in **IDW-06 - Infrastructure Service Policy Beyond.pl**.

#### *3.2.2.7. Employee Access Zone*

The Employee Access Zone includes all rooms, including Customer spaces in Data Center 2. The employee moves around the facility with an access card. The employee's zone is divided into access levels, while access levels are assigned to a particular employee on a necessity basis (least privilege). Access to the client's space with the use of the employee's card takes place in justified cases, and records of entry are available to the Client upon request.

Detailed rules for activating cards and assigning access levels to an employee are governed by the procedure **IDW-30 – Instruction on Handling Physical Access Control Cards.**

Detailed rules for handling traffic are specified in the procedure ***P-24 - Pedestrian and Vehicle Traffic.***

## 3.3. Data Center 2 Management

### *3.3.1. Personnel Structure*

The performance of Data Center 2 services is supervised by the Data Center Management Team. The team members have passed the company verification and training process. Data Center Management Team is divided into the Technical Service Team (ZOT), Logistics Team supervising Logistics Module operations, Physical Security Team executing security procedures, and the IT team supervising IT systems and providing support services for the Data Center 2 customers.

### *3.3.2. Services Management Center*

The ZOT technical team and the IT services team are stationed at the DC Services Management Center - the operators bridge. The room is located in the Data Center's Logistics Module and is equipped with a complete service monitoring system, alarm notification system, and a remote infrastructure management and diagnostics system.

## 3.4. Communication Policy

### *3.4.1. Important Contacts*

- **Helpdesk**
  +48 616674800
  help.desk@beyond.pl

- **Technical Service Team (ZOT)**
  +48 690 727 514
  zot.dc2@beyond.pl

- **Campus Security**
  +48 517 908 271
  ochrona.dc2@beyond.pl

### *3.4.2. Customers*

Detailed rules for communication, reporting of deliveries and visits for Customers using colocation services are specified in **IDW-06 – Infrastructure Term of Service**.

Detailed rules of communication for Customers using other services are defined in each case by the Agreement.

### *3.4.3. Maintenance*

Maintenance companies are required to submit a completed **F-38 - Work Permit Application** by 15:00 of the preceding day to **prace.dc2@beyond.pl**.
Maintenance service visit handling is detailed in the procedure:
***P-25 - Application of Permission to Perform Works Handling Procedure – Personnel version.***
***P-26 - Application of Permission to Perform Works Handling Procedure - Maintenance Services version.***

### *3.4.4. Guests*

Guests can access Campus premises when they provide the following details to a host:
- visitor's name and surname,
- ID number,
- company name (if applicable),
- vehicle registration number,
- date and time of planned visit,
- purpose of the visit.

Host inviting a Guest is required to comply with the internal procedure ***P-19 - Handling Guests and Tours***.

When a Guest is accompanied by a Beyond.pl employee towards the offices, the visitor route or to the Data Center 2 building including the Logistics Module, they are required to sign the form F-39 - Statement of Understanding of Beyond.pl Data Center Policy.

#### *3.4.5. Couriers and Postal Deliverers*

Campus personnel are required to comply with the internal procedure **P-27 - Courier and Postal Delivery Handling Procedure**.

In case of dimensional weight which requires entry through gate BR02 and use of unloading bay, the following procedures apply:
**P-20 - Collection and Supply Handling (Logistics) – Personnel version.**
**P-21 - Collection and Supply Handling (Logistics) - Customers and Maintenance Services version.**

# 4. Additional Information

## 4.1. Standing Orders

- The security of the facility operates within the framework of specialized armed security formations within the limits of authority in accordance with the provisions of the Act of August 22, 1997 on the Protection of Persons and Property (i.e., Journal of Laws 2016, item 1432, as amended).
- Security Guards can use means of direct coercion in duly justified cases.
- While at the facility, all persons are required to present their ID upon request by security.
- All persons must have and visibly display a valid ID badge received at the security check while at the facility.
- Security checks shall be carried out in the office building at the entry to the Data Center according to the procedure **P-30 Personal Security Check - Metal Detection and Baggage Screening**.
- Entry behind Gate BR02 is restricted to authorized employees vehicles and, upon appointment, to Maintenance, Supplier, and Customer vehicles which have passed the verification checks according to the procedure **P-31 - Vehicle Security Check**.
- Security Guards are authorized to assess the contents of the vehicle's trunk and chassis and the driver's cockpit.
- While at the facility, it is strictly forbidden to:
  - being under the influence of alcohol,
  - ***bring any pyrotechnic devices, explosives, or weapons, including firearms, blade weapons, teasers, stun guns, tear gas, or similar tools (does not apply to uniformed services),***
  - consume alcohol or smoke outside designated areas, or bring and use drugs, or psychotropic substances,
  - record videos or take pictures without permission from the facility management,
  - leave baggage or any other objects which may interfere with the operation of the facility unattended,
  - litter or pollute facility area,
  - use open fire or spray fragrances and smoke,
  - park vehicles outside designated areas.
- Transport of hazardous substances, particularly infectious agents, explosives, or radioactive materials is strictly prohibited.
- Transport of potentially hazardous substances, including acids, pyrophoric materials,

compressed gas, flammable materials, combustible materials, poisonous substances, cooling agents, toxic substances, or volatile substances, is only permitted in justified cases. Visitors shall justify the above transports in the form **F-38 - Work Permit Application.** Customers are forbidden to transport any hazardous materials.

- It is forbidden to bring unauthorized persons - who do not have the right of permanent access - into the premises without arranging it with the staff of the facility.
- Everyone who encounters a person without a badge, is obliged to notify the Security.
- Data Center personnel can request a person without a visitor badge or an ID, or not complying with the Data Center Policy or the facility security procedures, to leave the premises.
- Loss of an issued access card must be immediately reported to Security or the ZOT employee on duty.
- It is forbidden to bring any liquids and compressed flammable gases into electrical traffic and telecommunications rooms, including server chambers.
- In case you hear fire alarm, you must immediately go towards emergency exits and strictly adhere to ZOT and Security instructions.
- In the event of damage on the premises including the Data Center 2 area, not resulting from normal operation, caused by the fault of persons representing the Customer, the Customer is obliged to pay the actual costs. In particular, this applies to cases:

  - destruction or damage of the facility or facility equipment,
  - damage of hardware components or disruption of Service resulting from unauthorized configuration changes or repairs by Customer employees,
  - causing fire, floods, etc.,
  - causing false alarms or unjustified use of security services,
  - degrading Administrator provided services by unjustified and unauthorized involvement of facility staff,
  - disturbing air conditioning process by leaving equipment or packaging outside designated areas.

## 4.2. Information Security

**Persons staying on the premises are obliged to keep confidential any information obtained in connection with their stay. This applies, in particular, to technical, technological, legal and organizational information relating to IT and ICT systems and networks, as well as the data contained therein.**

Information constituting a business secret within the meaning of the provisions of the Act of April 16, 1993 on counteracting unfair competition (i.e. Journal of Laws 2003, No. 153, item 1503, as amended) provided orally, in writing, or in any other form shall be covered by secrecy.

The above shall not apply to the disclosure of information:

- publicly available;
- obtained independently from other legitimate sources;
- with written permission to distribute,
- required by law.

The above obligation also includes taking photos of Data Center 2 elements, especially equipment and cabinet locations. It is forbidden to take photos of the aforementioned elements without the written consent of Beyond.pl's Board of Directors.
Photo documentation of the Customer's infrastructure for internal purposes is possible, but requires prior arrangements. The Client is required to submit a written request specifying the scope of documentation. After obtaining permission, the Client may, only under the supervision of staff, photograph elements of its own infrastructure. The prerequisite is to leave a copy of the photographs taken with the Facility Administrator.
Persons on the premises of Data Center 2 are required to comply with the rules contained in the information security policies, procedures and instructions in force at the Beyond.pl campus.

Persons who come into possession of protected information are prohibited from:
- copying/replicating and making information available to unauthorized persons,
- transferring information by any means to third parties,
- profiting from the information obtained,
- offering to sell information covered by secrecy.

Persons who come into possession of information are obliged to return all documents, materials, as well as information carriers that come into their possession in connection with the performance of activities for the Administrator.
The obligation to maintain strict secrecy of all information regardless of its form is valid for a period of 5 (five) years, counting from the date of completion of the visit to the facility.
In case of violation of the provisions of Section 4.2, Beyond.pl may pursue any of its claims in court.

### 4.3. Policy Penalties for violations of campus regulations

CBTI Administrator has the right to apply the following penalties against persons, who do not adhere to Data Center 2 Policy:
- Warning
- Warning with notification to dedicated Customer representative,
- Removing authorized person from the premises and deactivating their access card.

Beyond.pl will claim compensation from a Guest or Customer who has violated this Policy causing damage.

### 4.4. Personal data protection

Personal Data Controller is Beyond.pl Sp. z o.o., with registered office at ul. Adama Kręglewskiego 11, 61-248 Poznań, Poland. Beyond.pl Sp. z o.o. appointed a Personal Data Protection Supervisor, whom you can contact by sending an email to **iod@beyond.pl.** Data is collected to process your visit at Data Center 2, and to ensure property protection and security at Controller’s premises. Providing personal data is voluntary, however, refusal to provide personal data will make visits to our facilities impossible. The basis for the processing of your data is Article 6(1)(f) RODO, i.e. the Administrator's legitimate interest in the need to verify the identity of visitors to Data Center 2 due to the need to ensure compliance of security procedures with the requirements of norms and standards ISO27001, PCI DSS, ANSI/TIA 942-B-Rated4, EN50600 class4.

The extent, to which you and Beyond.pl Sp. z o.o. are contractually bound or your visit at Beyond.pl Sp. z o.o. premises for the purpose of negotiating or concluding an agreement, the basis for personal data processing are the concluded agreement or actions leading to its conclusion in the future (RODO art. 6(1)(b). The scope of the data processed by Beyond.pl Sp. z o.o. corresponds to the scope of the data indicated in the relevant procedure, statement, application or regulations applicable to a particular visit at Data Center 2, listed under section 5 - "Related Documents" of this instruction. The scope of data also includes recorded video surveillance image

The company Beyond.pl Sp. z o.o. processes the data in a manner consistent with the current legal provisions, only for the purpose of fulfilling your visit and ensuring the security of the facility. Your data will be processed for a period of 36 months. Your recorded video surveillance image data will be processed for a period of 3 months. You have the right to access, copy, amend, rectify, delete, restrict data processing, transfer and object to the processing of your data. You also have the right to lodge a complaint with a supervisory authority if you consider that your data is not processed lawfully. Your data may be made available to the company providing security services and keeping entry and exit records at the Controller's facilities. Your data will not be transferred outside the European Economic Area. Beyond.pl does not profile your data, including automated decision making.

If you want to know more about your personal data send us an e-mail to: **help.desk@beyond.pl**
**Data Protection Officer: Aleksandra Zwolińska-Mańczak, iod@beyond.pl**

## 5. Related Documents

IDW-03 - Physical Security Instructions; *
IDW-06 - Infrastructure Terms of Service;
F-38 - Work Permit Application;
F-39 - Statement of Understanding of Beyond.pl Data Center 2 Campus Policy.
IDW-30 – Instruction on Handling Physical Access Control Cards;*
P-19 - Handling Guests and Tours; *
P-20 - Collection and Supply Handling (Logistics) – for Campus Personnel; *
P-21 - Collection and Supply Handling (Logistics) – for Customers and Maintenance Services;
P-24 - Pedestrian and Vehicle Traffic – for Campus Personnel; *
P-25 - Application of Permission to Perform Works Handling Procedure – for Campus Personnel; *
P-26 - Application of Permission to Perform Works Handling Procedure – for Maintenance Services.
P-27 - Courier and Postal Delivery Handling Procedure; **
P-30 - Personal Security Check;
P-31 - Vehicle Security Check.

**- * - INTERNAL PROCEDURES - AVAILABLE FOR AUTHORIZED CAMPUS PERSONNEL ONLY.**

**Approved by**
**The Board** _____
**Date and Signatures**