CUSTOMER'S REPRESENTATIVES IN THE DATA CENTER

The Customer's representatives may stay in the Contractor's Data Center only after registration of permanent or guest access.

Access can be issued either in the form of a pass or with the use of biometric authentication technologies. When using biometric technologies and when collecting, processing, and storing personal biometric data, the Contractor shall be guided by the appendix

to the paid services contract "Contract on the Terms of Personal Data Processing," as well as comply with the principles and rules of personal data processing envisaged by the Law of the Republic of Armenia No.ՀՕ-49-Ն dated 05/18/2015 "On Personal Data."

According to security requirements, the Customer may be denied permanent or guest access to the visitor and the Contractor shall not justify the reasons for the refusal.

Permanent access

Permanent access to the Contractor's Data Center shall be executed based on an application from an authorized person of the Customer (according to the Example of Appendix No.1 to this Regulation). The application shall be made for one specific Data Center and shall contain mandatory information:

- the name of the Customer's company;
- the number of a service agreement;
- full name of the visitor;
- passport series and number;
- full name of the applicant; and
- a list of premises for access.

If the request indicates the need to issue a permanent pass, a photo of the visitor of the required quality shall be attached to the request.

The authorized person of the Customer shall send a request for access to the Contractor's Account Manager.

The Customer shall be responsible for keeping the list of persons with permanent access to the Contractor's Data Center up to date.

When changing the list of persons, the Customer shall update the list by replacing the entire list with a mandatory indication of the changes made. It is not allowed to maintain several lists at the same time, it is not allowed to issue several permanent passes at the same time.

The list of persons for permanent access shall be necessarily updated when the Customer's representative is dismissed.

In the case of loss of the pass, the Customer shall immediately inform the Contractor thereabout in order to block the lost pass.

The updated list for permanent access shall be sent to the Contractor's Account Manager by e-mail.

The Contractor shall ensure that access and permanent passes are blocked to the Customer's representatives excluded from the list within 3 (three) business days. The responsibility for the use of these passes during the specified period shall rest with the Customer

The customer shall update the information on the list of persons annually for the next calendar year within the period from December 1 to January 31. Updating the list shall be mandatory even if there are no changes. If the application for access has not been submitted before January 31, permanent access shall be blocked by the Contractor. The list submitted in December of the current year shall be valid from the date of submission until January 31 of the year following the upcoming calendar year.

The Customer shall ensure that the ordered personalized passes are received within 1 (one) month from the date of receipt of the notification of readiness. In the case of non-demand for personalized passes from the Customer's representatives, after 1 (one) month from the date of registration, the passes shall be withdrawn from the places of issue. In this case, the access shall be ensured using one-time guest passes. Re-registration and execution of personalized passes can be performed provided that the Data Center is visited more than 1 (one) time per month.

Guest access

Guest (temporary) access to the Contractor's Data Center shall be executed at least 1 day before the time of the expected site visit. The authorized person of the Customer shall send the Contractor a request in a free form by e-mail or draw up an application according to the sample specified in Appendix No.2 to this Regulation.

Guest access shall be granted for a period of no more than 30 calendar days from the date of registration of access. A pass shall be issued for the duration of stay at the site.

The permitted time of temporary stay shall be limited to the date of the visit to the Data Center, as specified in the application, and 12:00 pm on the day following the day of the visit to the Data Center.

The Presence of the Customer's Representatives at the Technological Site

Access to the data center (a guarded area separated by fences) is carried out through specially equipped security posts.. Access through the unloading and loading gateways shall not be allowed.

In order to obtain a pass, the Customer's representative shall present an identity document to the entrance group. At the end of the stay, the pass shall be delivered to the entrance group.

The Customer's representatives, who have personalized permanent passes, shall present a personalized pass at the entrance group, If necessary, they may also request an identification document.

The transfer of any pass to another person, as well as the access of two or more persons using one pass, shall be strictly prohibited.

Persons arriving by motor vehicle (except for the driver specified in the request) shall leave the vehicle in front of the checkpoint barrier and head to the entrance group to present an identity document.

Persons departing by motor vehicle (except for the driver specified in the request) shall leave the vehicle in front of the checkpoint barrier and head to the entrance group.

Customer representatives shall be allowed into the Module only if accompanied by an engineer on duty. The engineer on duty shall not be required to stay with the Customer's representatives during the performance of the work.

If a Customer's representative with a permanent or guest pass wishes to remain in the Module without being accompanied by a duty engineer (for single full rack rentals only), then the duty engineer may leave without losing sight of the customer's representative, or in this case opaque curtains will be provided to the customer's representative. In such cases, customer representatives are obliged to inform the engineer about all types of technological work performed on the equipment.9.3.3. Workers with electrical safety group 2 are allowed to carry out work on placement, installation, dismantling, as well as maintenance work on electrical equipment (the customer can install his own electrical equipment only when renting one complete rack). The customer undertakes to independently monitor and ensure the availability of the necessary group with its representatives.

ENSURING ACCESSIBILITY TO SHELVES WITHIN THE PCI DSS FRAMEWORK

Based on the service, racks located in the data center are divided into two types:

- PCI DSS colocation and physical server deployment
- PCI DSS cloud infrastructure

PCI DSS racks intended for cloud infrastructures must be locked at all times, access is provided in accordance with the requirements of paragraph 4.12 of the IN 01.80.01 instruction.

In the case of PCI DSS colocation and physical server deployment, each client is issued a separate key for their rack. With different keys and locking technologies, the client makes the choice themselves.

The keys are stored in the key storage, the keys are identified by the racks or customers. The key to the key box is kept by the employee.

To receive the key from the security post, the duty engineer submits a request from the client to perform work.

The guard checks the request and the right of the duty engineer to receive the key according to the approved list.

Makes an entry in the key distribution register, which must include at least:

- Date of registration
- Name and surname of the duty engineer
- Customer application number
- Time of key receipt and return