Equipment Housing and Colocation – Terms and Conditions

Equipment Housing and Colocation – Terms and Conditions

The housing & colocation service is available at the shared DEEC/ISR/IT/INESCC Datacenter. This service consists of placing (colocation) a server or other IT equipment with network access in this facility.

As the server is supplied by the client, it will also be configured, administered, and maintained (hardware and software) by the client. In this way, the owner may install any software they wish and configure it in detail.

The space dedicated to this service has redundant connections to the network core and is connected to a UPS (limited to equipment without GPUs for computing purposes). It is physically secure; therefore, new requests are subject to availability verification.

Benefits and Features

Power – Access to UPS (limited to equipment without GPUs for computing purposes), ensuring greater electrical safety and equipment stability
Temperature Control – HVAC system (temperature and humidity control) providing continuous control of temperature and relative humidity
Connection to Network Core – Direct connection to the network core for greater stability, higher access speeds, and low latency between applications and users
Security – Restricted-access area providing increased equipment security

---

Owner Responsibilities

- Installation (support may be requested)
- Network configuration (support may be requested or required data provided)
- Base system configuration, accounts/access, application layer, and services

- Maintenance
- Operation
- Backups
- Software updates
- Troubleshooting
- Licensing

Best Practices

Access Control

- Use individual accounts; never shared accounts
- Apply the principle of least privilege (access only to what is strictly necessary); keep administrative accounts separate from regular user accounts
- Follow best practices for password usage
- Use passphrase-based passwords – https://www.keepersecurity.com/features/passphrase-generator/
- Do not include personal or institutional information
- NEVER reuse passwords from other services
- Enable two-factor authentication (2FA) whenever possible
- Use a password manager to facilitate the above best practices – we recommend https://bitwarden.com/
- Separate read, write, and administrative permissions, granting only what is strictly necessary
- Review permissions regularly

Organisation and Structure

- Use well-structured directories according to specific needs
- Avoid storing personal data outside authorised locations
- Review file system permissions regularly

Remote Access

- Access to administrative interfaces only via the institutional VPN
- Command-line access should be disabled whenever possible or allowed only via the institutional VPN when strictly necessary, and only using cryptographic keys
- Avoid direct Internet access without a firewall for any service that is not strictly necessary
- Disable unused services and ports

Updates and Maintenance

- Keep the operating system up to date
- Apply security updates as soon as they are available
- Remove obsolete or unused services

Backups

- Ensure automated backups are in place
- Follow the 3-2-1 rule: 3 copies of data, on 2 different types of media, with 1 copy off the primary system
- Periodically test backup restoration

Risks Associated with Improper Use of Systems

- Loss of irreplaceable data
- Breach of personal data
- Compromise of credentials
- Interruption of installed services
- Unauthorised access to sensitive information

Anomalies and Issues

For security reasons, in the event of detected anomalies (viruses, malware, software malfunction, etc.), security breaches (compromised accounts, etc.), or any other issue that may potentially impact the remaining infrastructure, the equipment will be immediately disconnected from the network and/or power supply and returned to the owner for correction of the identified issues.

(A.I. Translated Article from Termos e Condições de Housing de Equipamentos)

Revision #2
Created 2026-01-30 13:32:56 UTC by Francisco Maia
Updated 2026-01-30 13:34:03 UTC by Francisco Maia