Serviços Comuns

Aplicável a DEEC e pólo de Coimbra de ISR, IT e INESC.

- Termos e Condições de Housing de Equipamentos
- Equipment Housing and Colocation – Terms and Conditions
- Termos e Condições de Alojamento de site WordPress

Termos e Condições de Housing de Equipamentos

> **Os termos e condições abaixo indicados aplicam-se às seguintes Instituições:**
> - Departamento de Engenharia Eletrotécnica e de Computadores da Universidade de Coimbra (DEEC)
> - Instituto de Sistemas e Robótica - Pólo de Coimbra (ISR)
> - Instituto de Telecomunicações - Pólo de Coimbra (IT)
> - Instituto de Engenharia de Sistemas e Computadores de Coimbra (INESCC)

Está disponível o serviço de housing & Colocation no Datacenter comum DEEC/ISR/IT/INESCC. Este serviço consiste na colocação (colocation) do servidor ou outro equipamento informático com acesso à rede neste espaço.

Sendo que o servidor é fornecido pelo cliente, será este também configurado, administrado e mantido (hardware e software) pelo mesmo. Desta forma, o seu proprietário poderá instalar o software que desejar, bem como configurá-lo minuciosamente.

O espaço dedicado a este serviço possui ligações redundantes ao core da rede e ligação a UPS (limitado a equipamentos sem GPU para efeitos de computação) e é fisicamente seguro, pelo que novos pedidos carecem de verificação de disponibilidade.

Benefícios e Características

- Energia – Acesso a UPS (limitado a equipamentos sem GPU para efeitos de computação) , garantindo maior segurança eléctrica e estabilidade dos equipamentos
- Controlo de Temperatura – Sistema HVAC (Controlo de Temperatura e Humidade) permite ter um controlo constante da temperatura e humidade relativa
- Ligação a core da rede – Ligação directa ao core da rede para maior estabilidade, velocidade de acesso superior e baixa latência entre as aplicações e os utilizadores
- Segurança – Espaço com acesso limitado permite maior segurança dos equipamentos

Responsabilidades do Proprietário

- Instalação (podendo ser pedido o nosso apoio)

- Parametrização de rede (podendo ser pedido o nosso apoio ou solicitados os dados necessários)
- Configuração de sistema base, contas/acessos, camada aplicacional e serviços
- Manutenção
- Operação
- Cópias de Segurança
- Actualizações de Software
- Resolução de Problemas
- Licenciamento

Boas Práticas

- Controlo de Acessos
  - Utilizar contas individuais, nunca contas partilhadas
  - Aplicar o princípio do menor privilégio (acesso apenas ao necessário) - conta de administração separada das contas de utilizador regular
  - Utilizar as melhores práticas na utilização de passwords
    - Utilizar passwords baseadas em palavras - https://www.keepersecurity.com/features/passphrase-generator/
    - Não conter informação pessoal ou institucional
    - NUNCA reutilizar palavras-passe de outros serviços
    - Ativar autenticação de 2 fatores (2FA) sempre que possível
    - Utilizar gestor de passwords para facilitar a utilização das boas práticas acima indicadas - recomendamos https://bitwarden.com/
  - Separar permissões de leitura, escrita e administração adequadas apenas ao estritamente necessário
  - Rever permissões regularmente
- Organização e Estrutura
  - Utilizar pastas bem estruturadas conforme cada necessidade específica
  - Evitar armazenar dados pessoais fora de locais autorizados
  - Rever permissões de sistema de ficheiros regularmente
- Acesso Remoto
  - Acesso a interfaces de administração apenas mediante VPN institucional
  - Acesso a linha de comandos deve estar desativado sempre que possível ou mediante VPN institucional se estritamente necessário e apenas utilizando chaves criptográficas
  - Evitar acesso directo via Internet sem firewall a qualquer serviço não estritamente necessário
  - Desactivar serviços e portas não utilizados
- Actualizações e Manutenção
  - Manter o sistema operativo actualizado
  - Aplicar actualizações de segurança assim que disponíveis
  - Remover serviços obsoletos ou não utilizados

- Cópias de Segurança (Backups)
  - Garantir que existem backups automáticos
  - Seguir a regra 3-2-1: 3 cópias dos dados, em 2 tipos de suporte diferentes, 1 cópia fora do sistema principal
  - Testar periodicamente a reposição de backups

Riscos associados ao uso inadequado de sistemas

- Perda de dados irreproduzíveis
- Violação de dados pessoais
- Comprometimento de credenciais
- Interrupção de serviços instalados
- Acesso não autorizado a informação sensível

Anomalias e Problemas

Por razões de segurança, em caso de detecção de anomalias (vírus, software malicioso, mau funcionamento de software, etc.), quebras de segurança (contas atacadas, etc.) ou qualquer outro problema que tenha potencial impacto na restante infra-estrutura, o equipamento será imediatamente desligado da rede e/ou energia e entregue ao proprietário para correcção das situações identificadas.

Disposições finais

A instituição pode atualizar este regulamento periodicamente para responder a necessidades técnicas ou legais emergentes.

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)

Termos e Condições de Alojamento de site WordPress

> **Os termos e condições abaixo indicados aplicam-se às seguintes Instituições:**
> - Departamento de Engenharia Eletrotécnica e de Computadores da Universidade de Coimbra (DEEC)
> - Instituto de Sistemas e Robótica - Pólo de Coimbra (ISR)
> - Instituto de Telecomunicações - Pólo de Coimbra (IT)
> - Instituto de Engenharia de Sistemas e Computadores de Coimbra (INESCC)

Este regulamento define as regras de utilização do serviço de alojamento web para **sites WordPress** alojados em servidores de uma das instituições acima identificadas.

O serviço destina-se a apoiar a divulgação de **projectos académicos, de investigação ou de divulgação institucional**, promovendo uma presença online estável, segura e responsável.

Âmbito e utilização

1. O alojamento WordPress é facultado exclusivamente a docentes, investigadores, unidades de investigação, projectos, e iniciativas académicas devidamente aprovadas;
2. A utilização deve ser **compatível com a missão e atribuições das instituições**, em conformidade com o Regulamento de Utilização de Recursos de TIC da UC (Diário da República);
3. É **proibido o uso para fins comerciais, pessoais, ou não autorizados**, designadamente para alojar conteúdos que violem leis, direitos de terceiros, ou políticas de segurança.

Limites técnicos

1. Cada site WordPress alojado terá um **limite de armazenamento de dados de 5 GB** (*disco alocado para ficheiros, bases de dados e conteúdo do site*);
2. O limite de espaço é um **teto rígido**. A instituição reserva-se o direito de:
   - notificar o titular do site quando o uso se aproximar do limite;
   - bloquear temporariamente funcionalidades ou acesso até que o uso seja reduzido;
   - propor migração para soluções alternativas se necessário.
3. O titular do site é responsável pela gestão eficiente de conteúdo, nomeadamente a **optimização de imagens, limpeza de ficheiros antigos, e utilização racional do espaço**.

Segurança e responsabilidade

1. O utilizador deve manter WordPress, temas e plugins **actualizados e livres de vulnerabilidades**, para garantir a segurança do site;
2. É responsabilidade do titular:
   - assegurar cópias de segurança externas dos dados que considerar importantes;
   - não ultrapassar o uso de recursos que comprometa a estabilidade do servidor ou serviço a terceiros;
   - não instalar plugins ou código que possam criar riscos de segurança ou consumo excessivo de recursos.
3. A instituição pode **suspender ou remover sites que representem risco para a infraestrutura, contenham malware, ou violem leis ou normas internas**.

Conteúdos e conformidade

1. Todo o conteúdo publicado deve **cumprir legislação aplicável**, regras de direitos de autor, privacidade de dados (incluindo GDPR), e orientações institucionais;
2. A instituição reserva-se o direito de remover conteúdo que:
   - viole leis ou normas institucionais;
   - promova discurso de ódio, discriminação, ou conteúdos ofensivos;
   - expõe dados pessoais de terceiros sem consentimento.
3. A utilização de serviços adicionais (por exemplo, comércio electrónico, processamento de pagamentos, integração com APIs externas) deve ser previamente aprovada pela instituição e obedecer a políticas de segurança adequadas.

Procedimentos de pedido

1. Os pedidos de alojamento WordPress são feitos mediante pedido de suporte, contendo:
   - nome do responsável;
   - título e finalidade do site;
   - descrição do conteúdo;
   - nombre de domínio proposto.
2. A instituição avalia o pedido quanto à relevância académica/institucional e conformidade com este regulamento.

Monitorização e fiscalização

1. A instituição pode monitorizar a utilização dos recursos para garantir conformidade com este regulamento, em conformidade com os princípios gerais do Regulamento de Utilização de Recursos de TIC da UC (Diário da República);
2. A monitorização destina-se exclusivamente a assegurar:
   - cumprimento dos limites técnicos;

- segurança e estabilidade da plataforma;
- observância das boas práticas de utilização.

Revogação e penalidades

1. As infrações graves ou repetidas a este regulamento podem resultar na:
   - suspensão do site;
   - revogação do acesso ao serviço;
   - comunicação a instâncias superiores da UC, em casos de violação legal.
2. A decisão sobre penalidades é da competência do responsável pelo serviço de alojamento da instituição e pela Direção.

Disposições finais

1. A instituição pode atualizar este regulamento periodicamente para responder a necessidades técnicas ou legais emergentes.