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
- Gestão de sites
- Website management

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.

Gestão de sites

English version

Os sites alojados pelos serviços de informática do **DEEC, ISR, IT e INESC Coimbra** passam a ser atualizados num único sítio, **sites.deec.uc.pt**. Entra-se com a conta institucional e, por segurança, com verificação em dois passos. Substitui o acesso por FTP e as contas partilhadas de cada site.

A quem se destina

A docentes, investigadores, projetos e núcleos que tenham um site alojado por nós e precisem de atualizar os seus ficheiros (páginas, imagens, documentos).

Para ter acesso a um site, ou para dar acesso a outra pessoa, peça-o para **suporte@deec.uc.pt**, indicando o endereço do site e o nome de utilizador de cada pessoa. O acesso é pessoal: cada pessoa entra com a sua conta, e não há passwords partilhadas.

Entrar

1. Abra **https://sites.deec.uc.pt**.
2. Em **Utilizador**, escreva só o seu **nome de utilizador**, **sem @domínio**. Por exemplo `jsilva`, e não `jsilva@deec.uc.pt`.
3. Em **Password**, use a mesma password do correio institucional.
4. Carregue em **Iniciar sessão**.

Se não se recordar da password, contacte o suporte.

Ativar a verificação em dois passos (só na primeira vez)

No primeiro acesso é obrigatório ativar a verificação em dois passos (2FA). Só se faz uma vez e demora cerca de dois minutos. Precisa do telemóvel com uma aplicação de autenticação, por exemplo **Microsoft Authenticator** ou **Google Authenticator**, gratuitas na App Store e no

Google Play.

Os ecrãs desta parte estão em inglês.

1. Depois de entrar, aparece a página **«Two-factor authentication using Authenticator apps»**, com o aviso de que a sua conta exige 2FA. **Não altere nada** em **«Configuration»** (fica *Default*) nem em **«Require 2FA for»** (fica *HTTP*). Carregue no botão **«Enable»**.
2. Abre-se a janela **«Set up two-factor authentication»**, com um **código QR**. No telemóvel, abra a aplicação de autenticação e adicione uma conta:
   - **Microsoft Authenticator:** «+» → **«Outra conta (Google, Facebook, etc.)»**;
   - **Google Authenticator:** «+» → **«Ler código QR»**.

   Aponte a câmara ao código QR. A aplicação passa a mostrar uma entrada **Sites DEEC** com um código de 6 dígitos, que muda a cada 30 segundos.
   Se a câmara não funcionar, escolha na aplicação «introduzir chave manualmente» e escreva o código de letras e números que aparece por baixo do QR.
3. Escreva no campo por baixo do QR o **código de 6 dígitos que a aplicação mostra nesse momento** e confirme. Se aparecer *«Failed to validate the provided authentication code»*, espere pelo código seguinte e volte a tentar.
4. A verificação fica ativa. Na mesma página, na secção **«Recovery codes»**, carregue em **«Generate new recovery codes»** e **guarde esses códigos** num local seguro, por exemplo impressos ou num gestor de passwords. Cada código serve uma vez para entrar se perder ou trocar de telemóvel.

Nas entradas seguintes é pedida a password e, a seguir, o **código de 6 dígitos** da aplicação.

Gerir os ficheiros do site

Depois de entrar, vê uma pasta por cada site a que tem acesso. Dentro dela pode **enviar, substituir, renomear, criar pastas e apagar** ficheiros. Para enviar, arraste os ficheiros para a janela ou use o botão de envio.

As alterações ficam publicadas de imediato no site. Antes de apagar ou substituir, guarde uma cópia dos ficheiros importantes, porque não há forma de desfazer a partir da interface.

Ligar com o WinSCP ou outro programa

Programas como o **WinSCP** ou o **Cyberduck** ligam por **WebDAV**, que não permite a verificação em dois passos. Por isso, este tipo de ligação **só funciona a partir das redes internas do**

DEEC, ISR, IT e INESC Coimbra, ou com a **VPN** ligada.

Campo	Valor
Protocolo	**WebDAV**
Encriptação	**TLS/SSL Implicit encryption**
Servidor	`sites.deec.uc.pt`
Porta	`443`
Utilizador / password	o seu nome de utilizador (sem @domínio) e a password do correio
Diretório remoto (WinSCP: *Advanced → Directories*)	`/dav`

Neste tipo de ligação não é pedido o código de 6 dígitos.

O **FTP** foi descontinuado e não está disponível.

Limitações

- Por segurança, **não é possível enviar ficheiros executáveis** como `.php`, `.phtml`, `.phar`, `.htaccess` ou `.user.ini`, nem mudar o nome de um ficheiro para uma dessas extensões.
- Sites **WordPress** ou com outra programação do lado do servidor são tratados caso a caso. Contacte o suporte.
- Aplicam-se os Termos e Condições de Alojamento de site WordPress, na parte que se aplique.

Problemas frequentes

Situação	O que fazer
A password não é aceite	Confirme que escreveu o **nome de utilizador sem @domínio**.
O código de 6 dígitos é recusado	Confirme que o relógio do telemóvel está em modo automático e use o código seguinte.
Trocou ou perdeu o telemóvel	Entre com um dos códigos de recuperação. Se não os tiver, contacte o suporte para repor a verificação em dois passos.
Não vê a pasta do seu site	O acesso ainda não lhe foi atribuído. Contacte o suporte.

Situação	O que fazer
O WinSCP não liga	Está fora das redes internas: ligue a VPN ou use o navegador.

Suporte: **suporte@deec.uc.pt**

Website management

Versão em português

Websites hosted by the IT services of **DEEC, ISR, IT and INESC Coimbra** are now updated in a single place, **sites.deec.uc.pt**. You sign in with your institutional account and, for security, with two-step verification. It replaces FTP access and the shared accounts each website used to have.

Who it is for

Faculty, researchers, projects and student groups who have a website hosted by us and need to update its files (pages, images, documents).

To get access to a website, or to give access to someone else, write to **suporte@deec.uc.pt** with the website address and each person's username. Access is personal: everyone signs in with their own account, and no passwords are shared.

Signing in

1. Open **https://sites.deec.uc.pt**.
2. In **Utilizador** (username), type only your **username**, **without @domain**. For example `jsilva`, not `jsilva@deec.uc.pt`.
3. In **Password**, use your institutional e-mail password.
4. Click **Iniciar sessão** (sign in).

If you do not remember your password, contact support.

Turning on two-step verification (first time only)

Two-step verification (2FA) is mandatory on your first sign-in. You only do it once, and it takes about two minutes. You need a phone with an authenticator app, such as **Microsoft Authenticator** or **Google Authenticator**, both free on the App Store and Google Play.

1. After signing in, you see the page **"Two-factor authentication using Authenticator apps"**, saying your account requires 2FA. **Do not change "Configuration"** (leave it as *Default*) or **"Require 2FA for"** (leave it as *HTTP*). Click **"Enable"**.
2. The **"Set up two-factor authentication"** window opens with a **QR code**. On your phone, open the authenticator app and add an account:
   - **Microsoft Authenticator: "+" → "Other account (Google, Facebook, etc.)"**;
   - **Google Authenticator: "+" → "Scan a QR code"**.

   Point the camera at the QR code. The app now shows a **Sites DEEC** entry with a 6-digit code that changes every 30 seconds.
   If the camera does not work, choose "enter a setup key" in the app and type the letters and numbers shown below the QR code.
3. Type the **6-digit code the app is showing at that moment** in the field below the QR code and confirm. If you see "*Failed to validate the provided authentication code*", wait for the next code and try again.
4. Two-step verification is now on. On the same page, in **"Recovery codes"**, click **"Generate new recovery codes"** and **keep those codes somewhere safe**, for example printed or in a password manager. Each one lets you sign in once if you lose or replace your phone.

From then on, every sign-in asks for your password and then for the app's **6-digit code**.

Managing your website files

After signing in, you see one folder for each website you have access to. Inside it you can **upload, replace, rename, create folders and delete** files. To upload, drag the files onto the window or use the upload button.

Changes go live immediately on the website. Before deleting or replacing anything, keep a copy of important files: changes cannot be undone from the interface.

Connecting with WinSCP or another program

Programs such as **WinSCP** or **Cyberduck** connect over **WebDAV**, which does not support two-step verification. For that reason this kind of connection **only works from the internal networks of DEEC, ISR, IT and INESC Coimbra**, or with the **VPN** connected.

Field	Value
Protocol	**WebDAV**

Field	Value
Encryption	**TLS/SSL Implicit encryption**
Host	`sites.deec.uc.pt`
Port	`443`
User / password	your username (without @domain) and your e-mail password
Remote directory (WinSCP: *Advanced* → *Directories*)	`/dav`

This kind of connection does not ask for the 6-digit code.

FTP has been discontinued and is not available.

Limitations

- For security, **executable files cannot be uploaded**, such as `.php`, `.phtml`, `.phar`, `.htaccess` or `.user.ini`, and files cannot be renamed to those extensions.
- **WordPress** sites, or sites with other server-side code, are handled case by case. Please contact support.
- The WordPress website hosting Terms and Conditions apply where relevant.

Common problems

Situation	What to do
Your password is not accepted	Make sure you typed your **username without @domain**.
The 6-digit code is rejected	Make sure your phone's clock is set automatically, and use the next code.
You replaced or lost your phone	Sign in with one of your recovery codes. If you do not have them, contact support to reset two-step verification.
You cannot see your website's folder	Access has not been granted yet. Contact support.
WinSCP will not connect	You are outside the internal networks: connect the VPN or use the browser.

Support: **suporte@deec.uc.pt**