

## Política de Utilização Aceitável (PUA)

### Connection Design

1,1 A Connection Design, Prestação de Serviços, programadores informáticos, com o domínio [www.connectiondesign.pt](http://www.connectiondesign.pt) é da propriedade de Ângelo Pina, empresário em nome individual com o nº de identificação fiscal 243713053, CIRS 1332, sediada na urbanização panasqueira edifício tulipa Lt-2 7b 8365-149 Armação de Pêra. Serve este documento respeitante à política de utilização aceitável (PUA) para definir os termos de uma correcta utilização dos serviços disponibilizados entre a Connection Design e o subscritor dos serviços, doravante designado por cliente.

1,2 À presente política de utilização aceitável, deverão ser agregadas as condições gerais de prestação de serviços e respectivas condições específicas do serviço que o cliente subscrever.

1,3 Com a confirmação no formulário de subscrição de serviço, o cliente aceita expressamente, sem reservas ou ressalvas, de todas e quaisquer condições do presente documento, cláusulas das condições gerais de serviço, cláusulas em anexo referentes, em específico, aos serviços a subscrever.

1,4 A regularização do pagamento afecto à subscrição de serviço ou à renovação de serviços já adquiridos, efectiva também a aceitação, sem reservas ou ressalvas, de todas e quaisquer condições do presente documento, cláusulas das condições gerais de serviço, cláusulas em anexo referentes, em específico, aos serviços a subscrever.

## 2 Definições

As palavras ou expressões a seguir listadas e presentes no decurso do presente documento devem ser entendidas conforme os significados respectivos indicados:

Área de cliente: com acesso restrito, através de username e password e com verificação através de autenticação por dois factores como opcional, que permite ao cliente e / ou a contactos adicionais definidos por este, diversas acções tais como a consulta / gestão de informação de cliente e respectivos meios de contacto associados; consulta / gestão de todos os serviços adquiridos, em estado activo ou outro; consulta / gestão de todos os pagamentos, nos mais diversos estados; abrir / gerir contactos de suporte através de ticket e / ou live chat.

Ficha de cliente: Secção que contém toda a informação identificativa do cliente, nomeadamente nome do responsável, empresa, morada, endereço de e-mail, nº de contribuinte, contacto telefónico, preferências de contacto e preferência de método de pagamento.

## Política de Utilização Aceitável (PUA)

ID de cliente: Número identificativo do cliente. Este é único e serve o propósito de auxiliar na identificação eficiente do cliente.

Dados de acesso: Conjunto de credenciais que permitem o acesso seguro a plataformas / secções com acesso restringido.

E-mail principal: Endereço de e-mail associado ao contacto principal de uma ficha de cliente com a Connection Design.

Username: Conjunto de caracteres que identificam determinado utilizador de um sistema dotado de restrições de segurança.

Password: Código de segurança constituído por diversos caracteres aleatórios que em conjunto com o username identificam determinado utilizador de um sistema dotado de restrições de segurança.

Titular do serviço: Entende-se como titular do serviço a entidade identificada como contacto principal (owner), cujos dados estão definidos na secção 'Perfil', na respectiva área de cliente Connection Design.

PUA (Política de Utilização Aceitável): Entende-se como a política de utilização dos serviços prestados pela Connection Design. por forma a ser possível garantir a protecção dos seus sistemas garantindo a capacidade técnica, disponibilidade e protecção dos mesmos.

SLA (Service Level Agreement): Acordo sobre os termos em que determinado serviço é prestado entre as duas partes envolvidas, Connection Design e cliente.

Malware: É um termo genérico para qualquer tipo de "malicious software" ("software malicioso") desenvolvido para se infiltrar num dispositivo sem o seu conhecimento e com o intuito de realizar diverso tipo de acções sem o seu consentimento.

SPAM: É uma mensagem recebida através de correio electrónico, que é entregue ao destinatário sem o seu consentimento e expressa permissão.

SPAM Trap: As Spam Traps são endereços de e-mail existentes, mas não divulgados, utilizados por provedores de e-mail e entidades anti-SPAM para identificar remetentes de mensagens não solicitadas pelos destinatários (SPAM).

Spamvertised: Divulgação de conteúdos através do envio de SPAM.

IP Spoofing: É uma prática que consiste em mascarar (spoof) endereços IP utilizando endereços de remetentes falsificados.

Política de Utilização Aceitável (PUA)

ARP Spoofing: É uma prática que consiste em mascarar (spoof) endereços MAC associando-os a endereços IP que não correspondem ao endereço MAC real.

Gaming: Acto de jogar.

Teamspeak: Ferramenta de comunicação focada nas comunidades de jogos, que possibilita conversas por voz com outros utilizadores recorrendo a tecnologia Voz sobre IP (VoIP).

DDoS (Distributed Denial of Service): É um ataque com o objetivo de tornar inacessível um dispositivo ou rede, aos seus utilizadores. Os ataques DDoS conseguem isso sobrecarregando o alvo com tráfego ou enviando informações que desencadeiam um crash do sistema. Em ambos os casos, o ataque DDoS priva utilizadores legítimos do(s) serviço(s) ou recurso(s) disponibilizados através desse dispositivo(s) e / ou rede(s).

Flooding: É a acção de enviar de forma massiva pacotes de informação. Por norma é uma acção de forma comum associada a ataques do tipo DDoS.

Open Proxy: Servidor cujo acesso a serviço(s), ferramenta(s) é permitido, de forma intencional ou involuntária, ao público. São recorrentemente utilizados por terceiros de diversas formas incorrectas, sendo a mais comum para o envio de SPAM.

Phishing: É um tipo de ataque de engenharia social frequentemente utilizado para roubar informação privada e relevante ao destinatário, tais como credenciais de login e números de cartão de crédito. Ocorre quando um terceiro, disfarçado de entidade confiável, induz a vítima a abrir um e-mail, mensagem instantânea ou mensagem de texto. O destinatário é então induzido a clicar num link malicioso, o que pode levar à instalação de malware, ao crash do sistema como parte de um ataque de ransomware ou à revelação de informações confidenciais.

### 3 Disponibilização e consulta

3,1 O cliente entende e aceita que a consulta e leitura desta política de utilização aceitável é de carácter obrigatório antes de proceder a qualquer subscrição e / ou renovação de serviço.

3,2 Para além da consulta obrigatória referida no ponto anterior, a Connection Design poderá ainda pontualmente disponibilizar esta mesma política de utilização aceitável ao cliente, como acção preventiva e / ou como advertência quando se verifique alguma situação que vá contra o estipulado nos pontos mencionados neste documento.

### 4 Conteúdos

4,1 O cliente reconhece e aceita que a Connection Design se limita em exclusivo a prestar os serviços a que se dispõe, não sendo a mesma responsável pelos conteúdos da informação ou de quaisquer dados disponibilizados e / ou recebidos através da rede de comunicações da Connection Design.

### Política de Utilização Aceitável (PUA)

4,2 O cliente entende e aceita que é o único e total responsável pelos conteúdos alojados no(s) serviço(s) por si adquiridos junto da Connection Design declarando que entende e aceita que esses conteúdos não poderão incluir-se na listagem de proibições a seguir indicada:

- a) Disponibilização / alojamento de conteúdos que contenham informação protegida por direitos de autor e direitos de propriedade industrial em geral, sem devida autorização ou devido licenciamento.
- b) Disponibilização / alojamento de conteúdos / software que não estejam devidamente licenciados, se aplicável.
- c) Disponibilização / alojamento de conteúdos que incentivem à prática ou que constituam prática de qualquer acto ilícito ou ilegal e / ou ofensivos aos bons costumes .
- d) Disponibilização / alojamento de conteúdos que sejam ofensivos ou coloquem em causa os bons costumes ou a ordem pública.
- e) Disponibilização / alojamento de conteúdos que por qualquer forma façam a apologia a crimes de guerra, terrorismo ou qualquer acto discriminatório ou contra a humanidade.
- f) Disponibilização / alojamento de conteúdos que contenham e / ou que direcionem para conteúdo de carácter adulto, sob qualquer formato, sendo a Connection Design único e exclusivo árbitro do que determina como ‘conteúdo adulto’
- g) Disponibilização / alojamento de conteúdos que possam iludir o utilizador em relação à verdadeira identidade, autoria e / ou legitimidade do conteúdo em causa (Phishing).
- h) Disponibilização / alojamento de conteúdos que contenham ou consistam na sua totalidade a vírus, malware, ou qualquer tipo de conteúdo que possa prejudicar os utilizadores e / ou o bom funcionamento dos servidores da Connection Design.
- i) Disponibilização / alojamento de plataformas e demais conteúdos que estejam desactualizadas e / ou vulneráveis permitindo a sua exploração por terceiros.
- j) Disponibilização / alojamento de conteúdos divulgados através do envio de SPAM (Spamvertised).
- k) Alojamento de plataformas de gaming e / ou teamspeak.

## 5 Redes e sistemas

5.1 A Connection Design não autoriza qualquer violação, ou tentativa de violação, através de qualquer forma, dos sistemas que compõem a sua infraestrutura e / ou de terceiros interferindo directa ou indirectamente no seu bom funcionamento. É assim expressamente proibido:

- a) O acesso ou tentativa de acesso a servidores ou sistemas informáticos alheios sem a devida e expressa autorização para o efeito.
- b) Realizar pesquisa não autorizada de vulnerabilidades em servidores, serviços ou redes, nomeadamente através da detecção ou tentativa de detecção sistemática .
- c) Realizar de forma activa ou passiva acções de sobrecarga, conjugadas ou não com exploração de vulnerabilidades, com o intuito de impedir o correcto funcionamento de serviços (DoS – Denial of Service ou DDoS – Distributed Denial of Service).
- d) Realizar o envio massivo de pacotes (Flooding).
- e) A realização de qualquer tipo de ação com o intuito de bloquear ou perturbar serviços, servidores ou redes.
- f) Recorrer à infraestrutura através da qual é disponibilizado o serviço adquirido pelo cliente com a Connection Design para realizar ataques, de forma activa ou passiva a outros sistemas informáticos ou redes.
- g) Fazer uso de endereçamento IP que não tenha sido devidamente atribuído pela Connection Design, ou cuja utilização não tenha sido expressamente permitida pela Connection Design.
- h) Realização de acções que consistam na alteração de endereço IP (IP Spoofing).
- i) Realização de acções que consistam na alteração de registos ARP (ARP Spoofing).
- j) Realização da interceptação ou tentativa de interceptação de dados transmitidos através das redes ou servidores sem a prévia autorização dos responsáveis ou legítimos proprietários.
- k) Recorrer aos servidores da Connection Design utilizando-os como “Open Proxy” permitindo a terceiros a exploração dos mesmos para a realização de qualquer tipo de ataque.

## 6 E-mail

6.1 Uma utilização abusiva dos sistemas de correio electrónico poderá, de forma directa ou indirecta, prejudicar o correcto funcionamento deste mesmo sistema à Connection Design e a todos os seus clientes. Assim e por forma a podermos garantir, dentro do possível, um correcto funcionamento dos sistemas de correio electrónico, são aplicadas as seguintes restrições:

- a) É totalmente proibido o envio de correio electrónico, independentemente do seu intuito – comercial ou pessoal -, a remetente(s) que tenham expressamente declarado não o pretender receber, vulgo SPAM.
- b) Não é permitido o envio de e-mails para listagens de endereços de e-mail adquiridas a terceiros.

- c) Disponibilizar conteúdos que permitam o envio de SPAM.
- d) Não é permitido o envio de e-mails para as denominadas “SPAM TRAPS”.
- e) Recorrer aos servidores da Connection Design utilizando-os como “SMTP Open Relay” permitindo a terceiros a exploração dos mesmos para o envio de SPAM.
- f) Realizar qualquer acção que tenha ou que possa ter como consequência a listagem de endereços IP da Connection Design em listas negras (Black Lists) e / ou afectar negativamente a sua reputação.
- g) Recorrer aos servidores da Connection Design para realizar o envio de e-mails recorrendo a domínio do qual não seja o responsável ou legítimo proprietário.

Política de Utilização Aceitável (PUA)