1. Regras sobre Conteúdos

A OverCloud reserva-se o direito de remover quaisquer aplicações ou restringir a prestação dos Serviços quando tenha conhecimento da existência de atividades ilegais, desenvolvidas através desses meios, nomeadamente:

a) Violação de qualquer lei, de qualquer jurisdição aplicável, incluindo leis sobre os conteúdos ou publicidade que podem ser difundidos na Internet, ligadas, designadamente a: álcool, concorrência, proteção de menores, substâncias ilícitas, exportação, armamento, importação, privacidade, títulos de crédito, telecomunicações e tabaco;

b) Prática de atos desonestos ou de qualquer forma injustos, incluindo a divulgação ou comunicação de informação difamatória, escandalosa, ameaçadora, injuriosa ou privada sem a permissão das pessoas afetadas, ou a divulgação de informação de tal forma que cause danos morais, quer devido à informação em si ou à frequência da sua divulgação;

c) Promoção, encorajamento ou defesa de violência contra qualquer estado, organização, grupo, indivíduo ou propriedade, ou divulgação de informação, formação ou apoio na concretização da referida violência;

d) Divulgação, envio ou receção de informação que viole direitos de "copyright", patentes,"trademarks", marcas comerciais, segredos comerciais, acordos de licenciamento de software ou outros direitos de propriedade intelectual de terceiros;

e) Programas, Scripts ou Aplicações que coloquem em causa o normal funcionamento dos Serviços disponibilizados;

f) Participar ou permitir a realização de jogos de fortuna ou azar.

2. Lista Negras de domínios e IP'S (Blacklist's)

A OverCloud compromete-se a prestar os serviços de acesso à Internet, mail relay e correio electrónico de uma forma plenamente funcional, naquilo que depende da sua infraestrutura de rede e de acordos estabelecidos com os seus parceiros e prestadores de serviços.
O CLIENTE aceita e reconhece que existem situações em que o serviço prestado pela OverCloud poderá ser afetado pelo registo dos endereços IP, ou domínios, em nome próprio ou em nome dos seus clientes, em listas negras públicas anti-spam, (também designadas "blacklists").

Estas ocorrências não são específicas nos serviços prestados pela OverCloud, ocorrendo igualmente com qualquer outro Internet Service Provider - ISP, tanto nacional como internacional.

3. Propriedade dos endereços IP

A OverCloud mantém, controla e administra as gamas de endereços IP que lhe são atribuídos pelo RIPE, durante o período contratual acordado. Assim, e com vista à correta utilização dos Serviços, a OverCloud reserva-se o direito de alterar ou remover os referidos endereços IP, sempre que se verifique ma utilização incorreta dos mesmos.

4. Regras do Serviço de Alojamento Web e Servidores

1. O conteúdo é da exclusiva responsabilidade do CLIENTE e não deverá, de modo algum, conter informação que:
a) viole os direitos de autor, nomeadamente, contenha, software "pirata", ficheiros de áudio (música) e vídeo (filmes) "piratas". Esta restrição estende-se ao alojamento, instalação, execução, utilização e/ou disponibilização deste tipo de conteúdos e/ou aplicações;
b) seja considerada ilegal, ofensiva, pornográfica, pedofila ou discriminatória com base em religião, sexo ou raça;
c) incite à prática de atos criminosos;
d) promova o dano físico ou moral contra quaisquer pessoas;
e) explore ou incite a exploração de menores.

5. Regras sobre Segurança de Rede e Sistema

1. Não é permitido ao CLIENTE ou utilizador dos Serviços a violação (ou tentativa de violação) de qualquer sistema de autenticação ou segurança que proteja contas de acesso, servidores, serviços ou redes. Nos casos de violação incluem-se, nomeadamente:
a) Acesso não autorizado a dados alheios (quebra de privacidade);
b) Pesquisa não autorizada de vulnerabilidades em servidores, serviços ou redes, nomeadamente detecção sistemática de resposta a serviços (Scan);
c) Entrada ou tentativa de entrada em máquinas sem autorização expressa dos responsáveis (Break In);
2. Não é permitido ao utilizador interferir intencionalmente no bom funcionamento de utilizadores, servidores, serviços ou redes. Nestes casos incluem-se, nomeadamente:
a) Ações de sobrecarga, combinadas ou não com exploração de vulnerabilidades de sistemas, que visem sabotar o funcionamento de serviços, (Denial of Service);
b) Envio massivo de pacotes (Flooding);
c) Quaisquer tipos de tentativas de entravar ou perturbar servidores, serviços ou redes;
d) Instalação, utilização e disponibilização de PROXYS de uso da conectividade disponibilizada para outros fins que não os da utilização do serviço contratado;

e) A manutenção de servidores OPEN RELAY;
f) Introdução de vírus informáticos, "worms", código prejudicial e/ou "cavalos de Tróia".
3. Não é permitida a intercepção de dados em qualquer rede ou servidor sem autorização expressa dos legítimos proprietários.
4. Não é permitido falsificar (introduzir, modificar, suprimir ou apagar, no todo ou em parte) dados, após a sua produção, com intenção de iludir e induzir em erro os receptores desses dados. Nos casos de falsificação incluem-se, sem se limitarem a isso:
a) Alteração de endereços IP (IP Spoofing);
b) Alteração da identificação de mensagens de Correio Electrónico ou New.