Acceptable Use Policy

Acceptable Use Policy

Acceptable Use Policy

1. Definitions

In this our Acceptable Use Policy all terms in capitals shall have the meanings set out in the Terms and Conditions, unless defined otherwise within this AUP.

2. General

This AUP applies to your use of the Solution and Services for the Term of your Agreement with the Company.

This AUP applies to all users of the Solution and Services (which includes but is not limited to you, Authorised Users, Customers and Partners).

Please read this AUP carefully, a copy of which can be found at www.cslucas.com/aup.

If you do not agree to the terms of this AUP, you have no right to use or to permit Authorised Users or Customers to use the Solution or Services.

3. Prohibited Activities

You may not use, or encourage, promote, facilitate or instruct others to use, the Solution or Services for any illegal, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive.

Prohibited activities or content include:

- Sharing, distributing, or disclosing login credentials, passwords, or access tokens to unauthorized individuals;
- Allowing access to your account by persons who are not designated

Authorised Users;
- Any activities that are illegal, that breach any third party rights, or that may be harmful to others, or the Company's operations or reputation;
- Content that infringes or misappropriates the intellectual property rights or proprietary rights of third parties;
- Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable; or
- Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancel bots.

4. Prohibited Activities

You may not use the Solution or Services to breach the security or integrity of any network, computer or communications system, software application, or network or computing device. Prohibited activities include:

- Accessing or using any system without permission, including attempting to probe, scan, or test the vulnerability of a system or to breach any security or authentication measures used by a system;
- Monitoring of data or traffic on a system without permission; or
- Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route.

You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

- Monitoring or crawling of a system that impairs or disrupts the system being monitored or crawled;
- Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective (DoS);
- Interfering with the proper functioning of any system, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques;
- Operating network services like open proxies, open mail relays, or open recursive domain name servers; or
- Using manual or electronic means to avoid any use limitations placed on a

system, such as access and storage restrictions.

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements.

You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission.

You will not collect replies to messages sent from another internet service provider if those messages breach this AUP or the acceptable use policy of that provider.

5. Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any breach of this AUP or misuse of the Solution or Services. We may:

- Remove, disable access to, or modify any content or resource that breach this AUP or any other agreement we have with you for use of the Solution or Services;
- Report any activity that we suspect breaches any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information;
- Cooperate with appropriate law enforcement agencies, regulators, or other third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP, where obliged to do so by law.

6. Changes to this Acceptable Use Policy

Any changes we may make to this AUP in the future will be posted on this web page and, where appropriate, notified to you by email.

AUP dated 3rd of March 2017