Acceptable Use Policy - Client Facing.

Document Name	Acceptable Use Policy - Client Facing
Revision No	V1.1
Approved By	Name and Job Title
Review Date	03/11/2021
Classification	Public

1. Introduction

1.1. This acceptable use policy ("AUP") outlines the principles that govern use of the systems, services and equipment provided by Connect Managed Services (UK) Limited.
1.2. You must read this AUP very carefully. It is important. It forms part of your agreement with us.
1.3. We may amend, modify or substitute this AUP at any time. Your continued use of any Connect services after any such amendment, modification or substitution constitutes your acceptance of any new AUP. We recommend that you visit our website regularly to check for any updates or amendments to this AUP

2. Definitions

2.1. “Customer(s)” or “you” means customers or anyone else who uses or access Connect Managed Services (UK) Limited services.
2.2. “Connect” means Connect Managed Services (UK) Limited services.

3. Scope

3.1. This Acceptable Use Policy (“AUP”) applies to all services supplied by Connect Managed Services (UK) Limited and is intended to help and protect our customers from inappropriate use of our services. A customer’s use of any service provided by Connect Managed Services (UK) Limited constitutes acceptance of this AUP.
3.2. In addition to the responsibilities set out in this AUP, customers are reminded that when using our services , they must comply with all relevant legislation, including but not limited to:
- Communications Act 2003
- Computer Misuse Act 1990
- Investigation of Regulatory Powers Act 2000

3.3. We reserve the right to update this AUP from time to time and updates will be posted on our website at www.weconnect.tech

4. Policy

4.1. By using the services, you agree to the latest version of this Policy.
4.2. You may not use, or facilitate or allow others to use, the Services:
- For any illegal or fraudulent activity;
- to violate the rights of others;
- to threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm;
- for any content or activity that promotes child sexual exploitation or abuse;
- to violate the security, integrity, or availability of any user, network, computer or communication system, software application, or network or computing device;
- to distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations (or “spam”).

4.3. 4.1 The following activities are prohibited:

- **Impersonation / Forgery**
  Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person or organisation by using forged headers or other identifying information is prohibited. The use of anonymous re-mailers and nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting.
- **Privacy Violations**
  Attempts, whether successful or unsuccessful, to gain access to any electronic systems, networks or data, without proper consent are prohibited.
- **Threats**
  - Threats of bodily harm or destruction of property are prohibited
- **Harassment**
  - Threatening or harassing activity is prohibited
- **Illegal Use**
  - The use of this service for illegal purposes is prohibited
- **Reselling**
  - The resale of any service without proper authorisation from Connect Managed Services (UK) Limited is prohibited. Anyone wishing to act as a reseller of our services should contact our sales team and request details of our wholesale / reseller programmes.
- **Copyright Infringement**
  - Connect Managed Services (UK) Limited services may not be used to create, access, download, transmit distribute or store any content which the customer does not own or to which the customer does not have the appropriate permissions. Connect Managed Services (UK) Limited will co-operate with all agencies attempting to assert their rights in these matters.
- **Threats to the Network**
  - Any activities, which adversely affect the ability of other people or systems to use Connect Managed Services (UK) Limited services, are prohibited.

- Interference with, or disruption of, use of the network by others, network services or network equipment is prohibited.
- It is the customer's responsibility to ensure that their network is configured in a secure manner. A customer may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A customer may not permit their network, through action or inaction, to be configured in such a way that it gives a third party the capability to use their network in an illegal or inappropriate manner.
- You must not run "port scanning" software which accesses remote machines or networks, except with the explicit prior permission of the administrator or owner of such remote machines or networks. This includes using applications capable of scanning the ports of other Internet users.

- **Email / Spam**
  - Connect Managed Services (UK) Limited does not tolerate, endorse or participate in e-mail spamming. Sending unsolicited commercial e-mail is prohibited.
  - Activities that have the effect of facilitating unsolicited commercial e-mail, or large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature, are prohibited. Users operating mail servers must ensure that they are not open relays.
  - In the event of any problems being caused by this type of activity, we will make every effort to ensure that the problem is resolved as quickly as possible. This includes full co-operation with any relevant authorities.

5.1 Violations of this AUP may be detected automatically by our systems or we may be alerted to potential breaches of these services by third parties.

5.2 In the event that we become aware of a potential policy violation we will take appropriate and proportionate action to prevent further violations. Such action may include:

- The issuing of written warnings or notifications of violations or suspected violations
- Temporary suspension of the service or aspects of the service, and informing the customer of our actions and the reasons for them
- Requesting that the customer identify and remediate the causes of any violations before service is resumed
- In cases of extreme or repeated violations of the policy, termination of the service in line with our Terms and Conditions.
- Invoicing the customer for administrative costs and/or reactivation charges.

5.3 We will, wherever possible work with the customer to help them understand and comply with this AUP, and will only resort to suspension or termination of service in extreme cases and with clear evidence of violation. We will always exercise good faith in the enforcement of this policy

-

5. Reporting Abuse

Connect Managed Services (UK) Limited requests that anyone who believes that there is a violation of this AUP should direct the information to the security team at this address: security@weconnect.tech.

6. Information Classification

This document is classified as Public.

7. Review

This Policy shall be reviewed on an annual basis, unless changes to business operations, relevant legislation or codes of practice necessitate an earlier amendment.

8. Version Control

Date	Version	Changes	Reviewer Name & Job Title	Approver Name & Job Title
02/11/2021	V1.0	New Version	Dimitris Damianou	
03/11/2021	V1.1	Layout amended	Fiona Thompson, Governance and Compliance Manager	

09/11/2021	V1.2	Add words	David Blackburn, Network CTO	