POLICY

ACCEPTABLE USE

This is a Policy as defined in the Agreement. In this Policy, references to Clauses are to Clauses of the Agreement, and references to paragraphs are to the paragraphs of: (i) this Policy; or (ii) whichever other document is specifically referred to. Defined terms that are used in this Policy which are not defined in paragraph 1 below shall have the same meanings as set out in Schedule 1 of the Agreement. The following Policy contains rules that govern your use of the Service.

This Policy may be amended from time to time by the Supplier on reasonable notice to the Company

1 Additional Definitions

In this Policy the following definitions have the following meanings:

Disruption means, but is not limited to, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, any otherwise unspecified form of denial of service (DoS) attack or attempts to crash a host

2 Restrictions on the Service(s)

2.1 The Company not permitted to use the Services to allow access to or to gain access to any illegal material

2.2 Linking to content that is illegal or allowing the Service to be used for any illegal activity is expressly prohibited.

2.3 The Company must ensure that the Services are not used to incite disorder, publish, disseminate or promote any material which encourages anything which is in any way pornographic, obscene, defamatory, menacing, offensive or in any way unlawful

2.4 The Company or the Company's customers, suppliers or 3rd parties are not permitted to publish any content, or link to any content, in which they do not own the right, without the prior permission of the owner, of the relevant right

2.5 The Services must not be used to transmit or post any material which may cause offence to others on the grounds of gender, race or religion or which may cause annoyance or offence to any person

2.6 The Services must not be used to distribute or promote any of the following;

(a) the sending of unsolicited emails or forged messages or spoofing

(b) software which may be used for port-scanning, virus creation, packet sniffing, smurfing, hacking, Trojan horses or any other illegal or anti-social activity;

(c) any activity which interferes with systems or networks' ability to operate including denial of service attacks in any form;

(d) lists of email addresses (unless all of the addressees on the list have given their explicit permission);

3 Security

3.1 The Company shall;

(a) not do anything, or allow any third party to do anything, which will compromise the security of the Service, or any services provide by the Supplier in delivering the Service.

(b) install and use appropriate virus checking software and security devices and to impose this same requirement on any of the Company's suppliers, 3rd parties or customers that use any of the Services.

(c) not share, or disclose to any third party, any passwords provided by the Supplier. Such passwords are the responsibility of the Company and the Supplier will not accept any responsibility for any loss or damages caused as a result of the passwords being compromised by a party other than the Supplier. It is the responsibility of the Company to take necessary steps to alter and protect passwords in the event that it is believed that any password(s) has become compromised to any unauthorised person or may be used in an unauthorised way In any event the Company must promptly notify the Supplier in the event of a compromise or suspected compromise of any password.

(d) not effect security breaches or Disruptions of communications including (but not limited to) accessing data of which the Company user is not the intended recipient or logging onto a server or account that the Company user is not specifically authorised to access.

3.2 The Company reserves the right to suspend or disconnect any of the Services if it identifies that systems and/or devices on the end of any connection to the Services, or and system provided as part of the Service are causing significant impact to the Company's Services or other Supplier customers Services, or are part of a 'botnet' (machines hijacked by others to distribute malicious software or other forms of abuse)