Acceptable Use Policy

1 About our Acceptable Use Policy

1.1 To ensure the availability of our Services to customers and their End-users, OptiComm has an Acceptable Use Policy that is designed to protect our Network from abuse.

1.2 We may immediately suspend, cancel or restrict the supply of the Service to the Customer or an End-user if the Customer or an End-user use the Service, or if any person who accesses the Service uses the Service, in any way which breaches this Acceptable Use Policy.

2 Prohibited use

2.1 The Customer, an End-user, and any person who accesses the Service, must not use, or attempt to use, the Service:

(a) for illegal purposes or practices;

(b) for any purpose if OptiComm has previously advised the Customer that such purpose is prohibited;

(c) in any way which damages or interferes (or threatens to damage or interfere) with the operation of a Service or with the efficiency of OptiComm's Network or a Supplier's Network (including as a result of attempts by the Customer to increase the capacity or performance of the Customer's system or Equipment);

(d) in any way which makes it unsafe or which may damage any property or injure or kill any person;

(e) to transmit, publish or communicate any material or engage in any conduct which is defamatory, abusive, menacing or harassing;

(f) to engage in abusive behaviour toward OptiComm's staff;

(g) to make inappropriate contact with children or minors;

(h) to access, store, reproduce, distribute, publish or commercially exploit any information or material of any kind that infringes any copyright, patent, trademark, design or other intellectual property right;

(i) to send, relay or distribute any electronic data, the contents or properties of which have been manipulated for the purpose of maliciously or illegally impersonating or obscuring the original source of that data. This does not include the use of Virtual Private Networks or similar concepts in circumstances where this is legal and otherwise complies with this Policy;

(j) to access, monitor, use or control any other person's equipment, systems, networks or data (including usernames and passwords) or to otherwise probe, scan or test the vulnerability of any other person's equipment, networks, systems or data, without that person's consent;

(k) to access, or attempt to access, the accounts or private information of others, or to penetrate, or attempt to penetrate OptiComm's or a third party's security measures,

computer software or hardware, electronic communications system or telecommunications system, whether or not the intrusion results in the corruption or loss of data. This does not include conducting network security testing specifically requested by the owner of the targeted network or system;

(l) to use or distribute software (such as password guessing programs, keyboard loggers, viruses or trojans) with the intent of compromising the security of any network or system;

(m) to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as 'pyramid schemes', 'Ponzi schemes', and 'chain letters';

(n) to engage in any unreasonable activity which impairs the ability of other people or systems to use OptiComm's Services or the Internet. This includes any malicious activity resulting in an adverse effect such as denial of service attacks against another network host or individual user, flooding of a network, overloading a service, improper seizing or abuse of operator privileges, and attempts to harm a system or network. For the avoidance of doubt, this clause does not capture an activity solely because it unintentionally contributes to network congestion;

(o) to access, store, reproduce, distribute or publish any content which is prohibited or unlawful under any Commonwealth, State or Territory law or classification system, or to provide unrestricted access to material that is unsuitable for minors; or

(p) to support carrier or service provider data aggregation applications, such as backhaul for mobile base stations or other networks or facilities, the provision of services to another carrier or carriage service provider to enable that carrier or carriage service provider to use the Service to provide retail services to End-users, multiplexed access systems and/or networks, or the provision of services to End-users on networks or facilities other than networks or facilities owned or operated by OptiComm.

2.2 Due to Payment Card Industry (PCI) requirements, the Customer, and any person who accesses the Service, must not use, or attempt to use, OptiComm's web-hosting Services to store credit card data without OptiComm's express consent in writing.

3 Spam

3.1 In this clause 3, "Spam" includes one or more unsolicited commercial electronic messages with an "Australian link" as contemplated by the Spam Act 2003.

3.2 The Customer, an End-user, and any person who accesses the Service must not use the Service to:

(a) send, allow to be sent, or assist in the sending of Spam;

(b) use or distribute any software designed to harvest email addresses; or

(c) otherwise breach the Spam Act 2003 or any regulations made under the *Spam Act 2003*.

4 General

4.1 The Customer and End-users must use reasonable endeavours to secure any device or network within the Customer's or End-user's control against being used in breach of this Acceptable Use Policy by third parties, including where appropriate:

(a) the installation and maintenance of antivirus and firewall software;

(b) the application of operating system and application software patches and updates;

(c) protecting account information and passwords and taking all reasonable care to prevent unauthorised access to the Service, including taking reasonable steps to secure any Wi-Fi network operated;

(d) for residential End-users, requiring any persons (for example, other members of the End-user's household) that the End-user allows to use the Service from time to time to also comply with this Policy; and

(e) for business and government End-users, maintaining and enforcing appropriate workplace and guest user policies that are consistent with the requirements of this Acceptable Use Policy.

4.2 Unless otherwise stated, OptiComm's rights to suspend, cancel or restrict the supply of the Service to the Customer or an End-user applies regardless of whether the breach or suspected breach was committed intentionally, or by means not authorised by the Customer or End-user (such as through Trojan horses, viruses or other security breaches).