ACCEPTABLE USAGE POLICY

1 INTRODUCTION

1.1 Thank you for taking the time to read ITEC's Acceptable Use Policy (AUP). By accessing this website, or by contracting with us for services, you agree, without limitation or qualification, to be bound by this policy and the terms and conditions it contains, as well as any other additional terms, conditions, rules or policies which may from time to time be made available to you in connection with this service/website. The AUP applies to all aspects of the Service. "Itec" means Itec Integrate (Pty) Ltd, and all of its affiliates (including direct and indirect subsidiaries and parents). "Itec Network" includes, without limitation, Itec's constructed or leased transmission network, including all equipment, systems, facilities, services and products incorporated or used in such transmission network.

1.2 The purpose of this AUP is to:

1.2.1 comply with the relevant laws of the Republic;

1.2.2 specify to Customers and users of our services/website, what activities and online behaviour are considered an unacceptable use of our services/website;

1.2.3 protect the integrity of our network; and

1.2.4 specify the consequences that may flow from undertaking such prohibited activities.

1.3 This document contains a number of legal obligations which you are presumed to be familiar with. As such, we encourage you to read this document thoroughly and direct any queries to our Customer services/legal department.

1.3.1 ITEC respects the rights of our Customers and users of our services to:

1.3.2 freedom of speech and expression;

1.3.3 access to information; and

1.3.4 privacy; human dignity, religion, belief and opinion in accordance with our constitution.

1.4 We undertake not to interfere with any of the rights set out in 1.4, unless:

1.4.1 required to do so by law;

1.4.2 such rights are exercised for unlawful purposes; or

1.4.3 the exercise of such rights threatens to cause harm to another person or affect the integrity of our network.

2 GENERAL

2.1 Itec specifies the actions prohibited to the Customers and the Users and its suppliers and subsidiaries. The Customer is required to adhere to this policy without exception. By using the Service, the Customer acknowledges that it is responsible for its Users compliance with the AUP, and that the Customer is responsible for violations of this AUP by any User. The AUP applies to all aspects of the Services provided by Itec in accordance with the relevant Service Order.

2.2 All cases of violation of the AUP should be reported to csoc@Itecgroup.co.za. Itec receives complaints directly from Internet users, through Internet organizations and through other parties. Itec shall not be required to determine the validity of complaints received, or of information obtained from anti-spamming organizations, before acting under this AUP. A complaint from the recipient of commercial email, whether received directly or through an anti-spamming organization, shall be evidence that the message was unsolicited. Itec has no obligation to forward the complaint to the Customer or the User or to identify the complaining parties.

2.3 The Customer acknowledges that Itec is unable to exercise control over the content of the information passing over the Services and the Internet, including any websites, e-mail transmissions, news groups or other material created or accessible over its Services. Therefore, Itec is not responsible for the content of any messages or other information transmitted over its Services. Itec does not make any commitment, nor do we have any obligation, to monitor or police activity occurring using any of the Services and will have no liability to any party, including the Customer, for any violation of the AUP.

2.4 Itec will attempt to notify the Customer of any activity in violation of the AUP and request that the Customer or the User cease such activity; however, in cases where the operation of the Core Network is, at its sole discretion, under threat, Itec reserves the right to suspend or terminate the Service or the Customer or the User's access to the Service without prior notification in order to preserve the integrity of its Services to other customers.

2.5 The Customer agrees to promptly investigate all such complaints and take all necessary actions to remedy any violations of this AUP. We may inform the complainant that the Customer is investigating the complaint and may provide the complainant with the necessary information to contact the Customer directly to resolve the complaint. The Customer shall identify a representative for the purposes of receiving such communication.

2.6 The Customer agrees to notify Itec immediately if they become aware of an impending event that may negatively affect the Core Network or its Services. This includes extortion threats that involve threat of "denial of service" attacks, unauthorized access, or other security events.

2.7 If the Customer or the User engage in conduct or a pattern of conduct, including without limitation repeated violations by a Customer or the User whereby correction of individual violations does not in Itec's sole discretion correct a pattern of the same or similar violations, while using the Service that violates the AUP, Itec reserves the right to –

2.7.1 inform the Customer's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AUP;

2.7.2 in severe cases to the discretion of Itec, suspend the Customer's account and withdraw the Customer's network access privileges completely until the Customer has corrected the violating condition of this AUP;

2.7.3 remove or prevent access to content that we deem to be in violation of the AUP or that we otherwise deem unlawful, harmful or offensive;

2.7.4 charge the offending parties for administrative costs as well as for machine and human time lost due to the incident; and

2.7.5 share information concerning the violation of the AUP incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies.

2.8 Because the Internet is an inherently open and insecure means of communication, any data or information a Customer or the User transmits over the Internet may be susceptible to interception and alteration. Itec makes no guarantee regarding, and assume no liability for, the security and integrity of any data or information a Customer or the User transmits via any of the Services or over the Internet, including any data or information transmitted via any server designated as "secure".

2.9 The Services shall not be used for any unlawful activities or in connection with any criminal or civil violation and the Services shall in all cases be used in compliance with applicable law. Use of the Service for transmission, distribution, retrieval, or storage of any information, data or other material in violation of any applicable law or regulation (including, where applicable, any tariff or treaty) is prohibited. This includes the use or transmission of any data or material protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the

transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory or otherwise unlawful.

2.10 Violations of system or network security by the Customer is prohibited and may result in civil or criminal liability. Itec will investigate incidents involving such violations and will involve and will co-operate with law enforcement officials if a criminal violation is suspected. Examples of such system or network security violations include the following –

- 2.10.1 unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of Itec;
- 2.10.2 unauthorised monitoring of data or traffic on the network or systems without express authorisation of Itec;
- 2.10.3 interference with service to any user, host or network including, without limitation, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- 2.10.4 forging of any IP Packet Header by IP Spoofing or any part of the header information in an email or a newsgroup posting;
- 2.10.5 intentionally transmitting files containing a computer virus or corrupted data;
- 2.10.6 attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of the Services;
- 2.10.7 attempts to circumvent user authentication or security of any host, network, or account (referred to as “cracking” or “hacking”);
- 2.10.8 attempts to interfere with Services to any user, host, or network (referred to as “denial of service attacks”);
- 2.10.9 obtaining and/or disseminating any unlawful materials, including stolen intellectual property, child pornography, and/or any unlawful hate-speech materials; and/or
- 2.10.10 any activity that disrupts, degrades, harms or threatens to harm the Core Network or Itec’s ability to deliver the Services to its other customers.

2.11 It is explicitly prohibited to send unsolicited bulk mail messages (“junk mail” or “spam”) of any kind (commercial advertising, political tracts, announcements); forward or propagate chain letters nor malicious e-mail; send multiple unsolicited electronic mail messages or “mail-bombing” to one or more recipient; send bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender; using redirect links in unsolicited commercial e-mail to advertise a website or service. This is strongly objected to by most Internet users and the repercussions against the offending party and Itec can result in disruption of service to other users connected to Itec.

2.12 Maintaining of mailing lists by the Customers and/or the Users is accepted only with the permission and approval of the list members, and at the members’ sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed by the Customer.

2.13 Public relay occurs when a mail server is accessed by a third-party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mail-server. The Customer’s mail servers must be secure against public relay as a protection to both themselves and the Internet at large. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed by the Customer.

2.14 Itec reserves the right to examine users’ mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the Customer and the User. Itec also reserves the right to examine the mail servers of any Customer using Itec mail servers for “smarthosting” (when the user relays its mail off an Itec mail server to a mail server of its own) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in strict accordance with Itec’s policy of preserving customer privacy.

2.15 The Customer may obtain and download any materials marked as available for download from the Internet but is not permitted to use its Internet access or the Services to distribute any copyrighted materials unless express permission for such distribution is granted to the Customer by the owner of the materials.

2.16 This AUP applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

2.17 The Services may be used to link into other networks worldwide and the Customer and the User agrees to conform to the acceptable use policies of these networks.

2.18 Service activity will be subject to the available bandwidth, data storage and other limitations of the specific service provided as per the Service Order.

2.19 To ensure that all customers and users have fair and equal use of the Services and to protect the integrity of the Core Network, Itec reserves the right, and will take necessary steps, to prevent improper, unlawful or excessive usage thereof, until such improper, unlawful or excessive usage is terminated by the Customer. Such action that Itec may take includes –

- 2.19.1 limiting Service throughout; and/or
- 2.19.2 preventing or limiting the Service access through specific ports or communication protocols; and/or
- 2.19.3 complete termination of the Service to Customers or the Users who grossly abuse the network through improper, unlawful or excessive usage.

2.20 Itec prohibits Customers from using Itec’s service to harm, or attempt to harm a minor, including, but not limited to, hosting, possessing, disseminating, distributing, or transmitting material that is unlawful, including child pornography.