ACCEPTABLE USE POLICY ('AUP')

A. General

Sure and its affiliates ("Sure") provide to business and consumer users a variety of information technology related products and services, including such service as internet access, content delivery services, various electronic mail (email) packages and services, world wide web hosting arrangements, ATM, Frame Relay, fixed and mobile voice and other data (eg: sms), online, and internet-related telecommunications services (each, a "Service" and collectively the "Services").

This Acceptable Use Policy ('AUP') defines the acceptable use of the Services with a view to ensuring quality of service and the privacy of our Customers and the integrity, security, reliability and privacy of the Sure network, systems, products, Services, server hosting facilities and data contained therein (collectively, the "Sure Network"). Sure's Customers (who for the purposes of this policy, are defined as any party who purchases a Service from Sure) are required to comply with this AUP as a condition of receiving Services from Sure.

Sure's Customers are solely responsible for the content and messages that they access, post, distribute or otherwise make available using the Sure Network. Sure encourages its Customers to self-rate their websites using a major rating agency such as the Internet Content Rating Association (ICRA) (http://www.icra.org).

.

B. Prohibited Activities

It is contrary to Sure policy for any of its Customers or other Service user to effect or participate in any of the activities listed below (whether actual or attempted and whether directly or indirectly) through a Service.

Each of the practices listed below (each, a "Prohibited Activity") constitutes an abuse of the Sure Network by and interfere with other Customers. Such practices are prohibited

1. Posting or sending messages substantially similar in content to 10 or more Usenet or other newsgroups, forums, listservs, or other similar groups or lists (each, a "List");
2. Posting or sending messages, articles, or other content to a List which are off-topic according to the charter or other owner-published FAQs or descriptions of the List;
3. Publishing mail bombs, chain letters or pyramid schemes;
4. Sending unsolicited commercial messages or communications in any form ("SPAM");
5. Falsifying user or other Service related information, including, but not limited to, intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return mailing and Internet protocol addresses, provided to Sure or to other Service users or engaging in any activities or actions intended to withhold or cloak Customer's or its End Users identity or contact information;
6. Unauthorised access to or use of data, Services, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;
7. Monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;
8. Interference with Service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
9. Use of an Internet account or computer without the owner's authorisation;
10. collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
11. Use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting;

12. Use of the Service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
13. Any activity or conduct that is likely to result in retaliation against our network;
14. Any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including data protection;
15. Introducing intentionally or knowingly into the Service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Services;
16. Misrepresenting yourself as other computer networks and users;
17. Any activity or conduct that unreasonably interferes with our other customers' use of our Services.
18. Engaging in any other activity that:
    i. violates a law or regulation (including, but not limited to, libel, slander, invasion of privacy, harassment, obscenity, child pornography, export laws and regulations, and infringement or misappropriation of another party's copyrights, trademarks, patents, trade secrets or other intellectual property rights);
    ii. threatens the integrity and/or security of any network or computer system (including, but not limited to, transmission of Viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware, malware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware);
    iii. has the purpose of harming or attempting to harm minors in any way;
    iv. attempts to use the Service in such a manner so as to avoid incurring charges for or otherwise being required to pay for such usage;
    v. otherwise degrades or interferes with other users' use of a Service;
    vi. breaches any legal duty owed to a third party, such as a contractual duty or a duty of confidence; or
    vii. violates generally accepted standards of Internet or other networks conduct and usage, including, but not limited to, denial of service attacks, web page defacement, port and network scanning, and unauthorised system penetrations.
    viii. is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
    ix. is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
    x. is defamatory or violates a person's privacy;
    xi. creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement bodies;
    xii. improperly exposes trade secrets or other confidential or proprietary information of another person;
    is intended to assist others in defeating technical copyright protections;
    xiii. infringes another person's trade or service mark, patent, or other property right;
    xiv. is discriminatory in any way, including by way of sex, race, or age discrimination;
    xv. facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;
    xvi. involves theft, fraud, drug-trafficking, money laundering or terrorism;
    xvii. is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to us; and
    xviii. is otherwise malicious, fraudulent, or may result in retaliation against us by offended viewers.
    xix. Content "published or transmitted" via our network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting, display or transmission that relies on the Internet.

19. Engaging in any of the activities listed above by using another provider's service, but channelling the activity through a Sure account, remailer, or otherwise through a Service.

ANY INDIRECT OR ATTEMPTED VIOLATION OF THIS AUP BY OR ON BEHALF OF A CUSTOMER OR A CUSTOMER'S END USER, AND ANY ACTUAL OR ATTEMPTED VIOLATION BY A THIRD PARTY ON BEHALF OF A CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED A VIOLATION OF THE AUP BY SUCH CUSTOMER OR CUSTOMER'S END USER.

C. Rights and Remedies

If Sure determines that a Customer, its representatives or its end users have breached or failed to comply with this AUP or engaged (or permitted others to engage) in a Prohibited Activity, Sure may take such action as it deems appropriate. This may include all or any of the following:

1. suspending and/or terminating a Customer's Service at any time;
2. Issuing of a warning to a Customer;
3. Commencing Legal proceedings against a Customer for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach of this AUP;
4. denying all traffic from known IP address blocks that support indiscriminate port scanning programs such as ProxyHunter, or other unlawful activity, for the purpose of preserving Customer's system and network resources;
5. undertaking further legal action against a Customer; and
6. in the event of illegal activities – investigating and notifying appropriate legal authorities.

If we receive a Court Order requesting us to reveal a Customer's identity to someone complaining that you have used the Services abusively, we will be entitled to do so. We will also be entitled to reveal your identity or other data we hold regarding your use of the Services to the police or other public authority if we are required to do so by law.
Sure will consider all cases and complaints according to their individual merits. Sure has the right not to take action against you even where a complaint is made against you for breach of this AUP.
Sure reserves the right to, where feasible, implement technical mechanisms to prevent a Prohibited Activity. In addition, Sure reserves the right to charge the Customer to cover administrative costs associated with the Prohibited Activities of the Customer including, but not limited to, recovery of the costs of identifying offenders and removing them from or discontinuing providing them Service, in an amount equal to Sure actual expenses incurred in preventing or responding to such activity.

For complaints of SPAM only: In addition to any applicable charges described above, Sure reserves the right to charge the Customer the amount set forth under applicable law or if no amount is specified US$10.00 per spam e-mail, such messages being not only annoying to internet users, but also seriously affecting the efficiency and cost-effectiveness of the Sure Network (they increase Sure costs by clogging the Network, rendering web-sites inaccessible and potentially leading to down time of Customers' mission-critical internet applications).

Nothing in this AUP limits Sure rights and remedies (available at law or in equity) in any way with respect to any Prohibited Activity.

D. Password Protection

Customers are responsible for protecting their password(s) and for any authorised or unauthorised use made of their password(s). Customers must not disclose your password or use or permit anyone to use Sure's Service to guess passwords or access other systems or networks without written authorisation. In the event a network or network device becomes compromised, Sure will assist in the tracking and/or expulsion of said offender on the network level to the extent Sure considers reasonable, at its sole and absolute discretion.

E. Access to Internet Data Centres

For Customers accessing Internet Data Centres (IDCs), in addition to, and to the extent not in conflict with, the rules of the individual IDC, only those individuals identified in writing by Sure or by Customer on the Customer Registration Form ("Authorised Personnel") may access the IDCs. Customer shall deliver prior written notice to Sure of any changes to the Customer Registration Form and the list of Authorised Personnel. Customer and its representatives shall not allow any unauthorised persons to have access to or enter any IDC. Customer and its representatives may only access that portion of an IDC made available by Sure to Customer for the placement of Customer's equipment and use of the IDC Services (the "Customer Area"), unless otherwise approved and accompanied by an authorised Sure representative.

F. Use of Internet Data Centre Facility

Conduct at Internet Data Centres. For Customers accessing IDCs, in addition to, and to the extent not in conflict with, the rules of the individual IDC, Customer and its representatives agree to adhere to and abide by all security and safety measures established by Sure and set forth in the Customer Guide provided by Sure to Customer.

Customer and its representatives shall also not do or participate in any of the following:

1. misuse or abuse any Sure property or equipment or any third party property or equipment;
2. make any unauthorised use of or interfere with any property or equipment of any other Sure Customer;
3. harass any individual, including Sure personnel and representatives of other Sure Customers;
4. engage in any activity that is in violation of the law or aids or assists any unlawful activity while on Sure property or in connection with the IDC Services.

Prohibited Items. For Customers accessing IDCs, in addition to, and to the extent not in conflict with, the rules of the individual IDC, Customer and its representatives shall keep each Customer Area clean, free and clear of debris and refuse. Customer shall not, except as otherwise agreed to in writing by Sure, (1) place any computer hardware or other equipment in the Customer Area that has not been identified in writing to Sure; (2) store any paper products or other combustible materials of any kind in the Customer Area (other than equipment manuals); and (3) bring any Prohibited Materials (as defined below) into any IDC. "Prohibited Materials" shall include, but not be limited to, the following and any similar items:

1. food and drink;
2. tobacco products;
3. explosives and weapons;
4. hazardous materials;
5. alcohol, illegal drugs and other intoxicants;
6. electro-magnetic devices which could unreasonably interfere with computer and telecommunications equipment;
7. radioactive materials;
8. photographic or recording equipment of any kind (other than tape back-up equipment).

G. Equipment and Connections

Customer Equipment. For Customers accessing IDCs, in addition to, and to the extent not in conflict with, the rules of the individual IDC, each piece of equipment installed in a Customer Area (the "Customer Equipment") must be clearly labelled with Customer's name (or code name provided in writing to Sure) and individual component identification. Each connection to and from a piece of Customer Equipment shall be clearly labelled with Customer's name (or code name provided in writing to Sure) and the starting and ending point of the connection. Customer Equipment must be configured and run at all times in compliance with the manufacturer's specifications, including power

outlet, power consumption and clearance requirements. Customer must use its best efforts to provide Sure with at least 48 hours prior notice any time Customer intends to connect or disconnect any Customer Equipment or other equipment.

H. Modification of This Policy

Sure reserves the right to update this AUP from time to time. You are expected to check this website page from time to time to take notice of any changes we make, as such updates are legally binding on you. Some of the provisions contained in this AUP may also be superseded by provisions or notices published elsewhere on our site or written documents issued to you.

I. Scheduled Maintenance

For information on scheduled maintenance, please view the maintenance schedule posted on Sure's World Wide Web site.

USE OF SURE Email Services -ADDITIONAL POLICY TERMS

J. Bulk Commercial E-Mail

1. You may not use a Sure E-Mail Service (such as @Suremail or @cwgsy.net) to send bulk mail. Please see the applicable Product Terms and Conditions for those Services. You may use your dedicated hosted system to send bulk mail, subject to the restrictions in this Acceptable Use Policy.

2. You must obtain our advance approval for any bulk commercial e-mail other than for market research purposes, for which you must be able to demonstrate the following to our reasonable satisfaction:

3. Your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure;

4. Your procedures for soliciting consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given;

5. You retain evidence of the recipient's consent in a form that may be promptly produced within 72 hours of receipt of recipient's or our requests to produce such evidence;

6. The body of the e-mail must include information about where the e-mail address was obtained, for example, "You opted in to receive this e-mail promotion from our Web site or from one of our partner sites," and information on how to request evidence of the consent, for example, "If you would like to learn more about how we received your email address please contact us at abuse@yourdomain.com";

7. You have procedures in place that allow a recipient to revoke their consent – such as a link in the body of the e-mail, or instructions to reply with the word "Remove" in the subject line and such revocations of consent are implemented within 72 hours;

8. You must post an abuse@yourdomain.com e-mail address on the first page of any Web site associated with the e-mail, you must register that address at abuse.net, and you must promptly respond to messages sent to that address;

9. You must have a Privacy Policy posted for each domain associated with the mailing;

10. You have the means to track anonymous complaints;

11. You may not obscure the source of your e-mail in any manner. Your e-mail must include the recipient's e-mail address in the body of the message or in the "TO" line of the e-mail.

12. These policies apply to messages sent using your E-mail Service or network, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site hosted via your E-mail Service. You may not use third party e-mail services that do not have similar procedures for all its customers.

13. We may test and monitor your compliance with these requirements, including requesting opt-in information from a random sample of your list at any time.

H. Unsolicited E-Mail

You may not send any unsolicited e-mail, whether commercial or non-commercial in nature, to any person who has indicated that they do not wish to receive it.

I. Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of the Sure E-Mail Services, system or network or to breach our security or authentication measures, whether by passive or intrusive techniques without our prior written consent.

J. Shared Systems

You may not use any shared system provided by Sure in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, we may prohibit the automated or scripted use of Suremail Services if it has a negative impact on the mail system, or we may require you to repair coding abnormalities in your Cloud-hosted code if it unnecessarily conflicts with other Cloud customers' use of the Cloud. You agree that we may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the system or other customers' data that is stored on the same system.

K. Other

1. You must have valid and current information on file with your domain name registrar for any domain hosted on our network.

2. You may only use IP addresses assigned to you by our staff.

3. You may not take any action which directly or indirectly results in any of our IP space being listed on any abuse database.

4. You agree that if you register a DNS record or zone on Sure managed or operated DNS

servers or services for a domain of which you are not the registrant or administrative contact according to the registrars WHOIS system, that, upon request from the registrant or administrative contact according to the registrars WHOIS system, Sure may modify, transfer, or delete such records or zones.

L. Export Control

Sure E-Mail Services may not be used by persons, organisations, companies or any such other legal entity or unincorporated body, including any affiliate or group company, which violates any applicable law or regulation including (but not limited to) export control laws and/or restrictive measures/sanctions. This should include involvement or suspected involvement in activities or causes and affiliation with others whatsoever who sponsor or support the above such activities or causes.