.NAME ACCEPTABLE USE POLICY

This Acceptable Use Policy (the "AUP") governs the use by registrants or users of .name domain names and email forwarding service (together, the "Services") offered by VeriSign, Inc. and its wholly owned subsidiaries ("Verisign"). Verisign created the AUP to promote the integrity, security, reliability and privacy of the Services and does not intend that the AUP be a mechanism to resolve disputes between users of the Services and third parties.

Verisign supports the free flow of information and ideas over the Internet. Accordingly, Verisign does not actively monitor, nor does it exercise editorial control over, the content of any message or web site accessible through its network. However, Verisign reserves the right to remove any materials that, in Verisign's sole discretion, are potentially illegal, may subject Verisign to liability, or otherwise violate the AUP. Verisign reserves the right to modify the AUP at any time. Unless significant modifications are made to the AUP, Verisign is not required to contact registrants about such changes. In the event of significant modifications, Verisign will send all registrants notice at their .name email addresses registered with Verisign.

Verisign reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, as it deems necessary, in its unlimited and sole discretion and without notice: (a) to protect the integrity, security and stability of the Domain Name system (DNS); (b) to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental agency or organization, or any dispute resolution process; (c) to avoid any liability, civil or criminal, on the part of Verisign, as well as its affiliates, subsidiaries, officers, directors, and employees; (d) per the terms of the registration agreement, (e) to respond to or protect against any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the Internet), (f) to comply with specifications adopted by any industry group generally recognized as authoritative with respect to the Internet (e.g., RFCs), (g) to correct mistakes made by Verisign or any Registrar in connection with a domain name registration, or (h) for the non-payment of fees to Verisign. Verisign also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

ILLEGAL USE

The Services may be used only for lawful purposes. Transmission, distribution or storage of any material via the Services in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates any applicable laws.

SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited and may result in criminal and/or civil liability. Verisign will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- Unauthorized access to or use of data, 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 authorization of Verisign.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.

UNSOLICITED COMMERCIAL EMAIL

To reduce the problem of unsolicited commercial email ("UCE" or "Spam"), Verisign will seek to implement the relevant parts of RFC 2505 - Anti-Spam Recommendations for SMTP MTAs. Notwithstanding Verisign's efforts to deter Spam, users are prohibited from engaging in Spamming activities and may be subject to criminal and/or civil liability to the extent that any user engages in such activities. Examples of Spam include, but are not limited to, the following:

Sending unsolicited bulk mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material. This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements and political tracts. Such material may only be sent to those who have expressly requested it. If a recipient asks to stop receiving such email, then any further sending would constitute Spam and violate this AUP.

- Harassment, whether through language, frequency, or size of messages.
- Creating or forwarding “make-money fast” type messages, “chain letters” or “pyramid schemes” of any type, whether or not the recipient wishes to receive such messages.
- Malicious email, including, but not limited to, flooding a user or site with very large or numerous pieces of email.
- Unauthorized use, or forging, of mail header information (i.e.,spoofing).

SIZE AND RATE LIMITS OF .NAME EMAIL

Verisign reserves the right to restrict the .name email service to operate inside the following restrictions:

- Maximum number of messages in the .name email queue originating from a singular user at a time will be limited to 500, after which Verisign will reserve the right to bounce messages from such user.
- Verisign reserves the right to bounce messages if the total .name email queue for any one user reaches a size of 50 MB.
- Verisign reserves the right to stop forwarding messages that are larger than 20 MB in size.
- Verisign reserves the right to block users that receive more than 3000 emails in any 24-hour period.
- Verisign reserves the right to rate control the number of mails received and the quantity of email forwarded by the .name email service in order to maintain a stable, secure and reliable service.

NON-INTERFERENCE WITH SERVICES

No party may use the Verisign network for actions which restrict or inhibit any person, whether a customer of Verisign or otherwise, in its use or enjoyment of the network or any service or product, including the Services, of Verisign.

CONSUMER PROTECTION

No party may use the Verisign network for any communications or activity which may involve deceptive marketing practices such as the fraudulent offering of products, items, or services. Moreover, no party may furnish false or misleading information to Verisign or any other party through its network, nor shall any party
use the network to facilitate the transmission of private or stolen data such as credit card information (without the cardholder's consent).

NETWORK INTEGRITY

No party may actually, nor attempt to, circumvent user authentication or security of any host, network or accounts, or penetrate security measures (“hacking”) on, related to, or accessed through the Verisign network. This includes, but is not limited to, accessing data not intended for such user, logging into a server or account which such user is not expressly authorized to access, falsifying a username or password, probing the security of other networks, and executing any form of network monitoring which will intercept data not intended for such user. Further, no party shall affect any security breach or disrupt any Internet communications including, but not limited to, accessing data of which such user is not an intended recipient or logging onto a server or account which such user is not expressly authorized to access. For purposes of this section, “disruption” includes, but is not limited to, p ort scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, and attempts to “crash” a host. Finally, no party may utilize the Verisign network in connection with the use of any program, script, command, or sending of messages, designed to interfere with a user's terminal session, by any means, locally or by the Internet.

COMPLIANCE WITH LAW: RESPECTING RIGHTS

No party shall post, transmit, re -transmit, distribute, promote, market, or store material on or through the Verisign network or otherwise using the Services, which (i) is threatening, abusive, hateful, obscene, indecent, or defamatory; (ii) involves the exportation of software or technical information in violation of applicable export control laws; (iii) encourages conduct that may constitute a criminal offense; (iv) constitutes a copyright infringement; or (v) involves the transmission, distribution, or storage of information or data which on its face is in violation of any law or contains a virus.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUP, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A USER OF .NAME EMAIL SHALL BE CONSIDERED VIOLATIONS OF THE AUP BY SUCH USER.

Complaints regarding Illegal Use or System or Network Security issues should be sent to cao@verisign-grs.com.