COS SYSTEMS ACCEPTABLE USE POLICY

1. **Introduction**
   COS Systems AB ("COS") is at all times committed to complying with the laws and regulations governing use of the Internet and e-mail transmission and preserving for all network subscribers ("Network Subscribers") of the participating Networks, Network Subscribers, and/or Service Providers using the COS Products ("Networks, Network Subscribers, and/or Service Providers") the ability to use the applicable Network and the Internet without interference or harassment from other users. This COS Acceptable Use Policy ("AUP") is designed to help achieve these goals. **By using any participating Network, participating service providers agree to comply, and agree to require their Network Subscribers to comply, with this AUP, the COS End User License Agreement and other policies implemented by COS. COS reserves the right to change or modify the terms of this AUP at any time, effective when posted on the COS web site at www.cossystems.com. Network Subscriber's use of the applicable Network, and the COS Products associated therewith, after changes to the AUP are posted online shall constitute acceptance of any changed or additional terms.**

2. **Scope of the AUP**
   The AUP applies to any use of the Network that provides (or includes) access to the Internet and uses COS Products.

3. **Prohibited Activities**

   1. **General Prohibitions:** COS prohibits use of the Network in any way that is unlawful, harmful to or interferes with use of any other systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

      Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, applications, or other services that are accessed via a link from the COS-branded or Network-branded website or from a website that contains COS-branded or Network-branded content is a violation of this AUP.

   2. **Unlawful Activities:** Network and COS Products shall not be used in connection with any criminal, civil or administrative violation of any applicable national or international law, treaty, court order, ordinance, regulation or administrative rule.

   3. **Violation of Intellectual Property Rights:** IP Service(s) shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise

reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of COS or any individual, group or entity, including, without limitation, any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

4. **Threatening Material or Content:** Network and COS Products shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others.

5. **Inappropriate Interaction with Minors:** COS complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the appropriate authority.

6. **Child Pornography:** Network and COS Products shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition shall be reported to COS. COS will report any discovered violation of this prohibition to the appropriate authority and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers; participating Networks, Network Subscribers, and/or Service Providers shall be responsible for the same.

7. **Spam/E-mail/Usenet Abuse:** Spam/E-mail or Usenet abuse is prohibited using Network. Examples of Spam/E-mail or Usenet abuse include but are not limited to the following activities by Network Subscribers (provided, however, the following shall not apply to COS, its affiliates, Network Operators, Service Providers, third party marketing companies or contractors, or any other party with whom COS has a contractual relationship):

    1. sending multiple unsolicited electronic mail messages or "mail-bombing" – to one or more recipient;
    2. sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
    3. sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;

4. sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
5. sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of any network by virtue of quantity, size or otherwise;
6. using another site's mail server to relay mail without the express permission of that site;
7. using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
8. using IP addresses that the Network or Network Subscriber does not have a right to use;
9. collecting the responses from unsolicited electronic messages;
10. maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
11. sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the Network or the Internet (e.g., through language, frequency, size or otherwise);
12. using distribution lists containing addresses that include those who have opted out;
13. sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
14. falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
15. using redirect links in unsolicited commercial e-mail to advertise a website or service;
16. posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
17. intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;
18. knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
19. using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to

violate this AUP or the AUP of any other network or service provider, including, but not limited to, the facilitation of the means to spam.

4. Security Violations

1. Security. Networks, Network Subscribers, and/or Service Providers are responsible for maintaining security of their systems and the machines that connect to and use the Network, and to ensure their Network Subscriber's maintain such security, including implementation of necessary patches and operating system updates.

    Network may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of the COS (or another party's) servers, Networks, Network Subscribers, and/or Service Providers, network access, personal computers or control devices, software or data, or other systems, or to attempt to do any of the foregoing. Examples of system or network security violations include but are not limited to:

    1. unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
    2. hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
    3. impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
    4. using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
    5. distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
    6. knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
    7. engaging in the sale or transmission, or other unlawful activity of pirated software;
    8. using manual or automated means to avoid any use limitations placed on the Network;

9. providing guidance, information or assistance with respect to causing damage or security breach to Network or systems, or to the network of any other network or service provider;

10. failure to take reasonable security precautions to help prevent violation(s) of this AUP.

2. **Network Responsibilities.** Networks, Network Subscribers, and/or Service Providers shall require their Network Subscribers to remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the Network. COS, and its affiliates and business partners, have no responsibility for any material created on a Network, including content provided on third-party websites linked to COS Products. Such third-party website links do not constitute in any way an endorsement by COS of the content(s) of such sites.

5. AUP Enforcement and Notice

1. Failure by Networks, Network Subscribers, and/or Service Providers and/or their Network Subscribers to observe the guidelines set forth in this AUP may result in COS taking actions anywhere from a warning to a suspension or termination of Network usage.

   COS reserves the right, however, to act immediately and without notice to suspend or terminate affected Network and/or Network Subscriber, in response to a court order or government notice that certain conduct must be stopped or when COS reasonably determines, that the conduct may: (1) expose COS to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of the COS network or Networks, Network Subscribers, and/or Service Providers with which the COS Products are interconnected, (3) interfere with another Network's or Network Subscriber's use of the COS Products or the Internet (4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to COS.