

iPass Acceptable Use Policy

Effective 5/3/18

Customer shall be responsible for ensuring that its Users are advised of, and comply with, iPass' acceptable use policy, which may be revised from time to time by iPass (the "Acceptable Use Policy") when using the iPass Network. This Acceptable Use Policy is expressly incorporated into and made a part of this Agreement Without limiting any of its rights or remedies under the Agreement, iPass reserves the right to suspend a User's use of the iPass Network and services in the event such Users do not comply with this Acceptable Use Policy. Each User will:

1. Maintain the confidentiality of their passwords and account information.
2. Not attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal functioning, operation, or security of any network, system, computing facility, equipment, data, or information.
3. Not attempt to gain unauthorized access to, or use, 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 the owner of the system or network. This includes using sniffers or SNMP tools to gain such unauthorized access.
4. Not attempt to circumvent user authentication or security of any host, network or account ("cracking"). This includes, but is not limited to, accessing data not intended for Users, logging into or making use of a server or account Users are not expressly authorized to access, or probing the security of other networks.
5. Not engage in any act of a malicious nature which may reasonably result in harm or damage to another user's service, equipment, or privacy. This includes Syn-flood attacks, or any attempt to overburden a recipient's computer system by sending a high volume of spurious data with the intent to impede functionality, or totally disable recipient system(s), and any other methods of denial of service. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.
6. Not interfere with service to any user, host or network with the intent to render said system dysfunctional including, without limitation, mail-bombing, (sending mass amounts in excess of ten (10) similar mail messages or more than 10MB of data to one recipient or system), flooding, and deliberate attempts to overload a system and broadcast attacks. This includes "denial of service" (DOS) attacks against another network host or individual user.
7. Not operate Maillist, Listserv, 'auto-responders', 'cancel-bots' or similar automated or manual routines which generate excessive amounts of net traffic, or disrupt net newsgroups or email use by others.
8. Not attempt to intercept, redirect, or otherwise interfere with communications intended for others.
9. Not use the Service to transmit excessive volumes of unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient.
10. Not use the Service to send unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e.g., E-mail "Spam"); or distribute, advertise or promote software or services that have the primary purpose of encouraging or facilitating unsolicited commercial E-mail (e.g., email "Spam").
11. Not use the Service for anything other than periodic, active use of email, newsgroups, file transfers, Internet chat, messaging, browsing of the Internet, and other legitimate personal and business use. Users may stay connected so long as they are actively using their connection for these stated purposes. Further, Users may not use the Service on a standby or inactive basis in order to maintain a connection. iPass reserves the right to terminate a User's connection following any extended period of inactivity.

12. Not use another site's mail server to relay mail without the express permission of the site.
13. Not attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than the User for purposes of deception.
14. Not alter, add, remove or modify a source IP address information or by using forged headers (a.k.a. "spoofing") in an effort to deceive or mislead.
15. Not attempt to fraudulently conceal, forge, or otherwise falsify a User's identity in connection with use of the Service.
16. Not use the Service to transmit, distribute, retrieve, or store any information, data, or other material in violation of any applicable law or regulation (including, where applicable any tariff or treaty). This includes, without limitation, 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.
17. Not use the Service to knowingly commit verbal or written threats towards another person. This may include posting or transmitting a person's real life information (name/address/phone number) in a malicious manner.
18. Not use the Service to send threatening or harassing messages which suggest that the sender is planning to engage in some type of criminal activity. Generally, threats to public officials, references to bombings, bank heists, and activities that threaten national security, are considered serious violations.
19. Not use the Service to intentionally transmit files containing a computer virus or corrupted data, or post or transmit any information or software which contains a virus, cancelbot, trojan horse, worm or other harmful component.
20. Not attempt to defeat any idle timer or system tool intended to enforce the part-time and personal nature of User's connection, including the use of pingbots and other methods of avoiding timing disconnection.
21. Not maintain more than one (1) concurrent online sessions per username and password.