

ACCEPTABLE USE POLICY

Background

From time to time ICO may impose reasonable rules and regulations regarding the use of its services in the form of the Acceptable Use Policy (AUP). The AUP is not exhaustive and ICO reserves the right to modify the AUP at any time, effective upon ICO notifying the Customer by e-mail of the modified AUP and by posting the modified AUP to www.ico.com.au.

By registering for and using the services, and thereby accepting the terms and conditions of the Service Level Agreement or its equivalent, you agree to abide by the AUP as modified from time to time. Any violation of the AUP may result in the suspension or termination of your account or such other action as ICO deems appropriate.

An unlisted activity may also be a violation of the AUP if it is illegal, irresponsible, or disruptive use of the Internet. No credits will be issued for any interruption in service resulting from policy violations.

Violation of any AUP is strictly prohibited and may result in the immediate termination or suspension of the services you receive from ICO. You shall remain solely liable and responsible for your use of the services and any and all content that you display, upload, download or transmit through the use of the services.

"Content" includes, without limitation, your e-mail, web pages, personal home pages, and domain names. It is ICO's policy to terminate repeat infringers. ICO reserves the right to refuse service to anyone at any time.

Customer Security Responsibilities

The customer is solely responsible for any breaches of security affecting servers under customer control. If a customer's server is involved in an attack on another server or system, it will be shut down and an immediate investigation will be launched to determine the cause/source of the attack. In such event, the customer is responsible for the cost to rectify any damage done to the customer's server and any other damages caused by the security breach. The labour used to rectify any such damage is categorised as emergency security breach recovery and is currently charged at \$400 AUD per hour. This charge is subject to change without notice. Enquiries regarding security matters may be directed to service@ico.com.au.

System and Network Security

Violations of system or network security are prohibited, and may result in criminal and civil liability. ICO may 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:

- Unauthorised 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 authorisation of the owner of the system or network.
- Unauthorised monitoring of data or traffic on any network or system without express authorisation 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.
- Forging of any TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting.

Violators of the policy are responsible, without limitations, for the cost of labour to clean up and correct any damage done to the operation of the network and business operations supported by the network, and to respond to complaints incurred by ICO. Such labour is categorised as emergency security breach recovery and is currently charged at \$400 AUD per hour required. This charge is subject to change without notice. Enquiries regarding security matters may be directed to service@ico.com.au

Privacy

ICO is concerned with the privacy of online communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, ICO urges its customers to assume that all of their online communications are insecure. ICO will not take responsibility for the security of information transmitted over ICO's facilities.

Password Protection

The customer is responsible for protecting customer's password and for any authorised or unauthorised use made of customer's password. The customer will not use or permit anyone to use ICO's service to guess passwords or to access other systems or networks without authorisation. ICO will fully cooperate with law enforcement authorities in the detection and prosecution of illegal activity.

Internet Etiquette

The customer is expected to be familiar with and to practice good Internet etiquette. The customer will comply with the rules appropriate to any network to which ICO may provide access. The customer should not post, transmit, or permit Internet access to information the customer desires to keep confidential. The customer is not permitted to post any material that is illegal, defamatory, tortious, indecently depicts children or is likely to result in retaliation against ICO by offended users. ICO reserves the right to refuse or terminate service at any time for violation of this section.

Copyright Infringement - Software Piracy Policy

The ICO network may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of Australian or state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights.

Making unauthorised copies of software is a violation of the law, no matter how many copies you are making. If you copy, distribute or install the software in ways that the license does not allow, you are violating copyright law. If caught with pirated software, you or your company may be liable under both civil and criminal law.

Network Responsibility

Customers have a responsibility to use the ICO network responsibly. This includes respecting the other customers of ICO. ICO reserves the right to suspend and or cancel service with any Customer who uses the ICO network in such a way that adversely affects other ICO customers. This includes but is not limited to:

- attacking or attempting to gain unauthorised access to servers and services that belong to ICO or its customers (i.e. computer hacking), and/or
- participating in behaviour which result in reprisals that adversely affect the ICO network or other customers' access to the ICO network.

ICO will react strongly to any use or attempted use of an Internet account or computer without the owner's authorisation. Such attempts include, but are not limited to, "Internet Scanning" (tricking other people into releasing their passwords), password robbery, security hole scanning, port scanning, etc. Any unauthorised use of accounts or computers by an ICO customer, whether or not the attacked account or computer belongs to ICO, will result in severe action being taken against the attacker. Possible actions include warnings, account suspension or cancellation, and civil or criminal legal action, depending on the seriousness of the attack. Any attempt to undermine or cause harm to a server, or customer, of ICO is strictly prohibited.

Lawful Purpose

All services may be used for lawful purposes only. Transmission, storage, or presentation of any information, data or material in violation of any applicable law, regulation, or AUP is prohibited. This includes, but is not limited to copyrighted material or material protected by trade secret and other statute or dissemination of harmful or fraudulent content.

Using any ICO service or product for the purpose of participating in any activity dealing with subject matters that are prohibited under applicable law is prohibited.

Any conduct that constitutes harassment, fraud, stalking, abuse, or other violations in connection with use of ICO services or products is prohibited. Using the ICO network to solicit the performance of any illegal activity is also prohibited, even if the activity itself is not performed. In addition, knowingly receiving or downloading a file that cannot be legally distributed, even without the act of distribution, is prohibited.

Servers hosted within ICO network may be open to the public. You are solely responsible for your usage of the ICO network and servers and any statement you make on servers hosted within the ICO network may be deemed "publication" of the information entered. Acknowledging the foregoing, you specifically agree not to use our service in any manner that is illegal or defamatory.

Commercial Advertisements with E-mail

ICO takes a zero tolerance approach to the sending of Unsolicited Commercial E-mail or SPAM over our network. Very simply, this means that customers of ICO may not use or permit others to use our network to send SPAM. Customers of ICO may not host, or permit hosting of, sites or information that is advertised by SPAM from other networks. Violations of this policy carry severe penalties, including termination of service.

Sending a message, especially an advertisement, to more than five recipients, is by itself spamming unless the individuals have specifically requested to be added to a mailing list on that topic. This includes both commercial advertisements and informational messages sent to recipients via electronic mail (email) as well as off-topic messages posted in discussion groups where the recipient has not requested or invited the message. E-mail is a person-to-person medium, not a broadcast medium.

Customers of ICO are strictly prohibited from using or permitting others to use SPAM over our network. As our Customers are ultimately responsible for the actions of their clients over the ICO network, it is advisable that Customers develop a similar, or stricter, policy for their clients. Violation of ICO's SPAM policy will result in severe penalties. Upon notification of an alleged violation of our SPAM policy, ICO will initiate an immediate investigation (within 48 hours of notification). ICO will notify the Customer immediately about any allegations made against the Customer in relation to ICO's SPAM policy.

During the investigation, ICO may restrict customer access to the network to prevent further violations. If a customer is found to be in violation of our SPAM policy, ICO may, at its sole discretion, restrict, suspend or terminate the customer's account. Further, ICO reserves the right to pursue civil remedies for any costs associated with the investigation of a substantiated policy violation. ICO will notify law enforcement officials if the violation is believed to be a criminal offense. Violation of ICO's SPAM policy may be reported to abuse@ico.com.au

IP Address Overlap

ICO administers the network on which customer servers reside. The customer cannot use IP addresses which were not assigned to them by ICO staff. Any server found using IPs which were not officially assigned will be suspended from network access until such time as the IP addresses overlap can be corrected.

Billing

The customer understands that the customer is responsible for paying for any network resources that are used to connect the customer's server to the Internet. The customer may request that the customer's server be disconnected from the Internet, but the customer will still be responsible for paying for any network resources used up to the point of suspension or cancellation.

Suspension

ICO reserves the right to suspend network access to any customer if, in the judgment of the ICO network administrators, the customer's server is the source or target of the violation of any of the other terms of the AUP or for any other reason. If inappropriate activity is detected, all accounts of the Customer in question will be deactivated until an investigation is complete. ICO will endeavour to provide the Customer with written notification about such suspension, however, prior notification to the Customer is not assured. In extreme cases, law enforcement agencies may be contacted regarding the activity. The customer will not be credited for the time the customer's machines were suspended. The Customer will be credited on a pro-rata basis based on the monthly fees the Customer pays for the servers that are suspended for the time the Customer's machines were suspended.

Cancellation

ICO reserves the right to cancel service at any time. If inappropriate activity is detected, all accounts of the customer in question will be deactivated until an investigation is complete. ICO will endeavour to provide written notification to the Customer about such termination, however, prior notification to the Customer is not assured. In extreme cases, law enforcement agencies may be contacted regarding the activity. All fees paid in advance of cancellation will be prorated and paid by ICO if ICO institutes its right of cancellation. Any violation of policies which results in extra costs to ICO will be billed to the Customer (i.e. transfer, space etc.).

Disclaimer of Responsibility

ICO is under no duty to look at each customer's or user's activities to determine if a violation of the AUP has occurred, nor do we assume any responsibility through our AUP to monitor or police Internet-related activities. ICO disclaims any responsibility for any such inappropriate use and any liability to any person or party for any other person's or party's violation of this policy. All Sub-Networks, resellers, managed and unmanaged servers of ICO must adhere to the above policies. Failure to follow any term or condition will be grounds for immediate Cancellation.

Indirect or attempted violations of the AUP and actual or attempted violations of the AUP and actual or attempted violations by a third party on your behalf, shall be considered violations of the AUP by you.