Fair use Policy

This Fair Use Policy applies to all services that you purchase from Audit IT.

This Fair Use Policy should be read in conjunction with any product/service specific Terms and Conditions and forms part of your Agreement.

1. **General**

1.1. This policy is designed to ensure that your use of Services does not break any laws, hinder the efficient operation of our network, interfere with the rights of other customers, or interfere more generally with the rights of end users.

1.2. You are responsible for ensuring that use of the service complies with this policy. You are also responsible for any use of the service by any user, including an End User to whom you supply the service.

1.3. "You" means you, an employee of your company, or the End User to whom you supply the service, or any other user.

1.4. "service/services" means any service you obtain from Audit IT.

1.5. You should consult this policy regularly to ensure that your activities conform to the most recent version.

1.6. If there is an inconsistency between the Terms and Conditions of the Service, and this policy, this policy will apply.

1.7. If you become aware of any violations of this policy by other users you should contact us.

2. **Illegal Activity**

2.1. You must not use the service for any activity that breaches any law or violates any local, state, federal or international law, order, regulation or industry code of practice. Prohibited activities include (but are not limited to):

2.2.1. posting, disseminating, or in some cases accessing, content which is unlawful, including:

2.2.1.1. content that is or would be classified by the Classification Board as RC rated or X rated and that is or would be classified by the Classification Board as R rated where a restricted access system is not in place,

2.2.1.2. content which violates the copyright or other intellectual property rights of others. You assume all risks regarding the determination of whether material is in the public domain, or

2.2.1.3. content that defames, harasses or abuses anyone or violates their privacy,

2.2.1.4. pyramid or other illegal soliciting schemes, or any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature.

3. **Security**

3.1. You are responsible for any misuse of a service; this includes paying any costs (including call costs) associated with the misuse of a service.

3.2. Where Audit IT incurs costs associated with a misuse of any service, you may be liable for the payment of these costs.

3.3. You agree to indemnify Audit IT against the consequences of any misuse of a service by you.

3.4. You must take all practical steps to ensure that others do not gain unauthorised access to any service.

3.5. The service must not be used to obtain or attempt to obtain unauthorised access to any computer, system or network. If you do not have authorisation, prohibited activities include (but are not limited to):

3.5.1. accessing, monitoring or using any data, systems or networks,

3.5.2. probing, scanning or testing the vulnerability of a system or network,

3.5.3. breaching any security or authentication measures for a system or network,

3.5.4. accessing the account or private information of any other person or entity,

3.5.5. accessing any server in violation of any acceptable use policy of that server, including any attempt to do any of the things mentioned in paragraphs (i) to (iv) above.

3.6. You must not:

3.6.1. use (or attempt to use) or distribute tools designed for compromising security including, but not limited to, password guessing programs, cracking tools, packet sniffers or network probing tools,

3.6.2. knowingly transmit or disseminate any information or software, which contains a virus or other harmful feature,

3.6.3. use (or attempt to use) the service in a manner that may interfere with the technical operation of the service or any other computer, system, network or telecommunications services, including (but not Fair Use Policy limited to) denial of service attacks, flooding of a network, overloading a service, improper seizing and abuse of operator privileges and attempts to 'crash' a host, or

3.6.4. interfere (or attempt to interfere) with the regular workings of our systems or network connections.

3.7. You are solely responsible for the security of any device you choose to connect to the service, including any data stored on that device.

3.8. We recommend against enabling file or printer sharing of any sort. We recommend that any files or services you unauthorised access.

3.9. You must notify us immediately of any unauthorised or attempted unauthorised use of your service and any other breach or attempted breach of security.

4. Risks of the Internet

4.1. Some activities that you can perform when accessing the Internet may be harmful or cause loss to you, other people that may access your service, or your equipment. Typical activities include (but are not limited to):

4.1.1. downloading content (including receiving emails) from the Internet which may introduce viruses or other harmful features to your computer,

4.1.2. purchasing goods or services using the Internet,

4.1.3. transmitting confidential information over the Internet (such as your credit card number or other personal information), or

4.1.4. accessing and viewing content on the Internet or otherwise available through the service that may be offensive to some individuals, or inappropriate for children (for example, it is possible to obtain access to content that is pornographic, offensive and/or unsuitable for children).

4.2. You bear all risk associated with the activities referred to above, and we do not have any liability for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to such activities.

4.3. You may minimise the risk of accessing illegal or offensive content as well as managing use of the Internet by using a filtering solution. We will provide access to one or more of these filtering solutions at a reasonable cost to you as part of the service.

4.4. You have the right to make complaints to the Australian Communications and Media Authority about Internet content which is or would classified by the Classification Board as X rated, RC rated, or R rated and does not have a restricted access system in place.

5. Content Publishing

5.1. You are solely responsible for any content that you publish via websites, email, newsgroups, online forums or other publishing mediums accessed via the service.

5.2. You must not publish material that is or would be classified by the Classification Board as RC rated or X rated via websites, email, newsgroups or other publishing mediums accessible via the service.

5.3. You must take appropriate precautions to prevent minors from accessing or receiving any content you have published that may be inappropriate for them. This includes implementing a restricted access system on content that is or would be classified by the Classification Board as R rated. We also encourage you to use

appropriate warnings

6. Automated Applications

6.1. If automated programs or programs that maintain a persistent connection to a remote service are used, they must only be used when you are physically present at the computer. These activities include (but are not limited to) automated file downloading, IRC 'bots', continuous streaming media and peer-to-peer file sharing applications.

7. IP Voice Reasonable Use

7.1. In the event of Excessive Usage of the Service by the Customer, Audit IT may require Customer:

7.1.1. To reduce the use of the Service, in the case of untimed calls; and/or

7.1.2. Pay additional charges to recover any costs or losses incurred by such excessive usage. Such charges shall be based on timed national call rate as per Audit IT's then current pricing schedule; and/or Cancel the Service for Customer or certain of Customer's End Users.

7.2. Customer agrees that Audit IT may republish/revise its Excessive Usage Policy at any time during the Term.

7.3. For the purposes of this Agreement "Excessive Usage" shall include, but is not limited to:

7.3.1. Average call duration that exceeds 9 minutes where calls are untimed.

7.3.2. An inbound to outbound ratio of calls that exceeds 3:1; and/or Fair Use Policy

7.3.3. Any other metric that Audit IT informs Customer in writing.

7.4. As a requirement of the Legal Intercept Plan, no asymmetrical routing of traffic is permitted. Audit IT stipulates that for the services associated with the numbers routed by Audit IT to Customer, Customer cannot (except in the situation of failure of the service offered by Audit IT) route outbound voice traffic via a third party carrier.

8. Violation of Fair Use Policy

8.1. If you, or someone with access (including unauthorised access) to a service, use the service in a way that we reasonably believe violates this policy, we may take any responsive action we deem appropriate.

8.2. Such actions may include (but are not limited to) the immediate suspension or cancellation of all or any portion of the service.

8.3. We may take any other legal or technical action we deem appropriate, including taking action against offenders to recover the costs and expenses of identifying them. If your use of the service causes a loss to third parties and we are required to pay compensation, we require you to reimburse us.

8.4. We are not obligated to regularly monitor your usage of the service however we reserve the right to monitor your use of the service to identify violations of this policy, and to protect our network, the other users of this service, and other Internet users.

8.5. We reserve the right to investigate any use of a service that we reasonably suspect violates this policy, including the gathering of information from the user(s) involved and the complaining party, if any, and examination of transmissions and material on our servers and network. During an investigation, we may suspend the IS Access services involved, and / or interrupt transmissions.

8.6. In order to enforce this policy, you authorise us (or our agents) to cooperate with:

8.6.1. law enforcement authorities in the investigation of suspected criminal violations, and

8.6.2. system administrators at other Internet service providers or other network or computing facilities.

8.6.3. Such cooperation may include us providing, for example, the username, IP

address or other identifying information about a user.

8.7. Any failure by us to enforce this policy, for whatever reason, shall not necessarily be construed as a waiver of any right to do so at any time.

8.8. You agree that, if any portion of this policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect.

8.9. This policy is governed by the laws of the Commonwealth of Australia and the laws of the state or territory in which you normally reside. You and we submit to the exclusive jurisdiction of the courts of the Commonwealth, and its states and territories.

9. **Unreasonable Use**

9.1. Audit IT services are designed to meet the requirements of businesses, and we consider your use of the service to be unreasonable if:

9.1.1. your usage of the service affects other customers' access to the network; or

9.1.2. you set up switch devices which potentially keeping a session open for hours and limiting the ability for other customers to access the service:

9.1.3. we reasonably believe you have breached this Fair Use Policy.

9.2. If we consider, at our sole discretion, that you have made unreasonable use of the service, we may terminate the service, temporarily suspend the service, or ask you to change the way in which you use the service.

9.3. If we terminate the service, you are liable for any early termination payment to us.

9.4. If we block your service, you are not entitled to claim back any charges that may have levied for the period of the suspension.