

Acceptable Use Policy

1. General

Attenda ("**Attenda**") provides managed hosting services for clients' websites and business critical applications and other related services (each, a "**Service**" and collectively the "**Services**"). A "**Client**" is any party who purchases a Service from Attenda. The "**Client Personnel**" consists of its employees, agents, sub-contractors (other than Attenda) and the Client's own customers

This document defines the Acceptable Use Policy ("**AUP**") of the Services with a view of ensuring the integrity, security and reliability of Attenda network, systems, products, services, server hosting facilities and data contained therein (collectively, the "**Attenda Network**").

2. Prohibited Activities

It is contrary to Attenda policy for any of its Clients or other Service user to effect or participate in any of the activities listed below (whether actual or attempted and whether directly or indirectly) through a Service.

Each of the below practices (each, a "**Prohibited Activity**") and any other similar activities constitutes abuse of Attenda's Services, network and facilities and interferes with other Service users. Accordingly, the Client shall not and shall ensure that the Client Personnel shall not:

- 2.1. Unauthorised Use:** Obtain or attempt to obtain unauthorised access to any account, network, internet service, computer or computer resource not belonging to that user, end user or user account;
- 2.2. Alteration of Information:** Engage in or attempt unauthorised access, alteration, corruption or destruction of information belonging to Attenda and/or any Attenda Client or falsifying user or other Service related information;
- 2.3. Interference to Network etc.:** Use Attenda Services to interfere with or degrade any service to any user, end user, user account, host or network, deliberately attempting to overload a service and/or attempting to crash a host, including but not limited to flooding networks, sending unsolicited bulk e-mail, denial of service attacks and mail bombing;
- 2.4. Interference to Communications:** Use any kind of program, script or command, or send messages of any kind, that are designed to or that cause any other party to interfere with a user's data communications, regardless of means, whether locally or via the Internet;
- 2.5. Covert Transmissions:** Intentionally omit, delete, fraudulently amend or misrepresent information transmitted or to be transmitted through the Services, including but not limited to TCP-IP header information, return-address information and Internet Protocol addresses ("spoofing"), or taking any other action intended to conceal or misrepresent the identity or contact information of the Client or its users;
- 2.6. Breach of Security:** Store and/or distribute materials and/or tools intended to breach or infiltrate security arrangements or attempt to scan, penetrate, bypass, test the vulnerability of (without Attenda's consent and co-operation) or engage in any activity which may threaten the security or integrity of any network or service (including but not limited to transmission of worms, viruses, logic bombs, Trojan horses, and other malicious codes and accessing any device or data without proper authorisation) whether by passive or intrusive techniques;

- 2.7. Inappropriate Monitoring:** Use the service to store, send or distribute software that covertly gathers information or covertly transmits information about any user or network, including e-mail addresses, screen names or any other personal identifiable information;
- 2.8. Inappropriate Software Products and Services:** Use or allow the Services to be used to promote illegal activities including allowing, permitting or facilitating the transmission, promotion or otherwise making available any software product or service that is either illegal or designed to cause or facilitate the hacking of any site.
- 2.9. Inappropriate Content:** Use or allow the Services to be used for publishing or transmitting content which is inappropriate or otherwise in breach of applicable law. The Client shall immediately implement a "notice and take down" procedure in respect of any content which is or may be reasonably considered to be inappropriate or in breach of applicable law which the Client's Personnel (other than the Client's customers) becomes aware and shall notify Attenda accordingly. Such inappropriate content shall include, but not be limited to content (or links to content) which Attenda reasonably believes:
- 2.9.1.** is illegal or promotes in any way any illegal act;
 - 2.9.2.** defames or otherwise violates a person's privacy;
 - 2.9.3.** depicts, promotes or relates in any manner to child pornography, pornography generally or sexual activity of any kind;
 - 2.9.4.** is violent, incites violence or threatens violence;
 - 2.9.5.** contains content which may be considered abusive, harassing or contain hate speech whether in respect of any individual or group of individuals or in respect of any gender, race, religion or ethnicity;
 - 2.9.6.** is deceptive under the appropriate consumer protection laws, including chain letters and pyramid schemes;
 - 2.9.7.** creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security or interferes with a police investigation or any other lawful investigation;
 - 2.9.8.** exposes sensitive commercial data, trade secrets or other confidential or proprietary information of another person, group or organisation;
 - 2.9.9.** bypasses or promotes information intended to bypass copyright or license protections;
 - 2.9.10.** infringes copyright, trade or service mark, patent or other property right;
 - 2.9.11.** promotes illegal drugs, trafficking, money laundering, or violates export control laws;
 - 2.9.12.** is otherwise malicious, fraudulent or may result in retaliation against Attenda.
- 2.10. Copyrighted Materials:** Use or allow the use of the services to publish, download, distribute or use in any way any image, software, text, data, music, video or other work in contravention of copyright legislation;
- 2.11. Bulk e-mail:** Engage in the despatch of bulk or commercial e-mail, unless approved in advance by Attenda, such approval to be dependent on reassurance to Attenda that:

- 2.11.1. the despatch of bulk e-mail is for legitimate commercial use which shall not include anything that may be considered as phishing, scamming, password robbery, spidering, or harvesting;
 - 2.11.2. the intended recipients have given their consent to receive e-mail;
 - 2.11.3. the Client has procedures in place requiring consent from intended recipients to receive bulk or commercial e-mail, including confirmation that where consent to receive e-mail is given, it is given by the owner of the respective e-mail address, that such evidence of consent is retained in a manner that may be produced on request, and that any such consent may be revoked by the intended recipient at any time;
 - 2.11.4. the Client must post an email address for complaints in a conspicuous place within the body of the e-mail or on any website associated with the e-mail, and must promptly respond to messages sent to that address;
 - 2.11.5. data collected regarding e-mail addresses or any other personal identifiable information is used and stored in accordance with the relevant data protection principles;
 - 2.11.6. the Client must not obscure the source of the e-mail in any manner, or purport to represent any other individual, body or organisation;
 - 2.11.7. the Client must not attempt to send any message to an e-mail address if 3 consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen days;
- 2.12. **IP address abuse:** Engage in any activity that results in any assigned IP addresses being listed on an abuse database;
- 2.13. **Accepted internet standards:** Engage in any activity that is likely to violate generally accepted standards of the internet, other networks conduct and usages, or codes of conduct including but not limited to any denial of service attacks, web page defacement, port and network scanning and unauthorised system penetrations;
- 2.14. **Applicable laws:** Failing to comply with any applicable law or regulation.

3. Rights and Remedies

Attenda may suspend and/or terminate a Client's Service at any time for any failure of Client, or the Client Personnel to comply with this policy or for engaging (or permitting others to engage) in any Prohibited Activity or similar/related activity.

Nothing in this Acceptable Use Policy limits Attenda's rights and remedies (available at law or in equity) in any way with respect to any Prohibited Activity. Attenda shall fully co-operate with any law enforcement authorities or court order requesting or directing Attenda to disclose the identity or locate anyone posting any material in breach of this policy.

4. Password Protection

Users are responsible for protecting their password and for any authorised or unauthorised use made of their password. Users will not use or permit anyone to use Attenda's Service to guess passwords or access other

systems or networks without written authorisation. If a user suspects that their password is known to another person, then they shall contact Attenda immediately to arrange for a new password to be issued.

THE CLIENT SHALL INDEMNIFY AND KEEP ATTENDA INDEMNIFIED AGAINST ALL DAMAGES, CLAIMS, COSTS, LOSSES AND LIABILITIES SUFFERED OR INCURRED BY ATTENDA AS A RESULT OF ANY BREACH (OR ANY SUSPECTED BREACH) OF THIS POLICY

5. Modification of This Policy

Attenda reserves its sole right to change this policy from time to time and such amended policy shall be enforced from the earlier of fourteen (14) days from the date of publication, or immediately upon its notification to the Client.

IT IS RECOMMENDED THAT YOU PRINT A COPY OF THIS POLICY FOR YOUR OWN REFERENCE PURPOSES

Issue Date: August 2011