

ATHAEM Managed Hosting

ACCEPTABLE USE POLICY

This Acceptable Use Policy (“AUP”) describes activities prohibited on the Athaem network for the protection of Athaem and its Representatives, Services, network and other customers. Questions regarding this policy should be directed to abuse@Athaem.com.

1. **ABUSE.** Customer shall not use Athaem's Services or network to engage in, foster, solicit or promote illegal, abusive or irresponsible behavior including:
 - a. conduct likely to breach any laws, codes or regulations applicable to the parties (including conduct infringing or misappropriating intellectual property, trade secrets, confidential or proprietary information; or which is fraudulent, unfair, deceptive or defamatory);
 - b. unauthorized access to, monitoring or use of, or interference with an internet account, computer, systems, networks, data or traffic;
 - c. intentionally, knowingly or recklessly introducing any malicious code into the Services;
 - d. conduct violating rules and conventions of any domain registrar, email service, bulletin board, chat group, or forum used in conjunction with Athaem Services or network (including using false, misleading or deceptive TCP-IP packet header information in an email or newsgroup posting);
 - e. deceitfully collecting, transmitting or using information, or distributing software which covertly gathers or transmits information about a user;
 - f. distributing advertisement delivery software unless the user affirmatively consents to download and installation based on clear and conspicuous notice of the nature of the software, and can easily remove software using standard tools included on major operating systems;
 - g. conduct likely to result in retaliation or adverse action against Athaem or its services, network, website or Representatives (including resulting in listing of Athaem IP space on an abuse database);
 - h. conduct intended to withhold or cloak identity or contact information, registering to use Services under a false name, or using an invalid or unauthorized credit card in connection with Services;
 - i. gambling activity violating any applicable codes of practice, required licenses or technical standards;
 - j. use of any Athaem provided shared system in a way that unnecessarily interferes with the normal operation of the shared system, or consumes a disproportionate share of system resources; and
 - k. conduct creating a risk to safety or health, national security or law enforcement.
2. **OFFENSIVE BEHAVIOR.** Customer shall not be abusive or offensive to Athaem Representatives. Customer shall not publish, transmit or store on or via the Services content or links to content that Athaem reasonably believes relates in any manner to child pornography, bestiality, non-consensual sex acts, or live sex acts; or is excessively violent, incites or threatens violence, contains harassing content or hate speech, violates a person's privacy, is malicious or morally repugnant.
3. **NO HIGH RISK USE.** Customer shall not use the Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities).
4. **MAIL REQUIREMENTS.** For bulk or commercial email sent by or on behalf of Customer using the Services or from any network that directly or indirectly refers recipients to a site hosted using the Services (including using third party distribution lists), Customer shall:
 - a. post a privacy policy for each associated domain;
 - b. post an email address for complaints in a conspicuous place on any associated website, promptly respond to messages sent to that address, and have means to track anonymous complaints;
 - c. obtain affirmative consent to receive e-mail from intended recipients using reasonable means to verify ownership of the e-mail address, honor and notify recipients of consent revocation, and evidence consent within 72 hours of recipient or Athaem request; and
 - d. include the recipient's e-mail address in the e-mail body or "TO" line.

5. **VULNERABILITY TESTING.** Customer shall not attempt to test the vulnerability of a Athaem system or network, or attempt to breach Athaem security measures, by any means (Customer may conduct vulnerability testing of their Hosted System only with Athaem's prior written consent).
6. **EXPORT CONTROL.** Customer shall ensure Services are not used in breach of export laws, controls, regulations or sanction policies of the United States or Customer's applicable jurisdiction. Customer shall ensure Services are not used by any person or entity suspected of involvement or affiliation with those involved in activities or causes relating to: human trafficking; illegal gambling; terrorism; narcotics trafficking; arms trafficking or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical, or biological weapons, weapons of mass destruction, or missiles.
7. **COOPERATION WITH INVESTIGATIONS AND PROCEEDINGS.** Customer agrees Athaem may permit a relevant authority to inspect Customer's content or traffic if Athaem is legally required to do so, provided Athaem gives Customer reasonable prior notice (where permitted by applicable law and regulation). Athaem may report to appropriate authorities any Customer conduct Athaem believes violates applicable law without notice to Customer (including providing any information about Customer, its users or traffic). Athaem may cooperate in response to a formal request from a law enforcement or regulatory agency investigating conduct Athaem believes violates applicable law, or in a civil action that on its face meets the requirements for such a request.
8. **DOMAIN NAMES, IP ADDRESSES AND DNS RECORDS.** Customer shall maintain valid information with Customer's domain name registrar for any domain hosted on the Athaem network, and only use IP addresses assigned to Customer by Athaem in connection with the Services. Customer agrees Athaem may modify, transfer or delete any DNS record or zone on Athaem managed or operated DNS servers or services upon request from the registrant or administrative contact according to the registrar's WHOIS system.
9. **CHANGES TO AUP.** Athaem may amend the AUP by publishing a revised version at www.Athaem.com/information/legal/aup, or in the event of a material adverse AUP change by providing Customer 30 days written notice. The revised AUP shall become effective as to Customer on the first to occur of:
 - a. Customer's execution of a new or additional agreement for all or part of the Services incorporating the revised AUP,
 - b. the first day of an Agreement renewal term beginning at least 30 days after revised AUP publication, or
 - c. expiry of written notice of material adverse AUP change. If compliance with the revised AUP would adversely affect Customer's use of the Services, Customer may terminate the affected Services (without payment of an early termination fee) by giving Athaem written notice of Customer's objection no later than 30 days following the date that the revised AUP would otherwise have become effective as to Customer; Customer may continue using the Services for up to an additional 90 days subject to the prior version of the AUP; and Athaem may decide to waive the AUP change as to Customer in which case the notice of termination shall be of no effect.
10. **AUP BREACH.** If Customer breaches the AUP (including unintentionally, resulting from Customer's failure to use reasonable security precautions, or as a result of activity occurring without Customer authorization) Athaem may block any content or traffic, suspend the Services, or terminate the Services in accordance with the Agreement. No credit shall be available under any Service Level Agreement for interruptions of Services resulting from AUP breach. Customer's use of the Services to assist another person in an activity that would breach this AUP if performed by Customer is an AUP breach.