

This page contains the Acceptable Use Policy ("AUP") and the Zero SPAM Policy under which you and/or your users (collectively, "Client") use Email, Email Marketing and On Demand Streaming Media Services. Client acknowledges and agrees to be bound by all the terms, conditions, and policies of the AUP, as set forth herein, including any future amendments.

Client acknowledges and agrees that it is responsible for continual compliance of this policy, in order to ensure the integrity, security and reliability of the Email, Email Marketing and Streaming Services and its networks, systems, facilities and data.

Consequences of Unacceptable Use

Service Provider reserves the right to suspend or terminate Client's access to the Email Services upon notice of a violation of this policy. Indirect or attempted violations of this policy, and actual or attempted violations by a third party on behalf of Client, shall be considered violations of this policy by Client.

Sending

Client may not send, or attempt to send, unsolicited email messages ("SPAM"). It is not only annoying to Internet users; it violates many federal and state laws and seriously affects the efficiency and cost-effectiveness of Email and Email Marketing Services. Sending can lead to industry blacklisting of Client's business and mail servers, resulting in interruption and/or termination of Client's Email and Email Marketing Services.

Service Provider will allow 1 click per 1,000 emails sent. If an account goes over this maximum limit then Service Provider will look for, in its system, the "closed-loop-confirmation" or the web form opt-in for the subscriber(s) in question. A "closed-loop-confirmation" is a confirmation email opt-in. A web form is a web form generated in the Service Provider's Web Form section. If there is no such record of the subscriber opting-in, via either method, then the Service Provider reserves the right to close Client's account for abuse and report Client to the proper authorities.

Specifically, Client agrees NOT to:

- Send, or attempt to send, of any kind from the Service Provider Network
- Send, or attempt to send, of any kind from third-party networks using a return email address that is hosted on the Service Provider Network, or referencing an email address hosted on the Service Provider Network
- Send email messages which result in complaints from the recipient or from the recipient's email provider, or which result in blacklisting of the sender's email address or mail server
- Send email messages which are excessive and/or intended to harass or annoy others
- Continue to send email to a recipient that has indicated that he/she does not wish to receive it
- Take any actions intended to cloak the Client's identity or contact information, including but not limited to intentionally omitting, deleting, forging or misrepresenting message headers or return addresses
- Take any other action that results in blacklisting of the sender's email address or mail server, or negatively impacts other Clients who use the Email Services

In the absence of positive, verifiable proof to the contrary, Service Provider considers complaints by recipients of emails to be de-facto proof that the recipient did not subscribe or otherwise request the email(s) about which a complaint was generated.

Past or present violations of this policy by Client at other email providers will be considered a violation of this policy and will be grounds for Service Provider to suspend or terminate Client's access to the Email Services.

You also cannot, in any way implicate our services in the use of SPAM. This includes, but is not limited to mentioning of an AttainResponse.com email address or URL in a bulk message or including these addresses on a bulk-advertised web page. You also can not hide behind throwaway web pages or fax-response front ends.

We log every IP or dial up address of anyone who logs onto our server or into any of the Control Panels to protect our clients and our business.

Even if AttainResponse services are not directly involved, it will lead to:

- IMMEDIATELY terminating your account, with no refund
- Charge you \$40 per hour for any interruption of our service
- Report your activities to your service provider and dial up service
- Give any information we have to the people being Spammed so they can take whatever action they feel necessary
- Take legal action to recover our money if necessary
- Block you from receiving any access to services

If you have been spammed, please notify abuse@attainresponse.com.

Sending "Opt-in" Bulk Email from the Business Email Hosting System

Client may not use the Email Services to send "Opt-in" Bulk Email. This is what the Email Marketing Service is used for. Service Provider defines "Opt-in" Bulk Email ("Bulk Email") as email messages of similar content that are sent to more than 250 recipients within a relatively short period of time.

The term "Opt-in" means that the recipients have signed up to receive the emails voluntarily, and implies that the Bulk Email is not. Service Provider has measures in place to prevent Bulk Email from being sent through its business email servers, and any attempt to do so may not be delivered and may result in interruption and/or termination of Client's Email Services.

Attempts to circumvent this Bulk Email restriction by breaking up bulk mailings over a period of time or by sending from multiple email accounts will itself be considered a violation of this policy.

Additionally, the Service Provider Business Email Network is not set up to process bounce messages for Bulk Email, like our Email Marketing Network is. Therefore, Client may not send Bulk Email from third-party networks using a return address that is hosted on the Service Provider Network, unless Client takes extreme care to prevent more than 100 bounce emails from arriving to the Service Provider Network as the result of sending Bulk Email from a third-party network.

Receiving Bulk Email

Client may not use the Email Services for the purpose of receiving Bulk Email. Submitting any email address that is hosted on the Service Provider Network to Bulk Mail organizations such as Safe lists, FFAs and databases is expressly prohibited. Client agrees to grant Service Provider the right to block Bulk Mail from such organizations.

Security

Client is prohibited from violating, or attempting to violate, the security of the Service Provider Network. Any violations may result in criminal and civil liabilities to the Client. Service Provider will investigate any alleged violations and will cooperate with law enforcement agencies if a criminal violation is suspected. Examples of violations of the security of the Service Provider Network include, but are not limited to: (i) accessing data not intended for Client, (ii) logging into a server or account which the Client is not authorized to access, (iii) attempting to probe, scan or test the vulnerability of a system, (iv) breach of security or authentication measures, (v) attempting to interfere with service to any User, host or network, or (vi) taking any action in order to obtain services to which the Client is not entitled.

Illegal Use

The Services may only be used for lawful purposes. For example, Client may not use the Service Provider Network to post, transmit, retransmit, create, distribute, or store content that, in the sole judgment of the Service Provider:

- (i) Violates a trademark, copyright, trade secret or other intellectual property rights of Others
- (ii) Violates export control laws or regulations
- (iii) Violates the privacy, publicity or other personal rights of others
- (iv) Impairs the privacy of communications
- (v) Contains obscene, offensive, unlawful, defamatory, harassing, abusive, fraudulent, or otherwise objectionable content as reasonably determined by Service Provider
- (vi) Encourages conduct that would constitute a criminal offense or give rise to civil liability
- (vii) Constitutes deceptive on-line marketing
- (viii) Violates reasonable regulations of Service Provider or other service providers
- (ix) Causes technical disturbances to the Service Provider Network, its partner networks or the network used by Client to access the Services, or violate the policies of such networks, including, but not limited to, intentional introduction of any viruses, Trojan horses, worms, time bombs, cancel bots or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system or data, or
- (x) Assists, encourages or permits any persons in engaging in any of the activities described in this section. If Client becomes aware of any such activities, Client is obligated to immediately notify Service Provider and take all other appropriate actions to cause such activities to cease.

Client is responsible for all content that is transmitted, received and stored by Service Provider through Client's use of the Email Services. Service Provider takes no responsibility for content passing through or stored on the Service Provider Network, including but not limited to, viruses, mail floods or other disabling features, or content provided on third party web sites that are linked to by content passing through or stored on the Service Provider Network. Service Provider does not adopt, nor warrant the accuracy of the content of any linked Web site and undertakes no responsibility to update the content. Use of any information obtained via the Service Provider Network is at Client's own risk.

Specific to Email Marketing

Client Security Obligation

Each Client must use reasonable care in keeping each server or network devices attached to AttainResponse infrastructure up-to-date and patched with the latest security updates. Failure to use reasonable care to protect your server may result in a security compromise by outside sources.

AttainResponse is not responsible for Client server level security unless a security administration package, firewall security administration package or fully managed operating system package is contracted for. A compromised server creating network interference will result in immediate Client notification and will be disconnected from the network immediately so as to not directly affect other Clients. No service credits will be issued for outages resulting from disconnection due directly to breached server security.

The Client is solely responsible for any breaches of security affecting servers under Client control. If a Client intentionally creates a security breach, the cost to resolve any damage to Client's server or other servers will be charged directly to the Client.

System and Network Security

Violations of system or network security are strictly prohibited, and may result in criminal and civil liability. AttainResponse investigates all incidents involving such violations and will cooperate with law enforcement if a criminal violation is suspected.

Examples of system or network security violations include, without limitation, the following:

1. Introduction of malicious programs into the network or server (example: viruses, worms, Trojan Horses and other executables intended to inflict harm).
2. Effecting security breaches or disruptions of Internet communication and/or connectivity. Security breaches include, but are not limited to, accessing data of which the Client is not an intended recipient or logging into a server or account that the Client is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to port scans, flood pings, email-bombing, packet spoofing, IP spoofing and forged routing information.
3. Executing any form of network activity that will intercept data not intended for the Client's server.
4. Circumventing user authentication or security of any host, network or account.
5. Interfering with or denying service to any user other than the Client's host (example: denial of service attack or distributed denial of service attack).
6. Using any program script/command, or sending messages of any kind, designed to interfere with or to disable, a user's terminal session, via any means, locally or via the Internet.
7. Failing to comply with the Company's procedure relating to the activities of Clients on the Company's premises. Violators of the policy are responsible, without limitations, for the cost of labor to correct all damage done to the operation of the network and business operations supported by the network. Such labor is categorized as emergency security breach recovery and is currently charged at \$295 USD per hour required. Network interference by any Clients that may cause or is currently causing network interference with another Client will be disconnected immediately. No service credits will be issued to Clients disconnected for network violations.

Internet Etiquette

Each Client is expected to execute reasonable Internet etiquette. The Client will comply with the rules appropriate to any network to which AttainResponse may provide access. The Client should not post, transmit, or permit Internet access to information the Client desires to keep confidential.

The Client is not permitted to post any material that is illegal, libelous, and tortuous, indecently depicts children or is likely to result in retaliation against AttainResponse by offended users.

AttainResponse reserves the right to refuse or terminate service at any time for violation of this section. This includes advertising services or sites via IRC or USENET in clear violation of the policies of the IRC channel or USENET group.

Child Pornography

AttainResponse will cooperate fully with any criminal investigation into a Client's violation of the Child Protection Act of 1984 concerning child pornography. Clients are ultimately responsible for the actions of their Clients over AttainResponse network, and will be liable for illegal material posted by their clients.

According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years or any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years.

Violations of the Child Protection Act may be reported to the U.S. Customs Agency at 1-800-BEALERT.

Copyright Infringement

AttainResponse data center infrastructure including network, leased hardware, co-location services, and other hardware located in the facility may only be used for lawful purposes.

Transmission, distribution, or storage of any information, data or material in violation of United States 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.

Creating, utilizing, or distributing unauthorized copies of software are a violation of federal and state law. If you copy, distribute or install the software in ways that the license does not allow, you are violating federal copyright law. AttainResponse will cooperate with all law enforcement agencies in relation to alleged copyright infringement housed in our data centers.

IP Allocation

AttainResponse administers an Internet network on which multiple Client servers reside. Clients shall NOT use IP addresses that were not assigned to them. Any server utilizing IP addresses outside of the assigned range will be suspended from network access until such time as the IP addresses overlap can be corrected. Use of an unauthorized IP address will result in a charge of \$25 per IP.

IRC Policy

IRC Servers are not allowed.

Specific to Email Templates and Content

Use of the Email Templates

AttainResponse and KMT grant to you a nonexclusive license to use the Email Templates provided that you agree to the following:

1. Client may use the Email Templates for their account only. Clients may not share the Email Templates with other Clients or persons.

2. Client may only use the templates they have subscribed to. Once Client subscription has ended Client must discontinue use of templates and remove any templates that have been added to their My Templates Category and their My Favorites folder.
3. The Client may not install the Email Templates on their or any other computer or network, the Email Templates must remain on the AttainResponse servers at all times.
4. Unless stated otherwise in the Documentation, you may display, modify, reproduce and distribute any of the Content included with the Email Templates. However, you may not distribute the Content on a stand-alone basis, i.e., in circumstances in which the Content constitutes the primary value of the product being distributed. Content may not be used in the production of libelous, defamatory, fraudulent, infringing, lewd, obscene or pornographic material or in any otherwise illegal manner. You may not register or claim any trademark rights in the Content or derivative works thereof.