LUXSCI ACCEPTABLE USE POLICY

Version 2021.10.28

1. OVERVIEW

This Acceptable Use Policy ("AUP") describes certain requirements and prohibited uses of the Services offered by LuxSci to Customer (also referred to herein as "you" or "your"). This AUP is automatically incorporated by reference into the Master Services Agreement ("MSA") between you and LuxSci. Capitalized terms used herein but not defined shall have the meanings set forth in the MSA.

LuxSci reserves the right to modify the AUP at any time by posting a modified AUP online at https://luxsci.com/aup, as indicated by the document last modified date at the beginning of the AUP. By registering for and using the Services, and thereby accepting the terms and conditions of the MSA, Customer agrees to abide by the AUP, as modified from time to time. No SLA credits or refunds will be issued in connection with the Service Level Agreement between you and LuxSci for any interruption in Services resulting from, in whole or in part, AUP violations.

VIOLATION OF THE AUP IS STRICTLY PROHIBITED AND MAY RESULT IN THE IMMEDIATE TERMINATION OR SUSPENSION OF YOUR ACCOUNT AND THE SERVICES YOU RECEIVE FROM LUXSCI OR SUCH OTHER ACTION AS LUXSCI DEEMS APPROPRIATE IN ITS REASONABLE DISCRETION. YOU SHALL REMAIN SOLELY LIABLE AND RESPONSIBLE FOR YOUR USE OF THE SERVICES AND ANY AND ALL CONTENT THAT YOU DISPLAY, UPLOAD, STORE ON, DOWNLOAD, OR TRANSMIT THROUGH THE SERVICES. "CONTENT" INCLUDES, WITHOUT LIMITATION, YOUR E-MAIL, WEB PAGES, FILES, TEXTS, MESSAGES, DATA, FORM DATA, AND DOMAIN NAMES. IT IS LUXSCI'S POLICY TO TERMINATE REPEAT INFRINGERS. LUXSCI RESERVES THE RIGHT TO REFUSE SERVICE TO ANYONE AT ANY TIME.

2. INTERNET ETIQUETTE

Customer is expected to be familiar with and to practice good Internet etiquette (netiquette). Customer will comply with the rules appropriate for any network to which LuxSci may provide access. Customer should not publicly post, transmit, or permit internet access to information that Customer desires to keep confidential. Customer is not permitted to post any material that is illegal, libelous, tortuous, indecently depicts children, or is likely to result in retaliation against LuxSci by offended users.

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, motor vehicles, or other modes of human mass transportation, or nuclear or chemical facilities).

4. CUSTOMER SECURITY RESPONSIBILITIES

If Customer's server or account is involved in a suspected or actual security breach or in an attack on another server or system (collectively, "security event"), it may be shut down or your Services may be disabled, and an immediate investigation may be launched by LuxSci to determine the cause/source of the security event. Customer is solely responsible for any breaches of security or security event affecting Services or servers under Customer control where said breaches are the result of, in whole or in part, Customer actions or inaction, Customer's users, security issues with Customer web site(s), or the actions or inaction of anyone who is using Customer logins, databases, web sites or other credentials in connection with the security event. In these cases, Customer is responsible for the cost to rectify any damage done to Customer's server, account, and any other systems affected by the security event. THE LABOR USED TO RECTIFY ANY SUCH DAMAGE IS CATEGORIZED AS EMERGENCY SECURITY BREACH RECOVERY AND IS CURRENTLY CHARGED AT $750 USD PER HOUR. Enquiries regarding security events should be directed to our support team at support@luxsci.com.

4.1 SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited and may result in criminal and civil liability. LuxSci may investigate incidents involving such violations and may involve and require your full cooperation with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

1. unauthorized 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 authorization of the owner of the system or network;**
2. unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network;
3. interference with service to any user, host, or network including, without limitation, mail bombing, scanning, flooding, deliberate attempts to overload a system, and broadcast attacks; and
4. forging of any TCP/IP packet header or any part of the header information in an email, message, or online posting.

Violators of the System and Network Security policy are responsible, without limitation, for the cost of labor 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 LuxSci. SUCH LABOR IS CATEGORIZED AS EMERGENCY SECURITY BREACH RECOVERY AND IS CHARGED AT THE HOURLY RATE REFERENCED IN SECTION 4 OF THIS AUP. LuxSci 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, LuxSci urges its customers to assume that all online communications are insecure, unless specific services are used to secure it.

4.2 PASSWORD PROTECTION

Customer is responsible for protecting Customer users' passwords and for any authorized or unauthorized use made of these passwords. Customer will not use or permit anyone to use LuxSci's Services to guess passwords or to access other systems or networks without authorization. Customer will fully cooperate with law enforcement authorities in the detection and prosecution of illegal activity related to account and password security.

Customer shall be solely responsible for maintaining the security of its accounts and passwords, and for preventing their unauthorized use. If the account holder shall become aware, or suspect, that any unauthorized person has obtained access through their account, then the account holder shall immediately notify LuxSci, change their password(s), and take any other recommended reasonable steps to enhance their account's security.

4.3 WEB HOSTING SECURITY

As a web hosting client, Customer is fully responsible for any and all security vulnerabilities in your web site(s). If any web site vulnerabilities are compromised, you will be fully responsible as if you had explicitly performed the compromise and associated resulting actions. This responsibility extends to the requirement that Customer update any third-party software installed in its web site(s) in a timely manner (e.g., updates to WordPress or its plugins) based on industry standard patch management programs designed to keep web applications secure.

4.4 NETWORK SECURITY

Customer has a responsibility to use the LuxSci network responsibly. This includes

respecting the other customers of LuxSci. LuxSci reserves the right to suspend and or cancel Customer's Services if Customer uses the LuxSci network in such a way that adversely affects other LuxSci customers. This includes, but is not limited to:

1. attacking or attempting to gain unauthorized access to servers and/or services that belong to LuxSci or its customers (i.e. computer hacking and unauthorized penetration testing);
2. participating in behavior that results in reprisals that adversely affect the LuxSci network or other customers' access to the LuxSci network; and
3. using LuxSci services in such a way that the network or these services are overloaded, and service is degraded or denied to other customers.

LuxSci prohibits any use or attempted use of an internet account or computer without the owner's authorization. Such attempts include, but are not limited to, "Internet Phishing" (tricking other people into releasing their passwords), password robbery, security hole scanning, port scanning, etc. Any unauthorized use of accounts or computers by Customer, whether or not the attacked account or computer belongs to LuxSci, 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 another customer of LuxSci is strictly prohibited.

Violations of this Network Security policy may be reported directly to the FBI's Infrastructure Protection & Computer Intrusion Squad. Customer will cooperate fully with any civil and/or criminal litigation arising from the violation of this Network Security policy.

5. EMAIL

5.1 BULK EMAIL

For bulk or commercial email sent by or on behalf of Customer using LuxSci Services or from any network that directly or indirectly refers recipients to a site hosted using LuxSci Services (including using third-party distribution lists), Customer shall:

1. post a privacy policy for each associated domain;
2. 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;

3. 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 LuxSci request; and

4. include the recipient's email address in the e-mail body or "TO" line.

5.2 SPAM AND COMMERCIAL ADVERTISEMENTS WITH EMAIL

LuxSci takes a zero-tolerance approach to the sending of Unsolicited Commercial E-mail ("UCE") or spam over its network. Very simply, this means that Customer may not use or permit others to use LuxSci's network to transact in UCE. Customer may not host, or permit hosting of, sites or information that is advertised by UCE from other networks. Violations of this spam policy carry severe penalties, including termination of service.

Sending an unsolicited message, especially an advertisement, to multiple recipients, is by itself spamming unless the individuals have specifically requested to be added to a mailing list on that topic or have an existing business or personal relationship with the sender. This includes both commercial advertisements and informational messages sent to recipients via email as well as off-topic messages where the recipient has not requested or invited the message.

As our customers are ultimately responsible for the actions of their users over the LuxSci network, it is advisable that Customer develops a similar policy for its users at least as restrictive as this policy.

Upon notification of an alleged violation of the spam policy, LuxSci may initiate an immediate investigation. During the investigation, LuxSci may restrict Customer access to the network to prevent further violations. If Customer is found to be in violation of the spam policy, LuxSci may, in its sole discretion, restrict, suspend or terminate Customer's account and block IP addresses or email addresses LuxSci believes to be the source of the spam. Further, LuxSci reserves the right to pursue civil remedies for any costs associated with the investigation of a substantiated policy violation. LuxSci may notify law enforcement officials if the violation is believed to be a criminal offense.

Violation of LuxSci's spam policy should be reported to abuse@luxsci.com.

5.3 EMAIL ADDRESS SELECTION POLICY

LuxSci reserves the right to require you to change email addresses in the event that they are deemed inappropriate. Possible inappropriateness includes, but is not limited to, names that are: racially offensive, sexually offensive, detrimental to LuxSci and/or its affiliates/partners/customers, or potentially a security issue.

This policy exists to ensure the highest possible degree of service to our customers. In a time when entire IP address ranges are blocked for little or no reason at all, we must aim to avoid any potential disruptions in mail service and to ensure that a positive image is always portrayed. We must also ensure that our Services are not used for phishing or the possible impersonation of other people or companies.

6. SMS AND SECURETEXT

LuxSci provides an SMS (aka texting) facility and SecureText uses this facility. Customer is prohibited from using SecureText or LuxSci's SMS facility to:

1. launch or facilitate, whether intentionally or unintentionally, a denial of service attack on any of the LuxSci's Services or any other conduct that adversely impacts the availability, reliability or stability of the LuxSci Services;

2. transmit any material that contains viruses, trojan horses, worms or any other malicious, harmful, or deleterious content. This includes sending content or automated traffic, generated by bots or otherwise, that harms networks, Services or other infrastructure of LuxSci or any third party;

3. use the LuxSci Services in any manner that violates any applicable industry standards, third-party policies or requirements that LuxSci may communicate to its users, including without limitation, all of the applicable guidelines published by the CTIA (Cellular Telephone Industries Association), the Mobile Marketing Association, or any other accepted industry associations, carrier guidelines or other industry standards;

4. engage in any unsolicited advertising, marketing or other activities, including, without limitation, any activities that violate anti-spam laws and regulations including, but not limited to, the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act;

5. use the LuxSci Services in connection with any unsolicited or harassing messages (commercial or otherwise) including but not limited to unsolicited or unwanted SMS or text messages;

6. use LuxSci Services to harvest or otherwise collecting information about others, including email addresses or phone numbers;

7. use LuxSci Services to engage in fraudulent activity with respect to third parties;

8. violate or facilitate the violation of any local or foreign law, including laws regarding the transmission of data or software;

9. take any action to encourage or promote any activity prohibited under this AUP;

10. transmit any material that infringes the intellectual property rights or other rights of third parties;

11. transmit any material that is libelous, defamatory, discriminatory or otherwise malicious or harmful to any person or entity;

12. create a false identity or forged email address or header, or phone number, or otherwise attempt to mislead others as to the identity of the sender or the origin of a message; and

13. send bulk messages using the default provided number or a custom long code (10-digit phone number). Bulk messaging is sending 30+ identical or similar SMS messages or 30+ SecureText messages in the space of 3 minutes or at a rate of more than 1 message/second. Customers needing to send such bulk campaigns are required to purchase a "short code" phone number.

Violation of LuxSci's SMS and SecureText policies should be reported to abuse@luxsci.com and can be grounds for immediate suspension of SMS access account-wide during an investigation of the situation. If Customer is found to be in violation of the SMS and SecureText policy, LuxSci may, at its sole discretion, restrict, suspend or terminate customer's account. Further, LuxSci reserves the right to pursue civil remedies for any costs associated with the investigation of a substantiated policy violation. LuxSci may notify law enforcement officials if the violation is believed to be a criminal offense.

7. LAWFUL PURPOSE

Services and the LuxSci network may be used for lawful purposes only. Transmission, distribution, storage, or presentation of any information, data or material in violation of any applicable law or this AUP is prohibited. This includes but is not limited to: misuse of copyrighted material or material protected by copyright, trademark, trade secret or other intellectual property right or dissemination of harmful or fraudulent content.

Using any LuxSci Services for the purpose of participating in any activity dealing with subject matters that are prohibited under applicable law is a violation of this AUP.

Any conduct that constitutes harassment, fraud, stalking, abuse, or a violation of federal export restriction in connection with use of LuxSci Services is prohibited. Using the LuxSci 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 LuxSci's network may be open to the public. Customer is solely responsible for your usage of the LuxSci network and servers and any public statement Customer makes on servers hosted within the LuxSci network may be deemed "publication" of the information entered. Acknowledging the foregoing, you specifically agree not to use our Services in any manner that is illegal or libelous.

If you suspect that any person is engaging in any illegal or fraudulent activity in connection with the Services, please report it to LuxSci at abuse@luxsci.com.

Please note that LuxSci is limited in its ability to review fraudulent activity that may occur outside of the Services or to assess the legality of certain activities and may require that persons work with law enforcement to validate the fraudulent nature or the illegality of the activity before LuxSci is able to take action related to a reported violation.

7.1 PORNOGRAPHY

Customer shall cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 ("Child Protection Act") concerning child pornography. Customer is ultimately responsible for the actions of your users over the LuxSci network and will be liable for illegal material posted by your users.

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 should be reported to the U.S. Customs Agency at 1-800-BEALERT.

LuxSci explicitly prohibits use or display of material containing pornographic material of any kind. The use of LuxSci Services for the storage of such materials is also prohibited, even if such materials are not apparently publicly available.

7.2 COPYRIGHT INFRINGEMENT: SOFTWARE PIRACY POLICY

Making unauthorized copies of software is illegal, no matter how many copies you are making. If you copy, distribute or install software in ways that the applicable license does not allow, you are violating federal copyright law. If caught with pirated software, you or your company may be liable under both civil and criminal law, and you may be fined up to $250,000 and/or receive up to 5 years in jail.

8. DEDICATED HOSTING

In addition to the other AUP terms, it is not permitted on Dedicated Servers of any kind to:
1. run internet relay chat ("IRC") bots, servers, clients, programs, or anything related to IRC.
2. run unauthorized servers, daemons, or long-running background processes.
3. attempt to probe, scan, penetrate, or test the vulnerability of a server or network or to breach the server's security or authentication measures, whether by passive or intrusive techniques, without explicit authorization.

4. distribute programs and tools designed to aid in the sending or unsolicited bulk email.
5. use the Services in such a way that the server becomes documented on recognized spam abuse lists.
6. store or transmit/publish content via the server's network or equipment, including Web content, email, messages, blog postings, chat and any other type of posting or transmission which relies on the Internet, that:
    i. is offensive;
    ii. constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts;
    iii. is excessively violent, incites violence, threatens violence or contains harassing or bullying content or hate speech (it isn't always clear whether something is hate speech, but if the intent is to attack a protected group the content is unacceptable);
    iv. is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
    v. is defamatory or violates a person's privacy;
    vi. creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security or interferes with an investigation by law enforcement;
    vii. improperly exposes trade secrets or other confidential or proprietary information of another person;
    viii. is intended to assist others in defeating technical copyright protections;
    ix. infringes on another person's copyright, trade or service mark, patent or other property right;
    x. promotes illegal drugs, violates export control laws, relates to illegal gambling or illegal arms trafficking;
    xi. is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to LuxSci;
    xii. is otherwise malicious, fraudulent or may result in retaliation against LuxSci by offended viewers; or
    xiii. falsely implies any sponsorship or association with LuxSci.

Furthermore, you agree that if the IP numbers assigned to your account are listed on an abuse database like Spamhaus, you will be in violation of this AUP, and LuxSci or Server Provider may take reasonable action to protect its IP numbers, including suspension and/or termination of your service, regardless of whether the IP numbers were listed as a result of your actions;

In compliance with the Digital Millennium Copyright Act (the "DMCA"), please send DMCA notifications of claimed copyright infringements to Support by e-mail at support@luxsci.com.

Customer must cooperate fully with any civil and/or criminal litigation arising from the violation of this Dedicated Hosting policy.

9. SHARED WEB HOSTING

If you are a shared web hosting customer (if you use Services on LuxSci web hosting server(s) shared with other LuxSci customers), you hereby agree to refrain from using your shared hosting accounts for running servers, daemons, or background processes of any kind. Long-running foreground processes and processes that take up significant CPU or bandwidth must also to be avoided. LuxSci shared hosting accounts should be used only for setting up, configuring, and installing working web sites and web applications, and not for the development and/or testing of software programs or scripts, or the use of Internet client programs which access non-LuxSci servers.

Any use of LuxSci shared web hosting system resources that disrupts or interferes with the normal use of the system for other LuxSci customers, the integrity or performance of the Services, or which diminishes the security of the server is considered to be an abuse of system resources and is grounds for administrative intervention. Some examples of system abuse include spawning an excessive number of processes, consuming excessive amounts of memory or CPU or server bandwidth, spamming or mass emailing using internal or external mail servers, and using amounts of disk space or cumulative bandwidth well beyond Customer's purchased limits. The remedial action taken may range, at the sole discretion of LuxSci administration, from a warning to the immediate termination of Customer's Services, depending on the severity of the abuse and Customer's history of abuse.

Remote access (i.e., access from servers other than those provided by LuxSci) to databases hosted on shared LuxSci servers is for administrative use only and concurrent connections should be limited to less than 10. Databases hosted on shared servers are not to be used as back-end databases for public web sites hosted with other service providers or other situations that could result in significant numbers of concurrent remote connections or significant sustained remote access.

10. SHARED EMAIL HOSTING

If you are a shared email hosting customer (if you use Services on LuxSci email hosting server(s) shared with other LuxSci customers), you must be responsible that your account does not use excessive bandwidth for the downloading of email (POP, IMAP, or WebMail). Individual user accounts using 1 GB or more of bandwidth per hour would be considered excessive. Similarly, multiple users in an account using an aggregate amount of outbound bandwidth exceeding 2 GB/hour may also be considered excessive. If it is determined that your account is using excessive bandwidth for email services, you may, at the sole discretion of LuxSci administration, and based on the severity of the usage, be warned, charged, and/or have the Service(s) of individual users or your entire account disabled and/or terminated without notice. If you anticipate requiring large amounts of bandwidth (i.e. for email migrations), please contact us for special arrangements (i.e., migration to a Dedicated Server).

As a shared email hosting customer, you also agree not to abuse shared email hosting

Services by performing actions such as, but not limited to, making excessive numbers of simultaneous connections to our email or WebMail servers, using excessive amounts of CPU, using amounts of disk space well beyond Customer's purchased quota, spamming or mass emailing using your purchased SMTP services, or other actions that infringe on the proper functioning of the email servers or which affect the quality of service we are able to provide to other customers on the shared servers. The remedial action taken may range, at the sole discretion of LuxSci administration, from a warning to the immediate termination of Customer's Services, depending on the severity of the abuse and Customer's history of abuse.

11. HIGH VOLUME EMAIL SENDING

This High Volume Email Sending Policy applies to High Volume outbound email service accounts only. "High Volume," as used in this policy, will collectively refer to all SMTP services allowing where Customer explicitly pays for SMTP capacity. High Volume outbound email accounts with overdue balances may be prohibited from sending any outbound email until their accounts are made current.

11.1 PROHIBITED CONTENT AND INDUSTRIES

High Volume services may not be used for the sending of email:

1. offering to sell illegal goods or services;
2. that violates the CAN-SPAM Laws;
3. that is marketing or commercial email being sent to recipients without their permission;
4. that contains pornography or other sexually explicit material; and

5. for any of the following industries:
    i. Work from Home, Make Money Online, and Lead Generation opportunities
    ii. Multi-level and Affiliate marketing
    iii. Get Out of Debt and Credit Repair opportunities
    iv. Gambling products or services
    v. Adult References or Adult Novelty Items
    vi. Escort services or Dating services (excluding legitimate Dating sites)
    vii. Loans or Mortgages
    viii. Offers to buy pharmaceutical products (unless you are directly employed by a major pharmaceutical company)
    ix. Stock Market content, Day Trading Tips, and other Online Trading content
    x. List Rental services and List Brokers
    xi. Vitamin, Herbal, and Nutritional supplements (unless you are employed directly by a major company producing these products).

If Customer wishes to send this type of content, Customer should consider setting up your own mail servers, as most legitimate email marketing companies will not be able to help you.

11.2 HIGH VOLUME USAGE

LuxSci has a zero-tolerance policy with regards to the sending of spam and UCE. UCE is defined as "unsolicited mass email to persons with whom you do not have a business relationship or have not requested (opted-in) to your mailing." The High Volume email services are *only allowed* for sending permission-based email marketing newsletters, transactional email, or for low volume non-bulk email. This implies that all of your marketing recipients must have explicitly opted into the receipt of any marketing mailings that you may send, and that there is a simple way for them to opt out at any time. The opt-out mechanism must be clearly stated in every bulk mailing sent.

Opt-ins can happen, for example:
- when visitors use your web site
- when people fill out digital or physical forms
- when people purchase services with your organization

Opt-ins must clearly state what kinds of email messages the recipient will receive and how often.

High Volume users are prohibited from:
1. using purchased lists of email addresses of any kind (opt in or not);
2. harvesting email addresses from web sites or news groups;
3. automatically opting visitors or purchasers into their subscriber list. This includes "pre-checking" an opt in box on forms;
4. automatically adding subscribers on one mailing list to unrelated mailing lists;
5. sending emails to subscribers that are unrelated to the purpose to which they opted in;
6. adding people to the mailing list without their permission;
7. sending messages to people who have requested to be removed from the mailing list;
8. using old lists without checking with the subscribers that their addresses are still valid and that they still wish to be subscribed;
9. repeatedly sending to defunct/non-working/invalid recipient email addresses (you must promptly remove failing addresses to prevent your IP from being blocked);
10. sending unsolicited bulk email;
11. including in your messages any material that was not created by you, provided for your use, licensed by you, or that would violate anyone's rights. That includes text, photos, graphics, and other content;
12. employing any incorrect or misleading email addresses, names, physical addresses, email subject lines, or other information in your LuxSci profile or in any emails created or sent using LuxSci;

13. sending non-transactional, marketing, or promotional email that will be delivered to recipients as text, SMS, or MMS messages;
14. uploading or sending to purchased lists, rented lists, or third-party lists of any kind; and
15. sharing your password publicly.

High Volume Email users are allowed to send regular mailings to their distribution lists containing opted-in recipients or email information to recipients who have asked to get content on that topic.

11.3 BASIC HIGH VOLUME "FROM" EMAIL ADDRESSES

It is the policy of LuxSci that all messages sent via the Basic High Volume service (i.e., High Volume sending that does not involve email encryption and other specialized services):

1. originate from valid "From" (and Reply-To) addresses;
2. any responses sent back to these "From" addresses are received and processed by the sender;
3. are not "From" addresses associated with free or public email services. I.e. no sending bulk messages from "AOL", "Gmail", "Hotmail", "Yahoo!", or a college email address;
4. are using "From" addresses that belong to the sender; the sender must have full rights and permissions to be sending email from these addresses;
5. are using "From" addresses that are approved by LuxSci before use. LuxSci reserves the right to refuse the use of any particular "From" address for any reason; and

6. cannot be sent from a "From" address to which the sender is not authorized, even after approval by LuxSci, and is grounds for immediate termination of Services.

11.4 HIGH VOLUME SECURE SENDING "FROM" ADDRESSES

It is the policy of LuxSci that all messages sent via the High Volume Secure Sending service (also known as the "Premium High Volume" service):

1. originate from valid "From" (and Reply-To) addresses;
2. any responses sent back to these "From" addresses are received and processed by the sender;
3. are not "From" addresses associated with free or public email services. I.e. no sending bulk messages from "AOL", "Gmail", "Hotmail", "Yahoo!", or a college email address;
4. are using "From" addresses that belong to the sender; the sender must have full rights and permissions to be sending email from these addresses; and
5. cannot be sent from a "From" address to which the sender is not authorized, even after approval by LuxSci, and is grounds for immediate termination of Services.

11.5 HIGH VOLUME AUP ENFORCEMENT

LuxSci reserves the right to review and/or store copies of any or all messages sent through the High Volume Email service for the purposes of ensuring that they comply with this AUP. The content of these messages is covered by our privacy and non-disclosure policies (and our HIPAA BAA, as applicable).

LuxSci will review all requests for High Volume email services to ensure that Customer intends to abide by our AUP. LuxSci reserves the right to postpone service while this review process takes place, to reject any potential customer we deem to be a potential AUP-violation risk, and to suspend or terminate Customer at any time due to actual or suspected AUP violations.

LuxSci may add headers to all email messages sent which include instructions on how to report abuse and which allows LuxSci to identify the sender and the message sent. LuxSci also keeps a log of all messages sent, including the IP addresses of the users who sent them.

Any High Volume user suspected of sending spam or UCE will be immediately suspended from using the High Volume services.

11.6 HIGH VOLUME COMPLAINT POLICY

LuxSci handles spam and UCE complaints by:

- Examining the content of the message sent
- Reviewing the list of email addresses to which the message was sent so as to look for patterns common to harvested email address lists or other spam lists.
- Examining the complaint itself
- Obtaining records from Customer with respect to the opting in of that subscriber

We recommend that you keep logs and/or records of all opt ins (i.e. where, when, etc.) so that subscribers who have "forgotten" that they have subscribed to your mailing list can be reminded, and to back up your claims that the subscriber was emailed legitimately. The lack of proof of "opt in" in the face of complaints and messages that look like spam or possible UCE may result in account suspension.

High Volume customers are required to remove people from their mailing list:
1. who have requested to be unsubscribed;
2. when their email address is no longer valid;

3. when those people *email such a request back to the "From" or "Reply-To" address of the message*; and
4. who have complained to their ISP that the mailing is unwanted/spam and where we have received those complaints though our feed-back loops.

Any failure of Customer to remove subscribers from the mailing lists in a timely manner will result in immediate termination of Services in the face of subsequent complains from such subscribers.

12. SUSPENSION

LuxSci reserves the right to suspend access to any Customer Services if, in the judgment of the LuxSci network administrators, Customer's server or Services are the source or target of the violation of any terms of this AUP. If inappropriate activity is detected, all Customer accounts may be deactivated until an investigation is complete. Prior notification to Customer is not assured. In extreme cases, law enforcement will be contacting regarding the activity. Customer will not be credited for the time Customer's Services were suspended.

13. CANCELLATION

LuxSci reserves the right to cancel your Services at any time if inappropriate activity is detected. All Customer accounts may be deactivated until an investigation is complete. Prior notification to Customer is not assured. In extreme cases, law enforcement will be contacting regarding the activity. All fees paid in advance of cancellation will be refunded on a prorated basis at the sole discretion of LuxSci, if LuxSci institutes its right of cancellation. Any violation of AUP policies that results in extra costs to LuxSci may be billed to Customer (i.e., bandwidth).

14. DISCLAIMER OF RESPONSIBILITY TO MONITOR

LUXSCI IS UNDER NO DUTY TO MONITOR CUSTOMER'S OR ANY USER'S ACTIVITIES TO DETERMINE IF AN AUP VIOLATION HAS OCCURRED, NOR DO WE ASSUME ANY RESPONSIBILITY THROUGH OUR AUP TO MONITOR OR POLICE INTERNET-RELATED ACTIVITIES. LUXSCI DISCLAIMS ANY RESPONSIBILITY FOR ANY SUCH INAPPROPRIATE USES AND DISCLAIMS ANY LIABILITY TO CUSTOMER OR ANY THIRD PARTY IN RELATION TO YOUR VIOLATION OF THIS AUP. INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUP AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON YOUR BEHALF SHALL BE CONSIDERED VIOLATIONS OF THIS AUP BY YOU.