

SURA RESIDENCE FACILITY COMPUTER AND NETWORK USE

1. Use of Facility computers is for legitimate business purposes. Personal use of Facility computers is permitted as long as it is not unreasonable or excessive, is appropriate, does not interfere with business needs or operations, and does not compromise the security integrity of SURA's systems. SURA has full and final discretionary authority to determine the appropriateness and reasonableness of the use of its systems.
2. Users of the wired and/or wireless network are responsible for adhering to the Cox Business Acceptable Use Policy (Attachment 1)
3. Use of SURA resources is permitted if such use:
 - a. Does not involve illegal activities, including violation of licenses, copyrights, trademarks, or other related contracts and agreements.
 - b. Does not involve activities that could create any liability for SURA or cause SURA to lose the services of its network provider, including any actions that may compromise SURA security in any way.
 - c. Does not involve activities for the purpose of generating personal income, such as operation of an active business, operating and advertising a commercial enterprise or professional service, etc.
 - d. Does not access offensive, threatening, harassing or intimidating materials, including materials that ridicule others on the basis of race, color, religion, gender, age, sexual orientation and gender identity, marital status, national origin, ancestry, personal appearance, family responsibility, genetic information, disability, political affiliation, status as a Vietnam-era veteran or disabled veteran, or any other protected class under applicable law.
 - e. Does not access explicit sexually oriented, obscene, or pornographic materials.
4. Electronic transmissions and records using Facility computers are SURA property and are subject to disclosure to SURA management on a need-to-know basis, as well as to law enforcement, government officials, or to other third parties in accordance with federal or state law.
5. SURA limits access to its wireless and wired networks to authorized guests only.
 - a. SURA secures its wireless network with a WPA key.
 - b. WPA keys are provided to Residence Facility guests only and may not be shared.
 - c. SURA will take appropriate action to respond to infringement notices from the internet provider.
5. No software or computer programming routine may be placed on Facility computers or through the use of SURA's resources, including:
 - a. Hacker software, password crackers or sniffers, etc.
 - b. Illegal or bootlegged software, movies or music (e.g., via "peer-to-peer" software)
 - c. Personal software such as personal holiday greeting card generators, screen savers, investment programs, etc.
 - d. Routines that may damage, detrimentally interfere with, or secretly intercept or commandeer any system, data or personal information.
 - e. Attempts to elude, alter or use any methods to bypass network security and/or filters.
6. Facility guests may use SURA resources cooperatively with other guests, including limited time on Facility computers so that others may access them.

Cox Business Acceptable Use Policy

Updated: 12/1/2020

CoxCom, LLC and its affiliates and/or distribution partners (collectively "Cox") are pleased that you have chosen Cox Business. This Acceptable Use Policy ("AUP") applies to all services provided by Cox Business, including without limitation all Internet services, and any related services provided through Wifi and broadband-based services such as Cox Business Security & Surveillance service (each a "Service" or "Services"). Use of any of the Services shall at all times be subject to the terms and conditions of this AUP. This AUP is incorporated into any applicable agreement between Cox and Customer that states the AUP applies, including without limitation any applicable Commercial Services Agreement, any retail or wholesale Master Services Agreement, and any Security Services Agreement (each an "Applicable Agreement"). The AUP may be updated by Cox from time to time and the current version will appear on the Policies page on cox.com. Revised versions of this AUP are effective immediately upon posting. Customer's continued use of the Services following an update by Cox to this AUP shall constitute acceptance by Customer of the updated AUP.

In the event of a conflict between an Applicable Agreement and this AUP, the terms of this AUP will govern. Questions regarding this AUP and complaints of violations of this AUP can be directed to abuse@cox.com.

A. General Information on Use of the Services

1. Illegal or Infringing Activity. Customer shall not use the Service in a manner that infringes upon the rights of others, interferes with or diminishes the use and enjoyment of the Service by others, or interferes with or diminishes Cox's ability to provide the Services. Additionally, Customer shall not:

- (a) Use the Services for any activity that violates, or constitutes an attempt to violate, any local, state, federal or international law, order or regulation, or to engage in tortious conduct;
- (b) Use the Services to harm or attempt to harm a minor, including, but not limited to, by posting, possessing, disseminating, or transmitting material that is unlawful, including child pornography;
- (c) Conduct, participate in, or otherwise facilitate, pyramid or other illegal soliciting schemes.
- (d) Take part in any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature.
- (e) Invade another person's privacy, stalk, harass, or otherwise violate the rights of others.
- (f) Post, transmit, or distribute content that is illegal, threatening, abusive, libelous, slanderous, defamatory, promotes violence, or is otherwise offensive or objectionable in Cox's sole discretion.
- (g) Modify any customer premise equipment (including but not limited to cable modems, Gateway, ONTs, etc.) connected to the Cox network, regardless of whether the modem is owned by Customer or leased from Cox, in order to commit theft of the Service, fraudulently use the Service or provide the Service to a third party. Cox may work with law enforcement if any such theft or fraud occurs.
- (h) Use the Services in a manner that infringes on the copyright, trademark, moral rights, patent, rights of privacy, rights of publicity or any other intellectual property right of any third party. Cox assumes no responsibility, and Customer assumes all risk regarding the determination of whether material is in the public domain, or may otherwise be used by Customer or any end-users of the Services for any purpose. In the event Cox receives a claim of infringement from a copyright owner, Cox may forward one or more such notices directly to you. Cox may suspend and, in appropriate circumstances, will terminate any Customer or end-user that Cox, in its sole discretion, determines is a repeat copyright infringer. For more information regarding Cox's policies and procedures addressing copyright infringement, please visit <https://www.cox.com/aboutus/policies/copyright.html>.
- (i) Restrict, inhibit, or otherwise interfere with the ability of any other person to use or enjoy their equipment or the Service, including, without limitation, by posting or transmitting any information or software which contains a virus, lock, key, bomb, worm, Trojan botnet, cancelbot, or other harmful feature.
- (j) Transmit such large amounts of data, information, and/or other content beyond typical/expected usage for the Cox Services, as Cox determines could disrupt or cause a performance degradation under actual or assumed network conditions, regardless of intent, purpose or knowledge, to the Service or any related network infrastructure or facilities used to deliver the Service.

Repeated violations of this policy may result in suspension or termination of Service. In the event of service termination, any broadband-dependent services, including security systems, may no longer function or transmit alarm signals.

2. Spamming/Unsolicited Email. Sending unsolicited email messages, including, without limitation, commercial advertising and informational email is prohibited. Unsolicited advertisements or solicitations sent from other networks which reference email accounts or websites hosted at Cox shall be treated as if they originated from the account referenced. Customer shall not:

- (a) use the Cox Service as an email drop for responses from unsolicited email;
- (b) falsify end-user information, including forging, altering or removing email headers;
- (c) reference Cox or any related entity (e.g. by including "Organization: Cox Business" or "Cox" in the header or by listing an IP address that belongs to Cox or any related entity) in any unsolicited email even if that email is not sent through the Cox network; or
- (d) use another site's email server to relay email without the express permission of the owners of such site.

Cox uses several spam reporting services to identify unsolicited email messages and senders. Listing by one or more of these services may result in suspension of Service to Customer. Each case will be individually investigated by Cox. Cox may condition reconnection of Services upon removal of the listing from the spam reporting service.

3. Harvesting/Spidering/Spyware. The collection of email addresses, screen names, or identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or the use of software (including "spyware") designed to facilitate this activity, or use of a list obtained from such means is not allowed. An end-user suspected or found harvesting email addresses may be blocked from sending email until Cox is satisfied that the activity has stopped.

4. Data Usage, Network Management, and Misuse/Abuse. Cox is committed to the ongoing management of its network to improve its service offerings, protect Customers, and create new Services and feature enhancements for its Customers. Unless requested by Customer, Cox does not shape or throttle Internet traffic based on the particular online content, protocols or applications a Customer uses. However, Cox, in its independent judgment, uses multiple measures to ensure the best overall user experience, including, without limitation, protecting customers from illegal and harmful Internet traffic, managing email systems, and addressing excessive data consumption.

Cox employs various means to protect Customers, children, and its network, including blocking access to child pornography (based upon lists of sites provided by a third party and an international police agency), and implementing network security measures (including identification and blocking of botnets, viruses, phishing sites, malware, and certain ports as set forth below).

Cox also limits bulk email (as set forth in our email policies), maintains email storage limits (including deletion of dormant or unchecked email), and rejects or removes "spam" or otherwise unsolicited bulk email to prevent abuse of our email platform.

Technologies, equipment, applications, and activities connected to the Internet consume data. Customer must ensure that any new or expanded uses of the Service are appropriate to Customer's Cox Business internet service tier, do not cause exceptional or abusive data consumption and related impacts to the network, and do not improperly restrict, inhibit, or degrade any other user's use of the Service or Cox's ability to deliver the Service and monitor the Service, backbone, network nodes, and/or other network services. Cox's disclosures related to its broadband Internet access services specifically ("BIAS" or "Internet Services" or "Services"), including its network practices can be found at <https://www.cox.com/aboutus/policies/internet-service-disclosures.html>.

Cox reserves the right to determine, from time to time and in its sole discretion, data usage thresholds which rise to the level of abuse or misuse of the network. Excessive or abusive data consumption can adversely impact use and enjoyment of the Cox network by certain other Cox customers. Cox may take any appropriate measures to manage its network, whether or not they are described in this AUP, including without limitation, suspension or termination of any Service, or transferring a Customer's internet connection or Service to an alternative Cox service tier or technology or speed or bandwidth.

(a) Situations in which Cox may undertake steps to address network impacts include, but are not limited to:

i) in response to extraordinary levels of usage or where data consumption is not characteristic of a typical commercial user of the Service as determined by Cox in its sole discretion;

ii) during denial of service, malware, viruses or other attacks; and/or

iii) under other exigent circumstances that may have a significant effect on our Customers' ability to use the Services or Cox's ability to provide the Services, so that Cox may provide consistent services and a positive experience to all of its customers.

(b) Common activities that may cause excessive data consumption (whether upstream or downstream) in violation of this Policy include, but are not limited to:

i) Numerous or continuous excessive transfers of extremely large files;

ii) Excessive backups, replication, etc.;

iii) Abusive activities tied to an open network provided by Customer to its end-users;

iv) Excessive streaming files, whether to the cloud or otherwise, and other high-capacity traffic.

v) Security cameras constantly streaming high definition/4K video to a cloud storage application

Although Cox has no obligation to monitor consumption levels of the Services provided and/or overall network usage, Cox and its various affiliates reserve the right to monitor bandwidth, usage, and content from time to time, (i) to operate our Services; (ii) to identify violations of this AUP; (iii) to protect the network and Cox customers; and/or (iv) for any other purpose in our sole discretion. Accordingly, Cox's network management practices will change and evolve along with the expanding scope and use of the Internet and its inherent challenges and threats.

Transmission speed of the Service may vary with the number of end-users using the Services.

In some rare cases, where individual use reaches an abusive level, Cox may take any reasonable steps, as determined in its sole discretion, to inform Customer. Where Cox is unable to reach Customer, or if the issues in question have not been resolved after consultation with Cox, Cox reserves the right to immediately to suspend or terminate the Service, move the Customer's Service to a different bandwidth speed or tier or a different technology, and/or terminate the Agreement for violations of this Acceptable Use Policy as it deems necessary to protect the network, the Service and other Cox users, with or without notice.

Neither Cox nor its affiliates, suppliers, or agents will have any liability for any such actions. These actions are not Cox's exclusive remedies, and Cox may take any other legal or technical actions it deems appropriate with or without notice. Cox reserves the right in its sole discretion to move Customer to a different service tier or a different transport technology. Any termination of Cox services arising from an unresolved violation of this AUP shall be subject to the terms of Customer's Service Agreement, to include any early termination fees.

5. Customer Responsibility for End-Users. All references to "Customer" in this AUP shall apply to any end-user of the Service(s). If Customer allows others to use the Services, Customer is responsible for ensuring that all such end-users comply with this AUP. Customer is responsible for ensuring that all accounts, sub-accounts, and alternative account names associated with Customer's principal account comply with this AUP. Customer shall adopt and reasonably implement a policy that provides for the termination of end-users' account in appropriate circumstances, including end-users who are repeat copyright infringers. In the event of a suspected violation of this AUP, Customer will cooperate with Cox and will promptly provide Cox with information about Customer's end-users upon request from Cox. Cox may suspend or terminate Services to Customer (including Customer's end-users) if Cox determines or receives a complaint that an end-user has violated or is violating this AUP.

6. Resale and Redistribution of Services.

(a) The Services are provided to an individual person or company pursuant to the Applicable Agreement and such use is subject to the Applicable Agreement and this AUP. It is a violation of this AUP to provide Services to any third parties not named, described or authorized in the Applicable Agreement without prior written permission from Cox. This includes, but is not limited to, the sharing of bandwidth or services through wireless access points or wired links. Notwithstanding the foregoing, educational institutions, hotels, and military barracks may resell, provide or redistribute Cox Business Internet Service to its residents, students or guests located on their property or other approved property subject to the terms and conditions set forth in this Section 6. If permitted by the Applicable Agreement between Cox and a sales agent or service broker, such sales agent or service broker may be authorized by Cox to resell the Services to end-users approved by Cox; however, such Services may not be resold by anyone other than the sales agent or service broker authorized by Cox, including any end-user of such sales agent or service broker.

(b) Approved Resale. If Customer has been authorized in writing by Cox to resell the Services, the following provisions apply, and Customer agrees that:

(i) any resale of the Services shall not relieve Customer of its payment obligations under the Applicable Agreement with Cox;

(ii) Customer shall be solely responsible for managing end-user trouble reports and providing all support to its end-users using the Services, and Customer shall not have its end-users contact Cox directly in the event that technical support is needed except as otherwise provided in the Applicable Agreement;

(iii) Customer shall be responsible for and shall indemnify and hold Cox harmless from and against any and all liabilities, judgments, claims, losses, obligations, damages, penalties, actions, or other proceedings, suits, costs, fees, expenses and disbursements (including reasonable attorney's fees) arising out of, relating to or resulting from any violations of this AUP by Customer or its end-user(s) in connection with the use of the Services,

(iv) Customer shall not make any guarantees to its end-users regarding availability or speed of the Services;

(v) Customer shall not use any Cox trademarks or logos and shall not market or sell the Services using any Cox trademarks or logos;

(vi) Customer is responsible for ensuring that all end-users of the Services agree to the terms and conditions of this AUP, as may be amended from time to time;

(vii) if Customer becomes aware of a violation of the AUP by any of its end-users, Customer shall suspend the Services to such end-user and shall notify Cox in writing as soon as reasonably practicable;

(viii) Cox reserves the right to terminate or suspend the Services to Customer's end-user(s) if, in Cox's sole discretion, the AUP has been or is being violated by Customer's end-user(s); and

(ix) If Customer provides the Services to more than one (1) end-user and if Cox reasonably determines that Customer or any end-user of Customer is violating this AUP or any existing law or regulation in a manner that poses an immediate and substantial threat of harm to Cox's network or its ability to provide Services to Customer, its other end-users or other customers, Cox reserves the right to immediately suspend or terminate the Services to Customer, and if Cox does not have the ability to determine which end-user is responsible for the violation, to all of Customer's end-users. Customer understands that Cox may not have the ability to pinpoint the source of an AUP violation if end-users other than Customer are using the Services. Cox shall use commercially reasonable efforts to notify Customer and the offending end-user(s), if possible, of such suspension or termination and the reasons therefor as soon as reasonably practicable. If Customer sells or resells advertising or web space to a third-party Customer will be responsible for the contents of that advertising and the actions of that third party. Cox has the absolute right to reject any advertising or other third-party content that is illegal, offensive or otherwise in breach of this AUP. Cox may suspend or terminate the Services if Customer refuses to remove any advertising or other third-party content it deems objectionable.

7. Security. Customer is solely responsible for the protection of their computer equipment. Customer is responsible for any misuse of the Services, even if the inappropriate activity was committed by an employee, consultant, guest or other individuals who have access to Customer's system or network. Therefore, Customer must take steps to ensure that others do not gain unauthorized access to the Services. The Services may not be used to breach the security of other end-users or to attempt to gain access to any other person's or entity's computer, server, software or data, without the knowledge and consent of such person or entity, including attempts to circumvent the end-user authentication, or probing the security of other networks. Customer may utilize scanners, sniffers and any other such security analysis tools to maintain Customer's own network as long as Customer only uses such tools with respect to Customer's own network. Customer shall not scan, probe, or use security analysis tools against the Cox network or the networks of our other customers. Use of or distribution of tools designed for compromising security of non-Customer networks, such as password guessing programs, cracking tools, packet sniffers or network probing tools, is prohibited. Customer shall not willfully or knowingly disrupt the Services or interfere with computer networking or telecommunications services to any end-user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, and attempts to "crash" a host. The transmission or dissemination of any information or software which contains a virus or other harmful feature, and the improper or unauthorized seizing of operator privileges, are prohibited. Customer is solely responsible for the security of any device Customer chooses to connect to the Services, including any data stored on that device. If Cox detects that Customer's equipment or Customer's Internet transmissions contain viruses, trojans, worms or similar malicious content that adversely affects the Cox network or otherwise compromises the integrity or the operation of the Cox network, Cox may disconnect or suspend Customer from the Services immediately. In such event, Cox will make reasonable efforts to promptly contact Customer regarding the interruption of the Services. It is Customer's sole responsibility to ensure that any device they connect to the Cox network remains secure and virus free. Login credentials such as, but not limited to, passwords and personal identification numbers to any Cox managed or owned sites and servers must follow the Cox password requirements. Accounts that do not follow this guideline may be suspended until Customer complies and is secured. Cox will not make changes to Customer accounts without proper authorization. In the event of any partnership dissolution, corporate reorganization, or other legal proceeding involving Customer and the Services, Cox may put the account on hold and suspend the Services until the situation has been resolved to Cox's reasonable satisfaction. Customer is responsible for maintaining the confidentiality of his/her password. In the event of a breach of security through Customer's account, Customer will be liable for any unauthorized use of the Cox services, including any resulting damages.

8. Customer Information Disclosure. Cox and its distribution affiliates and vendors may cooperate with law enforcement authorities in the investigation of suspected criminal violations to the extent permitted by law. Cooperation may include Cox or its vendors providing the name, IP address(es), or other identifying information regarding Customer or its end-users. Cox will not release any personally identifiable information regarding Customer (except publicly available information) or Customer's end-users to law enforcement or government agency except upon presentation of:

(a) a subpoena issued by a government entity in a civil or criminal investigation or litigation;

(b) a civil investigative demand issued by a government entity; or

(c) a court order or other similar legal mandate. Cox may release such information based upon its sole reasonable judgment as to the validity of any such order. If Cox is ordered by a court of competent jurisdiction to monitor Customer's connection to comply with a court order or legal process, Cox will treat that information as confidential and only divulge the necessary information as required by such order or legal process.

9. Inappropriate Content and Unacceptable Links. Cox is not responsible for any information accessed by Customer through use of the Services. If using the Services to reproduce, publish, display, transmit and distribute content, Customer warrants that the content complies with this AUP and Cox and its distribution affiliates are authorized to reproduce, publish, display, transmit and distribute such content as necessary for Cox to deliver the content in a timely manner.

10. Newsgroups. Messages posted to newsgroups must comply with the written charters or FAQs for those newsgroups. Customer is responsible for determining the policies of a given newsgroup before posting to it. Posting or cross posting the same or substantially similar messages to more than eight newsgroups is prohibited. Repeated complaints about Customer not meeting the charter of a newsgroup or posting off-topic may result in termination of Cox Business Services. Customer shall not post to any Usenet or other newsgroup, forum, or list articles which are illegal or inappropriate in the local forum.

11. Internet Relay Chat. Cox Business Services may be used to participate in "chat" discussions; however, the Services may not be used to perform chat "flooding". Any single computer or other device connected through the Services may not maintain more than two simultaneous chat connections. This includes the use of automated programs, such as "bots" or "clones". Automated programs may not be used when the end-user is not physically present at the device. The Services may not be used to access any chat server in violation of the acceptable use policy of that server.

12. Misuse of System Resources. Customer shall not use scripts or programs which consume excessive CPU time or storage space to permit the use of email services, email forwarding capabilities, POP accounts, or auto responders other than for the Customer's account; or to resell access to scripts installed on Cox servers. Cox shall determine in its sole discretion whether Customer is misusing system resources.

13. Web Hosting. If Customer operates a website through Cox, the terms of this AUP will apply. In addition, if the website is hosted on a third-party web hosting service through agreement with Cox, the third party may also have additional requirements. If Cox receives a complaint about a Customer's website, Cox will make reasonable efforts to notify Customer about the complaint. Cox is not liable if a third-party web hosting service takes down Customer's website.

14. IP Addresses. Cox's IP address policy is based on RFC 2050 and the American Registry for Internet Numbers (ARIN) guidelines for Internet Service Providers. However, Cox may allocate IP addresses in any manner which it determines, in its sole discretion, is reasonable for the operation of the Services. When Cox assigns an IP address to Customer, ownership of the IP address does not transfer to Customer or any end-user; ownership of all IP addresses assigned by Cox remains with Cox at all times. IP address assignment may be changed by Cox at any time in order to enhance network efficiency, however, notice will be provided to Customer. Unused IP addresses may be reclaimed by Cox upon notice to Customer. IP addresses are relinquished by Customer upon the expiration, termination or cancellation of the Services. Cox may require an ARIN organizational ID from Customer to complete IP requests. If requested, the organizational ID must be provided. Customer may call ARIN at 703-227-0660 to obtain an ID. Please contact Cox for any questions regarding IP address rules and policies.

15. Domain Name Registrations. If Customer requests, Cox will register an available domain name on behalf of Customer, and such registration and use shall be subject to the terms and conditions required by the domain name registrar, which may be amended from time to time and are presently posted at <http://help.register.com/>.

16. Use of Residential Cox Internet Services. Cox customers using cox.net email addresses in conjunction with their Cox Business Services must also abide by the Cox Internet residential service Acceptable Use Policy ("Cox Residential AUP"). Please review the Cox Residential AUP for compliance located at <https://www.cox.com/aboutus/policies/acceptable-use-policy.html>.

17. Termination. Upon termination of Customer's Services, Cox is authorized to delete any files, programs, data and email messages associated with such account.

B. Features and Limitations of CoxMail® Email Service

1. When utilizing Cox email servers, end-users are restricted to 300 recipients per message. This includes recipients in the 'CC', 'BCC' and 'TO' fields. Each source IP may send a maximum of 900 messages per hour.

2. Forwarding/Filtering of Incoming Email. Cox is not responsible for the forwarding or storage of email sent by Customer or end-user where the account has been suspended or terminated. Cox has the right to block electronic communications from other entities on the Internet where necessary to protect the Cox network and Cox customers. Cox has the right to disable immediately any account in order to forestall further abuse or damage to email systems.

3. Email Virus Detection. Cox email servers employ virus detection and prevention methods. If a virus or malware is discovered in an email, the virus or malware will be cleaned or deleted. No report will be sent to Customer because most infected email contains a 'fake' reply address. Cox Customer Safety Department may contact Customer upon receiving a complaint.

4. Trash Folder retention. Messages that remain in the Trash folder on the CoxMail® server for 30 days or more after receipt will be deleted without notice. Customer may retain an email message indefinitely by moving it to an alternative folder.

5. Administration of Third-Party Email Server (Non-Cox Email Server). Cox prohibits the relaying of Customer email from Customer's or third party owned/administered email servers through Cox email servers. Customers who maintain their own email server or have an email server through a third party shall not use any Cox outbound email servers to deliver their email to the recipients.

6. CoxMail® Dormant Mailbox Retention

(a) Dormant Mailbox Locked: When a non-administrative Mailbox* is not checked for new email for at least 120 days, it is considered dormant and will be locked ("Dormant Mailbox"). New messages sent to a Dormant Mailbox will be returned as undeliverable. Dormant Mailboxes can be reactivated by accessing Customer's CoxMail® Mailbox via webmail (coxmail.com), POP-3 client (ex. Outlook), or by setting up an automatic forward to an active email account. (*A non-administrative mailbox is a mailbox that does not have administrative rights. Administrative mailboxes, which allow an end-user to manage and provision mailboxes, are not locked for non-use). For more information on CoxMail® administrative Mailboxes go to <http://control.coxmail.com>.

(b) Dormant Mailbox Deleted: When a Dormant Mailbox is not checked for new email for an additional 60 days after it is locked, the Mailbox and any messages in the Mailbox at that time are deleted. PLEASE NOTE: Deleted email cannot be recovered. New messages sent to a deleted Dormant Mailbox will be returned as undeliverable. If Customer's mailbox is deleted, Customer will lose any personalization (all folders, address book entries, and preferences). If this occurs and Customer wishes to set up a new mailbox, Customer must contact its local Cox customer support representative.

C. Mass Mailing

1. Definition of Mass Mailing. Mass Mailing is defined as emailing to more than 150 recipients per message by either Cox customers or through their 3rd party email agents. Before Customer or its end-users engage in Mass Mailing, Customer must obtain written approval from Cox. Customer must complete the [Mass Mailing request](http://massmailing.coxmail.com) form located at <http://massmailing.coxmail.com>, and, if approval is granted by Cox, Customer must comply with all instructions and requirements outlined by Cox before Customer may engage in Mass Mailing. Cox may request to review the content of Customer's bulk mailings prior to approval. Please allow up to 72 hours for a response. Mass Mailing is not included as part of any Cox service offering and Customer has no contractual right to engage in Mass Mailing until and unless Customer receives written approval from Cox. Cox may approve, deny, or condition permission in its sole discretion. Cox may rescind previously granted permission in its sole discretion if Customer violates any Mass Mailing policy. Formal approval must be received before Mass Mailing can commence; lack of response to a Mass Mailing request is deemed a denial of Mass Mailing authorization.

2. Customers may only send email to recipients who have intentionally requested to receive information via electronic distribution from the originating domain name or business referenced within the content of the email. Without exception, Cox prohibits the practice of mass mailing unwanted email solicitations of any type ("Spam"), regardless of content, and will take action to prevent this practice. Email distribution lists that are purchased or freely received from a third-party and/or are represented to Customer as "opt in" clean lists are not exempt from this AUP.

3. Mass Mailing Requirements for Approved Mass Mailing Customers

(a) Recipient Limits and Send Rate: When approved for mass mailing and utilizing Cox email servers, end-users are restricted to 300 recipients per message and 100,000 recipients per hour. Cox email servers also limit each source IP address to approximately 900 messages per hour. If Customer uses a third-party mail server or Customer's own mail server to send mass mailings, these restrictions do not apply.

(b) All email distributions must have a functional and clear option or instructions for unsubscribing or "opting-out" of the subscriber list.

(c) For all email distributions, the subject of the email must match or relate to the body of the text.

(d) The email must contain a valid physical postal address.

(e) "From", "Reply-To", "Return-Path" and "Error-To" headers must be valid and each email address must accept any bounces at the rate they may occur.

Messages that do not follow these requirements will be rejected by the server.

Cox reserves the right to reject any request to perform a mass emailing for any reason. Cox reserves the right to cease processing a sender's email if the mailing is overly burdensome on the Cox email servers. For example, this could happen due to an exceptionally large attachment or an attempt to flood the server, but should not occur with normal sending usage.

D. Complaints and AUP Violations

If Cox receives a complaint against Customer or believes there is a violation of this AUP, Cox will investigate and if appropriate, inform Customer of the complaint. Cox will work with Customer to obtain a mutually satisfactory resolution to the complaint/violation and advise as to any necessary corrective action; however, if a resolution cannot be reached in a reasonable period of time depending upon the nature of the complaint or violation, Cox may suspend or terminate the Services. Cox reserves the right to act immediately and without notice to suspend, restrict, or terminate Services in response to a court order, government mandate, or if Cox reasonably believes Customer's activity is harmful to the Cox network or its other customers. The failure of Cox to enforce this AUP for whatever reason does not constitute a waiver of any right to do so at a later time. Cox is not liable for suspension or termination of Services arising from an alleged or actual violation of this AUP.