ESSEX ACCEPTABLE INTERNET USE POLICY STATEMENT AND GUIDELINES

Policy Statement

Essex Property Trust ("ESSEX") is dedicated to sustaining the integrity and security of corporate data and intellectual property and maintaining the responsiveness of our network by limiting certain unauthorized activities. Further, Essex is committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging and preserving for all of those users (including both Essex Corporate Network Users and Essex Guest Network Users) that have agreed to the Essex Terms and Conditions of Internet Use (collectively, "Essex Network Users") the ability to use the ESSEX CORPORATE NETWORK and the Essex Guest Network without interference or harassment from other users. This Acceptable Internet Use Policy Statement and Guidelines ("AUSG") will assist in protecting ESSEX's employees and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Scope and Application of the AUSG

This AUSG applies to the ESSEX services that provide or include access to the Internet, or are provided over the Internet or wireless data networks (collectively "IP Services"). By using IP Services, Essex Network Users agree to comply with the terms of this AUSG and remain responsible for complying with this AUSG. ESSEX reserves the right to change or modify the terms of this AUSG at any time, effective when posted on ESSEX's web site at www.essex.com/AUSG. Essex Network Users' use of the IP Services shall constitute acceptance of any changed or additional terms to this AUSG.

Connection to Essex Corporate Network and Essex Guest Network

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of ESSEX. These systems are to be used for business purposes in serving the interests of ESSEX and of ESSEX's employees, vendors, contractors and subcontractors in the course of normal operations.

ESSEX CORPORATE NETWORK: The Essex Corporate Network consists of the network equipment, computers, laptops and mobile devices. Only devices owed and paid for by ESSEX are allowed to connect to the ESSEX CORPORATE NETWORK. Personally owned devices are ***NOT*** allowed to connect to the ESSEX CORPORATE NETWORK.

ESSEX GUEST NETWORK: The Essex Guest Network consists of computers, laptops and mobile devices. Personally owned devices may connect to the ESSEX GUEST NETWORK.

Prohibited Activities

General Prohibitions: ESSEX prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of ESSEX's networks or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

High-bandwidth activities (such as downloading a full length movie or downloading large quantities of music files) or use of streaming audio or video services, including but not limited to use of Spotify, itunes, Pandora, Rdio, Apple Music, iheartradio, Grooveshark, Netflix, Hulu, Amazon Prime, HBO Go and/or Apple TV, in excess of 62MB (megabytes) of data is prohibited, unless a higher usage is specifically authorized in advance by a member of the Senior Management Committee and may only be used for approved business purposes. By way of example, 62MB (megabytes) of data is approximately equal to a 1080p (higher def) five (5) minute YouTube video.

Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, applications, or other services that are accessed via a link from the IP Services is a violation of this AUSG.

Unlawful Activities: IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Violation of Intellectual Property Rights: IP Services shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of ESSEX or any individual, group or entity, including, but not limited to, any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Threatening Material or Content: IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize ESSEX provided web hosting, ESSEX reserves the right to decline to provide such services if the content is determined by ESSEX to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or is otherwise harmful to others.

Inappropriate Interaction with Minors: ESSEX complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the National Center for Missing and Exploited Children. For more information about online safety, visit www.ncmec.org.

Pornography including Child Pornography: IP Services shall not be used to publish, submit/ receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store pornography including child pornography. Suspected violations of this prohibition may be reported to ESSEX at the following Telephone Hotline Service: AlertLine 1-866-752-5307. ESSEX will report any discovered violation of this prohibition involving child pornography to the National Center for Missing and Exploited Children and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

Spam/E-mail/Usenet Abuse: Violation of the CAN-SPAM Act of 2003, or any other applicable law regulating e-mail services, constitutes a violation of this AUSG. Examples of violations of the CAN-SPAM Act of 2003 or other spam/email or usenet abuse include but are not limited to the following activities (unless approved by a member of the Senior Management Committee as a legitimate business use):

- sending multiple unsolicited electronic mail messages or "mail-bombing" to one or more recipient;
- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;

- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the ESSEX Guest Network or of the networks with which ESSEX interconnects, by virtue of quantity, size or otherwise;
- using another site's mail server to relay mail without the express permission of that site;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUSG;
- using IP addresses that the Essex Network Users does not have a right to use;
- collecting the responses from unsolicited electronic messages;
- maintaining your own website;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services or the Internet (e.g., through language, frequency, size or otherwise);
- using distribution lists containing addresses that include those who have opted out;
- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;
- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUSG or the AUSG of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Security Violations

Essex Network Users are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates.

IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of ESSEX's (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing. Examples of system or network security violations include but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;

- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software;
- with respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow Essex Network User's account to stay logged on while Essex Network User is not actively using the IP Services or using such account for the purpose of operating a server of any type;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to ESSEX's network or systems, or to the network of any other IP Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUSG.

Essex Network Users Responsibilities

Essex Network Users remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. ESSEX has no responsibility for any material created on the ESSEX Guest Network or accessible using IP Services. Such third-party website links are provided as Internet navigation tools for informational purposes only, and do not constitute in any way an endorsement by ESSEX of the content(s) of such sites.

Essex Network Users are responsible for taking prompt corrective action(s) to remedy a violation of this AUSG and to help prevent similar future violations.

AUSG Enforcement and Notice

Essex Network Users' failure to observe the guidelines set forth in this AUSG may result in ESSEX taking actions anywhere from a warning to a suspension or termination of Essex Network Users IP Services. When feasible, ESSEX may provide Essex Network Users with a notice of an AUSG violation via e-mail or otherwise allowing the Essex Network Users to promptly correct such violation.

Any employee found to have violated this AUSG, particularly those who either (1) knowingly commit serious violations of the guidelines provided for in this AUSG such as illegal activities or security violations, or (2) repeatedly violate any of the guidelines provided in this AUSG especially after warning, may be subject to disciplinary action, up to and including termination of employment.

ESSEX reserves the right, however, to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped or when ESSEX reasonably determines that the conduct may: (1) expose ESSEX to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of ESSEX's network or networks with which ESSEX is interconnected, (3) interfere with another Essex Network Users' use of IP Services or the Internet, (4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to ESSEX or Essex Network Users.

ESSEX has no obligation to monitor content of any materials distributed or accessed using the IP Services. However, ESSEX may monitor content of any such materials as necessary to comply with applicable laws, regulations or other governmental or judicial requests; or to protect the ESSEX network and its Essex Network Users.

Incident Reporting

Any complaints (other than claims of copyright or trademark infringement) regarding violation of this AUSG by Essex Network Users should be directed to the Legal Department at the contact information provided for below. Where possible, include details that would assist ESSEX in investigating and resolving such complaint (e.g. expanded headers, IP address(s), a copy of the offending transmission and any log files).

Copyright complaints: If you believe that your work has been copied and posted, stored or transmitted using the IP Services in a way that constitutes copyright infringement, please submit a notification to ESSEX's Legal Department at:

Attn: Legal Department
1100 Park Place, Suite 200
San Mateo, CA 94403
Phone: (650) 655-7932
E-mail: Legal2@essex.com

Contact Information: Any notification that ESSEX sends to its Essex Network Users pursuant to this AUSG will be sent via e-mail to the e-mail address on file with ESSEX, or may be in writing to Essex Network Users' address of record. It is the Essex Network Users' responsibility to promptly notify ESSEX of any change of contact information.

Administration of AUSG

This AUSG will be administered by the Chief Technology Officer in association with the General Counsel and the legal department. Exceptions to this AUSG may be made by a member of the Senior Management Committee and may only be used for approved business purposes.

Date: December 29, 2015