ExoLisT - Acceptable Use Policy

1. Overview

The intention for publishing an Acceptable Use Policy for ExoList is not to impose restrictions that are contrary to it’s proposed openness and free use. ExoLisT is committed to protecting it's stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.

All systems and software relating to the function of ExoList, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, SSH, FTP, and SFTP, are the property of ExoList. These systems are to be used for the intended list sharing and recording purposes of the ExoLisT web application in serving the interests of the users of the application in the course of its normal operations.

Effective security is a team effort involving the participation and support of every stakeholder and affiliate who deals with the information and/or information systems of ExoList. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of the computer equipment and software resources of ExoList. These rules are in place to protect the users of the application. Inappropriate use exposes ExoList stakeholders to risks including virus attacks, compromise of network systems and services, breach of personal information, and potential legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to carry out the functions of Exolist or interact with internal networks and systems, authorized to be used/ controlled by ExoLisT, the user, or any other third party.

Anyone using the ExoLisT application is responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with ExoList policies and standards, as well as local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to all who use ExoList application resources, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by ExoLisT.

4. Policy

4.1 General Use and Ownership

. 4.1.1 ExoLisT proprietary information stored on electronic and computing devices whether owned or leased by ExoLisT, the employee or a third party, remains the sole property of ExoLisT. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

. 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of ExoLisT proprietary information or ExoLisT user information.

. 4.1.3 You may access, use or share ExoLisT proprietary information only to the extent it is authorized.

. 4.1.4 Users are responsible for exercising good judgment regarding the reasonableness of personal use.

. 4.1.5 For security and network maintenance purposes, authorized individuals within ExoLisT may monitor equipment, systems and network traffic at any time.

. 4.1.6 ExoList reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user of ExoLisT authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing ExoLisT-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.2.1 System and Network Activities
The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ExoLisT.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ExoLisT or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account other than the user’s own for any purpose is prohibited byExoLisT.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Making fraudulent offers of products, items, or services originating from any ExoLisT account.

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. Port scanning or security scanning is expressly prohibited.

9. Executing any form of network monitoring which will intercept data not intended for the user's host.

10. Circumventing user authentication or security of any host, network or account.

11. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.

13. Providing information acquired about ExoLisT users, or lists of, users to parties outside the users of ExoList.

4.3.2 Communication Activities

When using Exolist resources, users must realize they need to respect the rights of other users. Questions may be addressed to the developer of ExoList. alec.sokso@icloud.com.

1. Sending unsolicited information, including the excessive sharing of unwanted lists or other advertising material to individuals who did not specifically request such material (spam).

2. Any form of harassment via email, list sharing, whether through language, frequency, or size of messages.

3. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4. Use of unsolicited messages originating from within ExoLisT's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by ExoList or connected via ExoList's network.

5. Posting the same or similar non-application-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5. Policy Compliance

5.1 Compliance Measurement

ExoLisT will verify compliance to this policy through various methods, including but not limited to, network scans, database auditing, and feedback from specified users.

5.2 Exceptions

Any exception to the policy must be approved by the developer of ExoLisT in advance.

5.3 Non-Compliance

An user found to have violated this policy may be subject to having his to her account disabled without warning.

References:

Acceptable Use Policy. (2014, June 1). Retrieved November 1, 2014, from https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy