Acceptable Use Policy

Author: Daniel Nelms

Date: September 19, 2013

---

1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Final Frontiers Foundation in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Final Frontiers Foundation provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope

All employees, contractors, consultants, representatives, temporary and other workers at Final Frontiers Foundation, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Final Frontiers Foundation, or to devices that connect to a Final Frontiers Foundation network or reside at a Final Frontiers Foundation site.

Information Security must approve exceptions to this policy in advance through written approval by the Board President.

3 Policy Statement

3.1 General Requirements

3.1.1 You are responsible for exercising good judgment regarding appropriate use of Final Frontiers Foundation resources in accordance with Final Frontiers Foundation policies, standards, and guidelines. Final Frontiers Foundation resources may not be used for any unlawful or prohibited purpose.

3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the Final Frontiers Foundation network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

3.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of Final Frontiers Foundation at all times. Conducting Final Frontiers Foundation business that results in the storage of proprietary information on personal or non- Final Frontiers Foundation controlled environments, including devices maintained by a third party with whom Final Frontiers Foundation does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Final Frontiers Foundation, or its partners, for company business.

3.3 Computing Assets

3.3.1 You are responsible for ensuring the protection of assigned Final Frontiers Foundation assets that includes the use of computer cable locks or other security devices. Promptly report any theft of Final Frontiers Foundation assets to the Vice President of Domestic Operations.

3.3.2 All PCs, PDAs, Phones, Tablets, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

3.3.3 BYOD (Bring Your Own Device) this can include computers such as laptops, desktops, tablets, smart phones, USB drives, CD/DVD or other optical media, hard disc drives, etc, may be used for personal communication and

storage only. Company assets including intellectual property should not be stored on your own personal devices without the express written permission of the Board President. In the event of termination of employment or contact any company property including data and intellectual property must be removed immediately from any personal devices in your possession. Failure to do so may result in litigation including civil and criminal charges against you.

3.3.4 Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, logging devices, firewalls, etc.

3.4 Network Use

You are responsible for the security and appropriate use of Final Frontiers Foundation network resources under your control. Using Final Frontiers Foundation resources for the following is strictly prohibited:

3.4.1 Causing a security breach to either Final Frontiers Foundation or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.2 Causing a disruption of service to either Final Frontiers Foundation or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3 Introducing honeypots, honeynets, or similar technology on the Final Frontiers Foundation network.

3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.4.5 Use of the network for viewing, or transmitting pornographic material.

3.4.6 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

3.4.7 Use of the Internet or Final Frontiers Foundation network that violates Final Frontiers Foundation policies, or local laws.

3.4.8 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and

keyloggers.

3.4.9 Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5 Electronic Communications

The following are strictly prohibited:

3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates Final Frontiers Foundation policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, mail, or other forms of communication.

3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.5.4 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam), social networks, forums, etc.

3.5.5 Use of company assets and intellectual property for personal or unapproved business use is strictly prohibited. This includes but is not limited to, our mailing list, donor information, contact details of sponsors, financial records, company documents, video footage, photos, strategic information about the company's methods of operation, etc.

3.5.6 Use of a Final Frontiers Foundation e-mail or IP address to engage in conduct that violates Final Frontiers Foundation policies or guidelines. Posting to a public newsgroup, bulletin board, social network, or listserv with a Final Frontiers Foundation e-mail or IP address represents Final Frontiers Foundation to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Final Frontiers Foundation.

5 Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings, social networks, and postal mail. Messages that are unsolicited, unwanted, and irrelevant.

_____

Signature – Acknowledge receipt of policy and understanding of the contents

_____ _____

Printed Name Date