To Whom It May Concern,

We created a shorter version of our Acceptable Use Policy to host it on the following machines: the Firewall, the Active Directory and the Debian. The version is as follows:

**\* \* \* \* \* \* \* \* \* \* W A R N I N G \* \* \* \* \* \* \* \* \* \***

This computer system is the property of the FROG.com Domain. It is for authorized use only.  By using this system, all users acknowledge notice of, and agree to comply with, the Acceptable Use of Information Technology Resources Policy (“AUP”).  Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in FROG.com’s AUP. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

Users have no personal privacy rights in any materials they place, view, access, or transmit on this system. The University complies with state and federal law regarding certain legally protected confidential information, but makes no representation that any uses of this system will be private or confidential.

**LOG OFF IMMEDIATELY** if you do not agree to the conditions stated in this warning.

**\* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \***

On the following page is the more extensive version of it, more suitable to have the employees read and sign. That version has been taken from the SANS Institute and adapted to our needs.

Kind regards,

Team 17.

Acceptable Use Policy **Consensus Policy Resource Community**

**Acceptable Use Policy**

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

**Last Update Status:** Updated June 2014

**1. Overview**

Infosec’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Frog.com’s established culture of openness, trust and integrity. Infosec is committed to protecting Frog.com's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 Frog.com. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Frog.com employee and affiliate who deals with information and/or information systems. 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 computer equipment at Frog.com. These rules are in place to protect the employee and Frog.com. Inappropriate use exposes Frog.com to risks including virus attacks, compromise of network systems and services, and legal issues.

**3. Scope**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Frog.com business or interact with internal networks and business systems, whether owned or leased by Frog.com, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Frog.com and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Frog.com SANS Institute 2014 – All Rights Reserved Page 2

**Consensus Policy Resource Community**

policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Frog.com, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Frog.com.

**4. Policy**

**4.1 General Use and Ownership**

4.1.1 Frog.com proprietary information stored on electronic and computing devices whether owned or leased by Frog.com, the employee or a third party, remains the sole property of Frog.com. 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 Frog.com proprietary information.

4.1.3 You may access, use or share Frog.com proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Frog.com may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.

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

**4.2**

**Security and Proprietary Information**

4.2.1

All mobile and computing devices that connect to the internal network must comply with

the

*Minimum Access Policy*

. SANS Institute 2014 – All Rights Reserved Page 3

**Consensus Policy Resource Community**

The lists below are by no means exhaustive, but attempt to provide a framework for activities

which fall into

the category of unacceptable use.

4.3.1

System and Network Activities

The following activities are strictly p

rohibited, 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 pr

oducts that are

not appropriately licensed for use by Frog.com.

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 <Company

Name> or the end user does not have an active license is strictly prohibited.

3.

Accessing data, a server or an account for any purpose other than conducting <Company

Name> business,

even if you have authorized access, is prohibited. SANS Institute 2014 – All Rights Reserved Page 4

**Consensus Policy Resource Community**

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

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

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Frog.com computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Frog.com account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. 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.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

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

14. Introducing honeypots, honeynets, or similar technology on the Frog.com network.

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

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

17. Providing information about, or lists of, Frog.com employees to parties outside Frog.com.

SANS Institute 2014 – All Rights Reserved Page 5

**Consensus Policy Resource Community**

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

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

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

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

6. Use of unsolicited email originating from within Frog.com's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Frog.com or connected via Frog.com's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam). 4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Frog.com’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Frog.com’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Frog.com’s policy, is not detrimental to Frog.com’s best interests, and does not interfere with an employee's regular work duties. Blogging from Frog.com’s systems is also subject to monitoring.

2. Frog.com’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Frog.com confidential or proprietary information, trade secrets or any other material covered by Frog.com’s Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Frog.com and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing

SANS Institute 2014 – All Rights Reserved Page 6

5. Policy Compliance **Consensus Policy Resource Community**

comments when blogging or otherwise engaging in any conduct prohibited by Frog.com’s *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to Frog.com when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Frog.com. Employees assume any and all risk associated with blogging.

**5.** Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Frog.com’s trademarks, logos and any other Frog.com intellectual property may also not be used in connection with any blogging activity 5.1 Compliance Measurement

**5. Policy Compliance**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**6. Related Standards, Policies and Processes**

* • Data Classification Policy
* • Data Protection Standard
* • Social Media Policy
* • Minimum Access Policy
* • Password Policy

**7. Definitions and Terms**

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

* • Blogging

SANS Institute 2014 – All Rights Reserved Page 7

Responsible **Consensus Policy Resource Community**

* • Honeypot
* • Honeynet
* • Proprietary Information
* • Spam

|  |  |  |
| --- | --- | --- |
| **8. Revision History Date of Change** | **Responsible** | **Summary of Change** |
| June 2014 | SANS Policy Team | Updated and converted to new format |