Acceptable Use Policy Sample

(Sample written policy to assist with compliance)

1.0 Overview

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to *[agency name]* established culture of openness, trust, and integrity. *<Agency name>* is committed to protecting *[agency name]*'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, internet browsing, File Transfer Protocol, and National Crime Information Center access are the property of the *[agency name]*. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every *[agency name]* 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.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at *[agency name]*. These rules are in place to protect the employee and *[agency name]*. Inappropriate use exposes *[agency name]* to risk including virus attacks, compromises of the network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at *[agency name]* *<Agency Name>*, including all personnel affiliated with LEIN, NCIC and third parties. This policy applies to all equipment that is owned or leased by *[agency name] <Agency Name>, or any device accessing the Agency's network*.

4.0 Policy

4.1 General Use and Ownership

1. While *[agency name]* network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the *[agency name]*. Because of the need to protect *[agency name]* network, management cannot guarantee the confidentiality of information stored on any network devise belonging to *[agency name]*.
2. 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 consult their supervisor or management.
3. *<Agency name>* recommends that any information that a user considers sensitive or vulnerable (etc. residual LEIN, NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.
4. For security and network maintenance purposes, authorized individuals within *[agency name]* may monitor equipment, systems and network traffic at any time, per *[agency name]* policy.
5. *<Agency name>* reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: Criminal Justice Information (CJI), agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. *(See Password Policy)*.
3. In accordance with FBI CJIS Security Policy, all personal computers, laptops, and workstations shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with policy.
5. All devices used by employees that are connected to the *[agency name]* Internet/Intranet/Extranet, whether owned by the employee or *[agency name]*, shall be continually executing approved virus-scanning software with a current database.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. *(See Malicious Code, Spam and Spyware Protection Policy)*

4.3 Unacceptable Use
The following activities are, in general, prohibited. Under no circumstances is an employee of *[agency name]* authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing *[agency name]* owned resources. The list below is by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

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

1. Unauthorized access, copying, or dissemination of classified or sensitive information (CJI).
2. Installation of any copyrighted software for which *[agency name]* or end user does not have an active license is strictly prohibited.
3. Installation of any software, without preapproval and virus scan, is strictly prohibited.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. 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 that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to *[agency name]*.
8. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee's host.
11. 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.
12. Providing information about LEIN/NCIC or list of *[agency name]* employees to parties outside *[agency name]*.

5.0 Penalties
Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access

revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

Other Related Resources:

- Notification of Criminal Penalties Document
- Password Policy (Not Required)
- Malicious Code, Spam and Spyware Protection Policy (Not Required)