# EMPLOYEE ACCEPTABLE USE POLICY

By

FELINDA E. HOLMES

MASTERS OF INFORMATION SECURITY

LEWIS UNIVERSITY

2009

# ABSTRACT

This paper is being produced to address some key issues at Federated Legal Systems, Inc. regarding end user's behavior and access within the company's computer network. While there is an employee computer usage policy, I believe it falls short, when it comes to addressing specific issues such as security. Because of the nature of Federated Legal Systems, Inc.'s business, it probably relies more on the existence of criminal laws to deal with any possible breaches to the company's network. While these laws would certainly address some generalities, an effective employee computer usage policy would be more beneficial, considering most of the damage to a company's network is usually committed by an employee.

My objective with this project is to create an Information Security Policy for this company that will not only address security, but the behavior and attitudes of end users that often lead to disaster and damage to a company's computer network system. Goals of the project include monitoring employee computing habits, collecting information from both employees and management staff, analyzing data, and defining an Acceptable Use Policy for employees. This will be completed by collecting data and with the assistance of a general survey of a number of Federated Legal Systems, Inc. employees. The survey will be developed by first monitoring employee's behavior and actions on the network and which will include how employees handle their passwords, surf the internet, use e-mail, workstation usage, data storage and more. Other areas include the the dissemination of data to external entities and anti-virus. Through analysis, I will be able to effectively define the necessary procedures that will assist in protecting the firm's assets.

# TABLE OF CONTENTS

## LIST OF FIGURES

*Number* *Page*

# INTRODUCTION

A local non-profit volunteer agency, which we shall call "Federated Legal Systems, Inc." diligently works toward the successful representation of those individuals that are indigent and cannot afford to pay for the legal counsel, that is necessary to fairly represent them in court against criminal prosecution or civil liens.

While Federated Legal Systems, Inc.'s computer system should be used mainly for business purposes to serve the interest of the office, clients and customers in the course of normal business operations, it does currently have an unwritten policy, that allows its end users to utilize their local workstation to surf the internet, read e-mail (including personal), listen to music and more. While the goal in the past was to create a free and somewhat liberal workplace, I believe it has failed to recognize the issues that accompany this freedom. I had an opportunity to monitor employee behavior and notice that many employees take for granted the statement of "o***ccasional use, but not abuse"*** when it comes to using company equipment.

Federated Legal Systems, Inc. is serious in its commitment to protecting its employees, clients and organization from illegal or damaging actions by individuals, either knowingly or unknowingly. However, effective security is a team effort involving the participation and support of every Federated Legal Systems, Inc. employee and affiliates who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. In order to achieve some sense of order and control over its information technology systems, the company has decided to tighten the reigns on its employees and create an "Acceptable Use Policy" which begins with basic desktop security and the end user.

The policy will be one of openness, trust and integrity, not onerous, overbearing, security measures without purpose.

As a Network Administrator of Federated Legal Systems, Inc., my purpose is to show that having at least an Acceptable Use Policy in place can be a start to computer network security for this organization. In Shon Harris' book, *ALL IN ONE CISSP* she summarizes a list of reasons why an organization should have a security policy [1]:

- Identifies assets the company considers valuable
- Provides authority to the security team and its activities
- Provides reference to review when conflicts pertaining to security arise
- States the company's goal and objectives pertaining to security
- Outlines personal responsibility
- Helps to prevent unaccounted-for events (surprises)
- Defines the scope for the security team and its functions

While the above list may not be complete, it does lay out a basic framework of the goals of a policy. This Acceptable Use Policy might be considered by some, a bare minimum, but there were several important steps involved in creating this policy. Now that I had some of my goals in place, I needed to define what a policy was. The text in *Principles of Information* Security defines a policy as a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization [2]. Research of course, was next on the agenda. Because I've never created anything like this before, I needed to do my homework. Other sources like Debra Hermann's book, *A Practical Guide to Security Engineering and Information Assurance*, spoke on

the topic of Operational Security or OPSEC. OPSEC is the implementation of standardized operational procedures that define the nature and frequency of interaction between users, systems and system resources, the purpose of which is to: maintain a system in a known secure state at all times and to prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources. While this generally refers to a single system, the concept in itself can be applied to an overall review of this firm's network computer system because it does consider the actions of personnel and staff [3]. In this policy, personnel and staff are not only the main stakeholders, but also potential culprits. Information Week's Larry Greenemeier explained "Insiders aren't the most common security problem, but they can be among the most costly and the most damaging to a company's reputation [4]." While this does not exactly outline an acceptable use policy, it does set the groundwork.

In addition to research, I needed to determine what computer components of Federated Legal Systems, Inc. were at stake. This mission critical step led me directly to the employee. In order to successfully develop and acceptable use policy, I needed to know what assets needed securing at the end user level. Specifically, I needed to know what they used the computer for. This is where some brainstorming was needed. We all have some basic computer uses in common, like e-mail, word processing functions, internet surfing and of course network access. And, while I could attest to my own usage, I could not do that of my peers. Therefore, it was important for me to gather information about their computing habits. This step was completed by monitoring their behavior and creating a short survey. Independent of Lewis University, I conducted this survey with a portion of the staff of Federated Legal Systems, Inc. The survey itself had its own development process. The next section of this paper will provide more detailed information regarding that process and the results of that survey.

I believe that taking these first steps were all milestones in their own right, and began the development process of not just the survey, but an appropriate Acceptable Use Policy for employees, clients and colleagues of Federated Legal Systems, Inc.

# Survey Development Process

I began developing the following survey by first monitoring the computing behavior of all 60 employees of Federated Legal Systems, Inc. during a two-week period of time. The first day I noticed an employee absent from his office, but a stranger utilizing his workstation. That was the first issue that jarred me. How can employee allow outsiders that no one is aware of to just sit at their desk and start typing things. We had no idea of the identity of the individual or the work they were completing. The next day, I noticed that an employee had posted her password on the side of her monitor. So, that was a big "Are you kidding me? For the next couple of days, I went to other users machines and noticed passwords hiding in all sorts of places, including hanging on the bulleting board over someone's desk.

As the next two weeks progressed I notice a number of employees surfing all kinds of social networking sites. While this is a big deal at most companies, social networking sites are used in the successful defense of some of Federated Legal Systems, Inc.'s clients.

Another issue that sparked my attention at the company was email. Many employees receiving e-mail from unknown sources such as "you have a Hallmark greeting from your friend" this virus laden e-mail drove the IT staff nuts for days. Some employees were even participating in the chain letter like e-mails. So, as you can see the development of an employee survey was very much in order. I started by looking at five crucial areas that are directly related to the end users. This includes, web surfing, e-mail, password handling, workstation access and software utilization. I then spoke with management and realized they were equally guilty of the offenses of their employees. However, the good news is I received verbal authorization to complete the following survey to try and clean up some of the mistakes that could ultimately cost the organization, if not in time and money, certainly its pristine reputation for being a leader in its field.

I distributed the following survey to about fifty percent of Federated Legal Systems, Inc. employees addressing those crucial areas of concern and found after speaking with several key employees, something very surprising. Some employees actually stated they were not concerned computer security too much because of the nature of the business that Federated Legal Systems, Inc. was in and that they believed the physical security the office has in place is more that sufficient to protect the office. Other employees' lack of concern was centered on the fact, that many employees had been there for years and they had a trust factor, that surely none of their co-workers would do something negligent or illegal to destroy the reputation of the company or another employee.

After receiving this information, I was quite eager to chart the results of the survey and determine what policies that needed to be in place immediately to start curtailing the damaging behavior that the firm's employees were conducting while on work time.

# Computer Usage Survey

## Passwords:

How long have you had the same password?

Do you or have you ever shared your network password with anyone?

Do you post your network password around your work area such as on the side of your monitor or under your keyboard, etc..?

## Network Access:

Do you have a screen saver w/password requirement on your computer?

Have you allowed other people to access your computer other than information technology personnel? (Employees or Non-Employees)

## Internet Usage:

Do you visit sites like MySpace, Twitter, Face Book?

How Often? Daily Weekly (circle one)

Do you pay bills on-line at work?

## E-mail:

Do you open e-mail from unknown persons?

Do you forward spam or chain-like mail?

Do you send or receive personal email? How Often? Occasionally Regularly (circle one)

## Software Installation:

Have you ever personally downloaded software to your work computer?
What source? Internet personal property (circle one)

Did you receive permission before performing downloads?

Do you own a license for any software you have downloaded?

# Survey Results

While changing passwords is essential in network security, employees at Federated Legal Systems, Inc. have resisted changing their passwords in the past, and so there is no policy in forcing the change of passwords. Out of the 30 people surveyed, 17 of them stated that their password is more than one year old. That is an estimated 56% of the group. In that same group, I asked a question about sharing network passwords. As you can see from the chart below, 18 people shared their passwords with others including members outside of Federated Legal Systems, Inc.'s firm. That's 60% of this group. Reasons given for this behavior included, going on vacation, being asked by a boss for it, and trusting that their spouse or loyal friend wouldn't tell anyone.

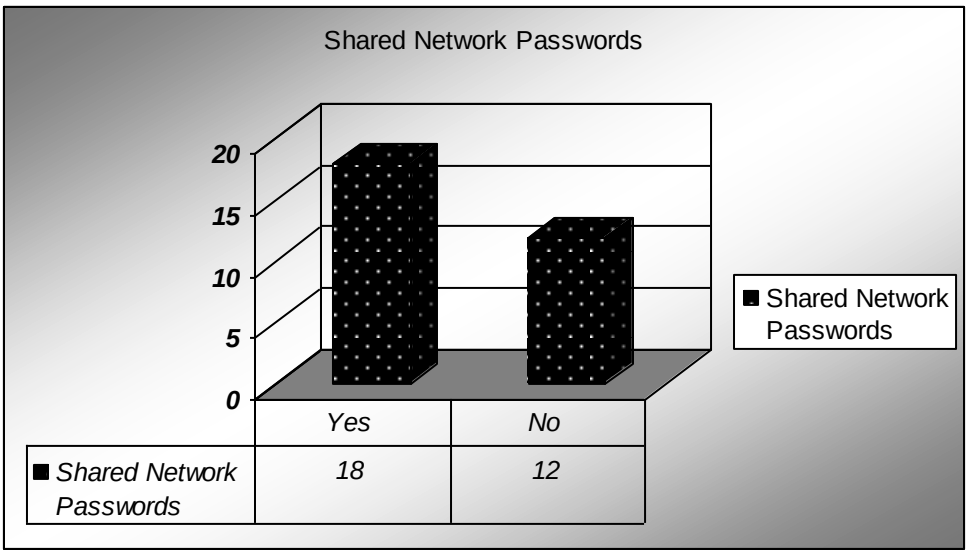


**Fig. 1 Shared Network Passwords**

The final question in the password category was about posting passwords. This is probably the cleanest area of the survey. Only 2 people admitted that they were careless in the storage of their

password. The other 93% 0r 28 employees thought it was a bad idea to publicly display their passwords for the world to see.

The next category on the survey was Network Access. This involved precautions that employees took or didn't take when they were away from their workstation for an extended period of time. The use of Screen Savers with password protect was not as widely used as I expected. Many employees just simply leave their workstation for lunch and assume no one would maliciously invade their computer. We did have one occurrence where an employee sat at the desk of some that was on lunch and deleted everyone single email that person had in the inbox and delete box. I guess no one took note of that disruptive event. Figure 2 gives a more detailed look at the data:

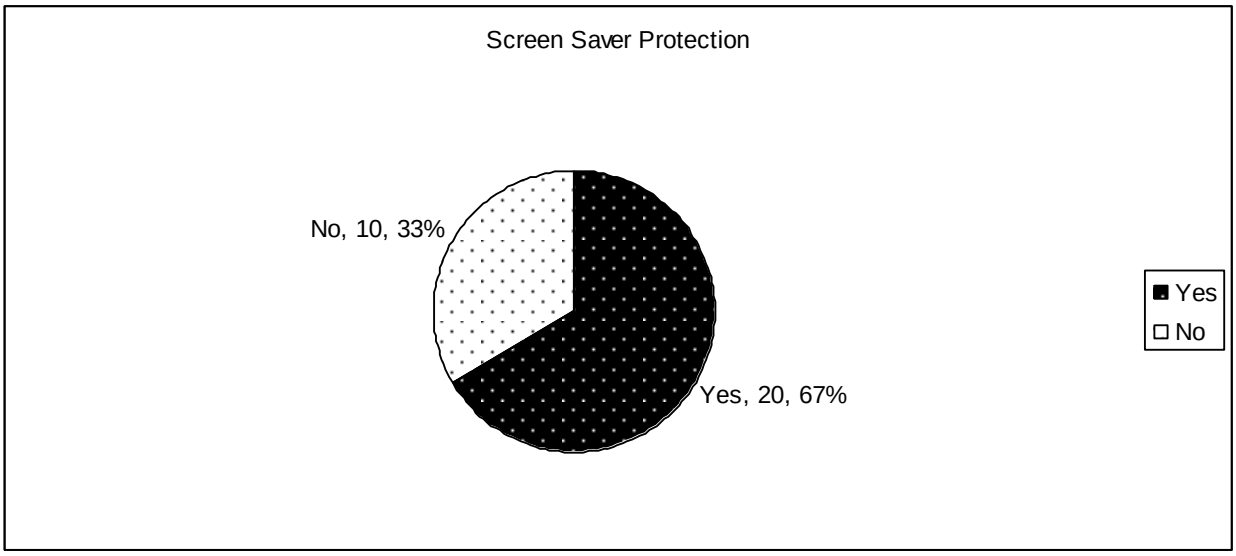


**Fig. 2 Screen Saver Protection**

That other question regarding network access is a crucial one. Why an employee would think it is acceptable to let unauthorized employees or non Federated Legal Systems, Inc. employees sit at

their computer and do anything? Unfortunately, not everyone is on the same page regarding this subject. 19 people of the 30 surveyed viewed this as a bad move, while 9 of those surveyed thought it was completely acceptable to do.

The third category in the survey deals with internet usage. Federated Legal Systems, Inc. does allow a portion of its legal staff to access social networking sites to help prepare their defense strategies for clients. The surveyed group results address this issue. Twitter, MySpace and Face Book are a vital source for the firm and therefore it's a burden both Management and IT must deal with.

The only difference with the social networking issue is the frequency of use of the sites. Of the 15 employees that use these sites, more than half surf them do so on daily basis. The rest of the group only visits the site when necessary to prepare a case. Those that are utilizing the sites on a daily are probably doing so for personal reasons because of the use, but not abuse rule at Federated Legal Systems, Inc.

The one question that I was curious about was the bill pay question. It's amazing to find out how many people actually pay their personal bills away from home. A an average 60 percent of the surveyed group state it's more convenient to do this on down time at work rather than wait until they get home at night. The chart below displays the results of that data:

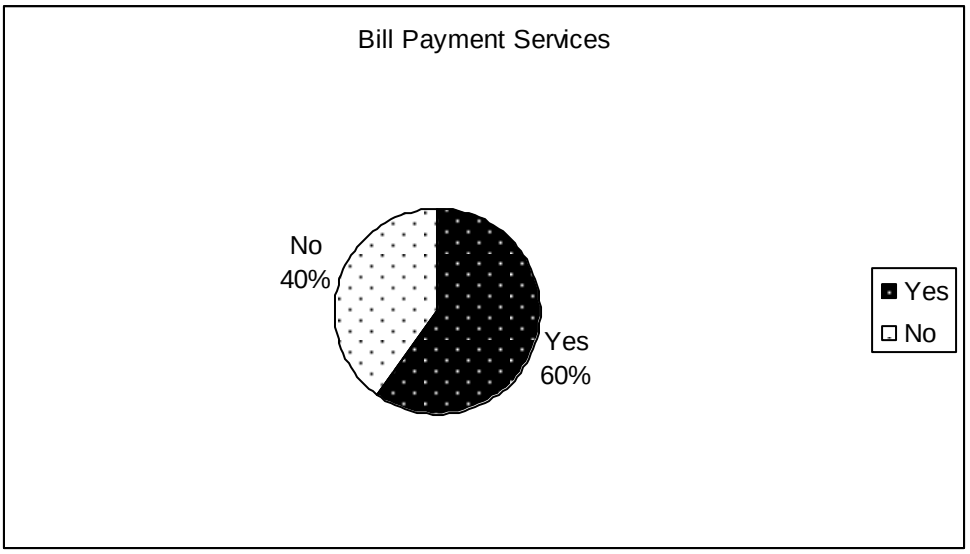


**Fig. 3 Bill Payment Services**

The Software Installation portion of the survey was equally interesting. About 13 surveyed stated they have downloaded software to their workstations. Of that thirteen, six of them neglected to get the necessary permission from a manager or IT to install any software themselves. More than half of that 13 also neglected to inquire about licensing for a product that they might have installed on their workstation.

When asked about opening emails from unknown sources 83% of the surveyed group stated that they do not and would not open e-mail from people they don't know. When I inquired about forwarding chain letter like emails or jokes 6 members of the group says that they are guilty of doing that but try to exercise caution when necessary, because they do realize that there is a potential risk to the firm's network. It is reassuring that there is some level of appreciation for the risks involved.

The last question to address in this category is regarding personal email. 26 of the 30 people surveyed stated that they both send and receive personal email. That's a staggering 87% of the people in the group. Again, this is where I believe that employees are taking advantage of that

occasional use, but not abuse policy at Federated Legal Systems, Inc. or they just don't care all together. Figure 4 below details the results of that data in a clearer form for this project:

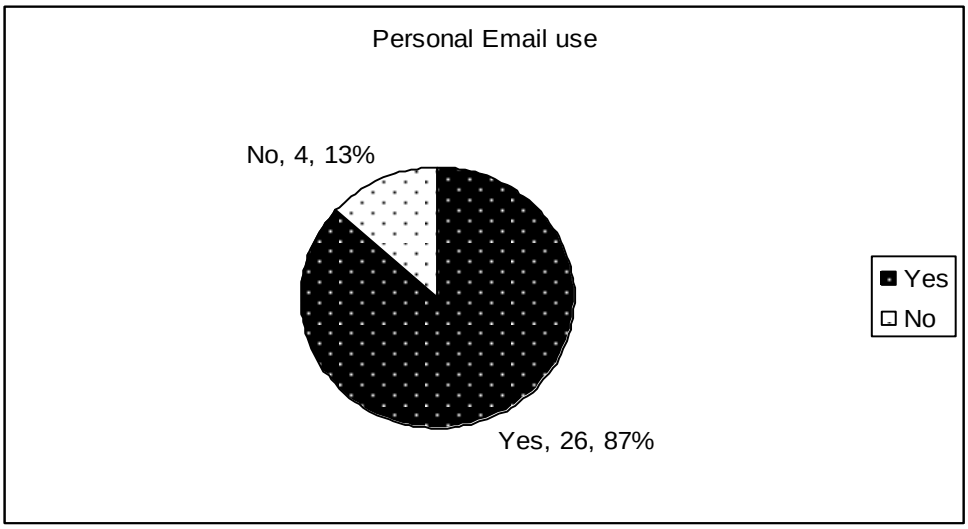


**Fig. 4 Personal Email Use**

Being able to chart this data really helped in completing the survey study. It showed me not only what activity the employees were performing on the network, but also to what extent. By collecting this data, a well-informed acceptable use policy can be created and attempt to reduce the occurrence of these bad practices. One of the main goals of any such policy is to educate the user. Previously, employees of this firm have been allowed to continue these negative practices without regard. However, if they can be properly educated by this basic policy, at the very least, they will have a better understanding of the pitfalls of bad computing behavior and possibly make and attempt to change them.

# Acceptable Use Policy Overview

Federated Legal Systems, Inc. Acceptable Use Policy has been established to protect its employees, colleagues, partners and the firm from illegal or damaging actions by individuals, either knowingly or unknowingly.

Federated Legal Systems, Inc.'s Internet, Intranet and Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic email systems, web browsing, and FTP services are the sole property of Federated Legal Systems, Inc.. These systems are to be used for business purposes in serving the interests of the firm, its partners and clients in the course of normal operations. .

Because effective security is a team effort, support and participation of every Federated Legal Systems, Inc. employee and affiliates who deal with information and/or information systems is expected. Therefore, it is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This overview is to serve as a guideline on the acceptable and unacceptable use of computer equipment owned and operated by the firm and its employees. These rules are in place to protect the employees and the firm from inappropriate use that expose the firm to risks which can range from viruses, hacker attacks, and legal action and security compromises of the network in general.

The scope of this outline and the following acceptable use policy applies to any and all parties, including employees, contractors and affiliates that utilize any Federated Legal Systems, Inc. property.

While Federated Legal Systems, Inc.'s 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 Federated Legal Systems, Inc. The first priority is to protect Federated Legal Systems, Inc.'s network, therefore, management cannot guarantee the confidentiality of information stored on any network device belonging to Federated Legal Systems, Inc.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. While individual departments may have additional guidelines concerning personal use of the internet, email and other computer systems, all employees are required to adhere to the Acceptable Policy Overview as a primer for handling equipment owned by Federated Legal Systems, Inc. In the absence of policies addressing specific questions regarding the usage of company property, an employee should consult their supervisor or manager.

Because there are several areas that directly apply to Federated Legal System, Inc. employees, this overview will only address basic generalities regarding those areas. The following Acceptable Use Policy is a culmination of several individual policies. Each of

which will outline specific rules that governs each section that must be followed by all employees. The basic framework of each of the following individual policies were adopted from ***SANS.org*** website which were created by and for SANS Institute and freely allows for modification of its Policies for this and other organizations including this Acceptable Use Policy Overview [5].

**I. Ethics**

Federated Legal Systems, Inc. purpose for an ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Federated Legal Systems, Inc. employee. Federated Legal Systems, Inc. will not tolerate any wrongdoing or impropriety at any time. Federated Legal Systems, Inc. will take the appropriate measures and act quickly in correcting issues involving the ethical code instituted by the firm. All employees should familiarize themselves with the ethics policy outlined in the Acceptable Use Policy [6].

**II. Confidentiality/Information Sensitivity**

Any and all data processed, stored or distributed by Federated Legal Systems, Inc. employees are considered sensitive and confidential. Therefore, each and every employee is responsible for understanding the rules outlined in the Acceptable Use Police regarding this area [7].

**III. Passwords**

Because passwords are the first level of our computer security systems at Federated Legal Systems, Inc., important measures must be taken to see that an adequate password is used on each and every system in the firm to protect itself. This means that every employee, vendor or contractor with access to computer accounts use the appropriate complexity measures outline in Federated Legal Systems, Inc. Password Policy [8].

**IV. Workstation Access**

As with all other property owned and operated by Federated Legal Systems, Inc. all employees should have a clear understanding that their workstations are no exception to the rule. Therefore, employees should take care to protect it and the assets contained within it. Employees should familiarize with the policy that governs workstation usage [9].

**V. Email Usage**

Email activities can have a major impact on Federated Legal Systems, Inc. if ever used inappropriately. Employees should take all necessary precautions when sending, forwarding, receiving solicited and unsolicited mail. This includes understanding the impact of engaging in “chain letters”, “pyramid schemes” and other potentially harmful activity. All employees that hold an e-mail account is required to abide by the Email Policy outlined in Federated Legal Systems, Inc. Acceptable Use Policy [10] [11] [12].

**VI. Software Installation**

Unless given express permission, no employee of Federated Legal Systems, Inc. should take it upon themselves to install software of any type to the workstation or laptop. The Information Technology Department exists for a purpose. If the firm does not own the necessary software for an employee to perform his or her job, he

should contact his direct supervisor for further direction. Employees are required to adhere to the Software Installation regarding this section [13].

## VII. Internet Usage

The internet can be very informative and quite helpful if used properly. However, employees must use good judgment when navigating to any websites on the network. The Internet Policy details basic guidelines to assist employees on the web [14].

## VIII. Anti-Virus Process

Because Viruses or prevalent in the computing world today, every employee is expected to use due diligence and care when dealing with data internal or external on Federated Legal Systems, Inc. computers. Details outlining the anti-virus process can be find in the Acceptable Use Policy [15] [16].

## IX. Personal Communication Devices

While several employees have been issued a variety of personal communications such as pagers or smart Phones, they are personally responsible for exercising due care that the items are not misplaced, abused or stolen. These employees must follow the Personal Communication Devices Policy accordingly [17].

## X. Removable Devices

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at Federated Legal Systems, Inc. Because these devices can contain confidential company data, written approval must be obtained from the Information Technology Manager and the Director of Operations. The devices must also contain encryption or equally stronger measures to protect the stored data [18].

## XI. Remote Access

While there is a group of personnel that are allowed to access Federated Legal Systems, Inc. network resources from home, all employees are required to known the specifics of the Remote Access Policy thoroughly [19].

## XII. VPN Access

This policy outlines the purpose and process of accessing the Virtual Private Network at Federated Legal Systems, Inc. [20].

## XIII. Clean Desk

Because first impressions often start with the first contact, Federated Legal Systems, Inc.'s goal requires employees to adhere to the newly implemented clean desk policy. This will not only assist with security measures, but also project a positive image to Federated Legal Systems, Inc. clients. Employees should ensure that they comply with this rule under the Acceptable Use Policy [21].

# I. ETHICS

## 1. Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will server to guide business behavior to ensure ethical conduct

## 2. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Federated Legal Systems, Inc. including all personnel affiliated with third parties.

## 3. Policy

### 3.1 Executive Commitment to Ethics

3.1.1 Top Administration Officials within Federated Legal Systems Inc. must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

3.1.2 Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

3.1.3 Executives must disclose any conflict of interests regard their position within Federated Legal Systems, Inc.

### 3.2. Employee Commitment to Ethics

3.2.1 Federated Legal Systems, Inc., employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

3.2.2 Every employee needs to apply effort and intelligence in maintaining ethics value.

3.2.3 Employees must disclose any conflicts of interests regarding their position within Federated Legal Systems, Inc.

3.2.4 Employees will help Federated Legal Systems, Inc. to increase client and law enforcement satisfaction by providing quality service and responding timely to case inquiries.

### 3.3 Company Awareness

3.3.2 Promotion of ethical conduct within interpersonal communications of employees will be acknowledged.

3.3.3 Federated Legal Systems, Inc. will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

### 3.4 Maintaining Ethical Practices

3.4.2 Federated Legal Systems, Inc. will reinforce the importance of the integrity message which will start with Office Administration. Every employee, supervisor, director and chief will consistently maintain an ethical stance and support ethical behavior.

3.4.3 Employees at Federated Legal Systems, Inc, should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

3.4.4 Federated Legal Systems, Inc. has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

**3.5 Unethical Behavior**

3.5.2 Federated Legal Systems, Inc. will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

3.5.3 Employees at Federated Legal Systems, Inc. will not tolerate harassment or discrimination.

3.5.4 Unauthorized use of office strategies, law enforcement information sources, operational, personnel, financial, source code & technical information integral to the success of our the firm will not be tolerated.

3.5.5 Federated Legal Systems, Inc. will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

3.5.6 Federated Legal Systems, Inc. employees will not use corporate assets or business relationships for personal use or gain.

## 4. Enforcement

4.1 Any infractions of this code of ethics will not be tolerated and Federate Legal Systems, Inc. will act quickly in correcting the issue if the ethical code is broken.

4.2 Any employee found to have violated this policy may be subject to disciplinary actions, up to an including termination of employment.

## 5. REF: [6].

# II. CONFIDENTIALITY

## 1. Purpose

The Confidentiality Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Federated Legal Systems, Inc. without proper authorization.

The information covered in these guidelines, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually including telephone and video conferences.

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Federated Legal Systems, Inc.'s confidential information (e.g., Federated Legal Systems, Inc. confidential information should not be left unattended in conference rooms).

## 2. Scope

2.1 All Federated Legal Systems, Inc. information is categorized into to two main classifications:
Federated Legal Systems, Inc. Public
Federated Legal Systems, Inc. Confidential

All Federated Legal Systems, Inc. Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Federated Legal Systems, Inc.

All Federated Legal Systems, Inc. Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as case strategies, development programs, potential acquisition targets, and other information integral to the success of the company. Also included is Federated Legal Systems, Inc. confidential information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Federated Legal Systems, Inc. Confidential information is "Federated Legal Systems, Inc. Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which as been entrusted to Federated Legal Systems, Inc. by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to expert witnesses, clients and law enforcement personnel. Extremely sensitive information includes information about confidential sources and whistleblowers that work closely with Federated Legal Systems, Inc. employees.

Federated Legal Systems, Inc. personnel are encouraged to use common sense judgment in securing Federated Legal Systems, Inc. Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his supervisor.

## 3. Policy

The sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Federated Legal Systems, Inc. confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of Federated Legal Systems, Inc. Confidential information in questions.

Minimal Sensitivity: General corporate information; some personnel and technical information.

## 4. Enforcement

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

## 5. REF: [7].

# III. PASSSWORD POLICY

## 1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## 2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Federated Legal Systems, Inc. facility, has access to the Federated Legal Systems, Inc. network, or stores any non-public Federated Legal Systems, Inc. information.

## 3. Policy

### 3.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- App production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 4 months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other electronic forms of communications.
- All user-level and system-level passwords must conform to the guidelines described below.

### 3.2 Guidelines

1.1.1 General Password Construction Guidelines

Passwords are used for various purposes at Federated Legal Systems, Inc. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail, and local route logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor or weak passwords have the following characteristics:

- The password contains less than six characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family members, pets, friends, co-workers, fantasy characters, etc.
    - The words "Federated Legal System, Inc." "Federated", "Federated" or any derivation of the company's name.

- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, qweew, etc.

3.3 Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./).
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a word in any language, slang, dialect, jargon, etc?
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

3.4 Password Protection Standards

Do not use the same password for Federated Legal Systems, Inc. accounts as for other non-Federated Legal Systems, Inc. access (e.g., personal ISP account, option trading, benefits, etc…). Where possible, don't use the same passwords for various Federated Legal Systems, Inc. access needs. For example, select one password for the Engineering systems and a separate password for AIT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Federated Legal Systems, Inc. passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Federated Legal Systems, Inc. information.

Here is a list of "don'ts:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name)
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the information Security Department or Management.

Don't use the "Remember Password" feature on any of your applications (e.g., Outlook, Netscape Messenger).

Again, passwords should not be written down and stored anywhere in the office. Do not store passwords in any file on ANY computer system (including Palm Pilots or similar devices) without encryption. And, all employees are required t o change passwords at least once very 4 months.

### 4. Enforcement

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

## 5. REF: [8].

# IV. WORKSTATION/NETWORK ACCESS

## 1. PURPOSE

The purpose of this policy is to establish a standard for guideline for access to the office network resources.

## 2. SCOPE

The policy applies to all Federated Legal Systems, Inc. employees, contractors, workforce members, vendors and agents with a Federated Legal Systems, Inc. owned or personal-workstation connect to the Federated Legal Systems, Inc. network.

## 3. POLICY

Appropriate measure must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access sensitive information is restricted to authorized persons.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

3.2 Federated Legal Systems, Inc. will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.3 Appropriate measures may include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area for an extended period of time to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers in cabinets.
- Complying with Portable Workstation Encryption Policy.
- Complying with the Anti-Virus Policy.
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.

- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access Policy.

## 4. ENFORCEMENT

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

## 5. REF: [9].

# V. EMAIL USE POLICY

## 1. Purpose

To prevent tarnishing the public image of Federated Legal Systems, Inc., when email goes out from Federated Legal Systems, Inc. the public will tend to view that message as an official policy statement from Federated Legal Systems, Inc. to prevent the unauthorized or inadvertent disclosure of sensitive company information.

## 2. Scope

This policy covers appropriate use of any email sent from a Federated Legal Systems, Inc. email address and applies to all employees, vendors and agents operating on behalf of Federated Legal Systems, Inc. This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Federated Legal Systems, Inc.

## 3. Policy

- **Prohibited Use**

The Federated Legal Systems, Inc. email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content form any Federated Legal System employee should report the matter to their supervisor immediately.

- **Unauthorized Use of Sensitive Information**

Information is considered sensitive if it can be damaging to Federated Legal Systems, Inc. or its clients reputation. Therefore, intentional or unintentional revealing of restricted information to people, both inside and outside Federated Legal Systems, Inc. who do not have a need to know that information is a violation of this policy.

- **Automatically Forwarding Email**

Employees must exercise utmost caution when sending any email from inside Federated Legal Systems, Inc. to an outside network. Unless approved by an employee's manager at Federated Legal Systems, Inc. email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy.*

- **Personal Use**

Using a reasonable amount of Federated Legal Systems, Inc. resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Federated Legal Systems, Inc. email account is prohibited. Virus or malware warnings and mass mailings from Federated Legal Systems, Inc., shall be approved by Federated Legal Systems, Inc., Inc. Director of Operations before sending. These restrictions apply to the forwarding of mail received by a Federated Legal Systems, Inc., Inc. employee.

- **Monitoring**

Federated Legal Systems, Inc. employees shall have no expectation of privacy in anything they store, send or received on the company's email system. While Federated Legal Systems, Inc. is not obliged to monitor email messages, Federated Legal System, Inc. may monitor messages without prior notice.

- **Email Retention**

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained for how long. The retention specifications regarding email are secondary to Federate Legal Systems, Inc. policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All Federated Legal Systems Inc. email information is categorized into four main classifications with retention guidelines:

Administrative Correspondence (4 years)
Fiscal Correspondence (4 years)
General Correspondence (1 year)
Ephemeral Correspondence (Retain until read, destroy)

a. Administrative Correspondence

Federated Legal Systems, Inc., Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@FederatedLegalSystemsInc.com has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department**.**

b. Fiscal Correspondence

Federated Legal Systems, Inc. Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@FederatedLegalSystemsInc.com has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

c. General Correspondence

Federated Legal Systems, Inc. General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence**.**

d. Ephemeral Correspondence

Federated Legal Systems, Inc. Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

e. Instant Messenger Correspondence

Federated Legal Systems, Inc. Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriated email retention address.

f. Encrypted Communications

Federated Legal Systems, Inc. encrypted communications should be stored in a manner consistent with Federated Legal Systems, Inc. Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

g. Recovering Deleted Email via Backup Media

Federated Legal Systems, Inc. maintains backup tapes from the email server and once a quarter a set of tapes is taken out of ration and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

## 4. Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action, up to an including termination of employment.

## 5. REF: [10] [11] [12].

# VI. SOFTWARE INSTALLATION POLICY

## 1. Purpose

To prevent the firm from being exposed to unnecessary threats such as hacking, malware, conflicting file version or other incompatibility issues, Federated Legal Systems, Inc. has instituted a software installation policy which prohibits employees from personally installing software on their workstations.

## 2. Scope

This policy applies to all Federated Legal Systems, Inc. computers, servers, PDA's, smart phones and other computing devices operating within Federated Legal Systems, Inc.

## 3. Policy

1. Employees may not personally install software on Federated Legal Systems, Inc. computing devices operated within the Federated Legal Systems, Inc. network. Software requests must first be approved by the requester's supervisor and then be made to the Information Technology division via email or in writing.
2. Software must be selected from an approved software list, maintained by the Information Technology division, unless no selection on the list meets the requester's need.
3. A copy of a valid license must be submitted to the Information Technology division, if the requested software is not part of Federated Legal Systems, Inc. approved software list.
4. The Information Technology division will obtain and track the licenses, test new software for conflict and compatibility issues, and perform the installation.

## 4. Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action, up to an including termination of employment.

## 5. REF: [13].

# VII. INTERNET USAGE POLICY

## 1 Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use form any host within Federated Legal Systems, Inc.'s network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

## 2. Scope

This policy applies to all Federated Legal Systems, Inc. employees, contractors, vendors and agents with a Federated Legal Systems, Inc. owned or personally-owned computer or workstation connected to the Federated Legal Systems, Inc. network. The policy applies to all end user initiated communications between Federated Legal Systems, Inc. network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

## 3. Policy

1) **Web Site Monitoring**

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

2) **Access to Web Site Monitoring Reports**

General trending and activity reports will be made available to any employees as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email requests to Information Systems form a Human Resources Representative.

3) **Internet Use Filtering System**

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Federated Legal Systems, Inc. corporate environment. The following protocols and categories of websites will be blocked:

- Adult/Sexually Explicit Material
- Advertisement & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Spam, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

4) **Internet Use Filtering Rule Changes**

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

5) **Internet Use Filtering Exceptions**

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticked to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

## 4. Enforcement

The IT Security Officer will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy.

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

**5. REF: [14].**

# VIII. ANTI VIRUS POLICY

1. **Purpose**
    - **a.** The main reasons for an Anti Virus policy are:
        - **i.** A clean desk can produce a positive image when our customers visit the company.
        - **ii.** It reduces the threat of a security incident as confidential information will be locked away when unattended.
        - **iii.** Sensitive documents left in the open can be stolen by a malicious entity.

2. **Responsibility**
    - **a.** All staff, employees and entities working on behalf of <company> are subject to this policy

3. **Scope**
    - **a.** At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
    - **b.** At the end of the working day the employee is expected to tidy their desk and to put away all office papers. <Company> provides locking desks and filing cabinets for this purpose.

4. **Action**
    - **a.** Always run the corporate standard, supported anti-virus software is available from the application services network drive. Download and run the version the current version; download and install anti-virus software updates as they become available.
    - **b.** **NEVER** open any files ore macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
    - **c.** **Delete** spam, chain letters, and other junk email without forwarding, in with Federated Legal System's Acceptable use Policy
    - **d.** Never download files from unknown or suspicious sources.
    - **e.** Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
    - **f.** Always scan a floppy diskette from an unknown source for viruses before using it.
    - **g.** Back-up critical data and system configurations on a regular basis and store the data in a safe place.
    - **h.** If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

i. New viruses are discovered almost every day. Periodically check the Lab Anti-Virus Policy and this Recommended Process list for updates.
j. Allocate time in your calendar to clear away your paperwork.
k. Always clear your workspace before leaving for longer periods of time.
l. If in doubt – throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept – it will probably be better to place it in the shred bin.
m. Consider scanning paper items and filing them electronically in your workstation.
n. Use the recycling bins for sensitive documents when they are no longer needed.
o. Lock your desk and filing cabinets at the end of the day
p. Lock away portable computing devices such as laptops or PDA devices
q. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

5. **Enforcement**
   a. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6. REF: [15] [16].

# IX. PERSONAL COMMUNICATION DEVICES

## 1. Purpose

This policy describes Information Security's requirements for Personal Communication Devices for Federated Legal Systems, Inc.

## 2. Scope

This policy applies to any use of Personal Communication Devices issued by Federated Legal Systems, Inc. or used for Federated Legal Systems, Inc. business.

## 3. Policy

i. Issuing Policy

ii. Personal Communication Devices (PCD's) will be issued only to Federated Legal Systems, Inc. personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCD's are defined to include handled wireless devices, cellular telephones including BlackBerry's, laptop's, flash drives, external hard drives, cameras and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, Federated Legal Systems, Inc. personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters; Bluetooth 2.0 Class 1 devices have a range of 330 feet.

iii. Loss and Theft

Files containing confidential or sensitive data may not be stored in PCD's unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment in also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

Personal Use

PCD's are issued for Federated Legal Systems, Inc. business. Personal use should be limited to minimize incidental use.

Conducting telephone calls or utilizing PCD's while drive can be a safety hazard. Drivers should use PCD's while parked or out of the vehicle. If employees must use a PCD while driving, Federated Legal Systems, Inc. requires the use of hands-free enabling deives.

## 4. Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action that leads to be ineligible for continued use of PCD's. Extreme cases could lead to additional discipline, up to an including termination of employment.

## 5. REF: [17].

# X. REMOVABLE MEDIA POLICY

## 1. Purpose

To minimize the risk of loss or exposure of sensitive information maintained by Federated Legal Systems, Inc. and to reduce the risk of acquiring malware infections on computers operated by Federated Legal Systems, Inc.

## 2. Scope

This policy covers all computers and severs operating in Federated Legal Systems, Inc.

## 3. Policy

a. Federated Legal Systems, Inc. staff may only use Federated Legal Systems, Inc. issued removable media in their work computers.
b. Federated Legal Systems, Inc. issued removable media may not be connected to or used in computers that are not owned or leased by Federated Legal Systems, Inc. without explicit permission of the Federated Legal Systems, Inc. Information Technology staff.
c. Sensitive information should be stored on removable media only when required in the performance of the employee's assigned duties or when providing information required by other state or federal agencies.
d. When sensitive information is stored on removable media, it must be encrypted in accordance with Federated Legal Systems, Inc. Acceptable Encryption Policy.
e. Exceptions to this policy may be requested on a case-by-case basis by Federated Legal Systems, Inc. exception procedures**.**

## 4. Enforcement

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

## 5. REF: [18].

# XI. REMOTE ACCESS POLICY

## 1. Purpose

The purpose of this policy is to define standards for connecting to Federated Legal Systems, Inc.'s network from any host. These standards are signed to minimize the potential exposure to Federated Legal Systems, Inc. from damages which my result from unauthorized use of Federated Legal Systems, Inc. resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Federated Legal Systems, Inc. internal, systems, etc.

## 2. Scope

This policy applies to all Federated Legal Systems, Inc. employees, contractors, vendors and agents with a Federated Legal Systems, Inc. owned or personally-owned computer or workstation used to connect to the Federated Legal Systems, Inc. network. This policy applies to remote access connections used to do work on behalf of Federated Legal Systems, Inc., including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

## 3. Policy

a. General

1. It is the responsibility of Federated Legal Systems, Inc. employees, contractors, vendors and agents with remote access privileges to Federated Legal Systems, Inc.'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Federated Legal Systems, Inc.
2. General access to the Internet for recreational use by immediate household members through the Federated Legal Systems, Inc. Network on personal computers is permitted for employees that have flat-rate services. The Federated Legal Systems, Inc. employee is responsible to ensure the family member does not violate any Federated Legal Systems, Inc. policies, does not perform illegal activities, and does not use the access for outside business interests. The Federated Legal Systems, Inc. employee bears responsibility for the consequences should the access is misused.
3. Please review thee following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Federated Legal Systems, Inc.'s network:
    a. Acceptable Encryption Policy
    b. Virtual Private Network (VPN) Policy
    c. Wireless Communications Policy
    d. Acceptable Use Policy

4. For additional information regarding Federated Legal Systems, Inc.'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

i. Requirements

1. Securing remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Federated Legal Systems, Inc. employee provide their login or email password to anyone, not even family members.
3. Federated Legal Systems, Inc. employees and contractors with remote access privileges must ensure that their Federated Legal Systems, Inc. owned or personal computer or workstation, which is remotely connected to Federated Legal Systems, Inc's network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the users.
4. Federated Legal Systems, Inc. employees and contractors with remote access privileges to Federated Legal Systems, Inc. corporate network must not use non Federated Legal Systems, Inc. email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Federated Legal Systems, Inc. business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Federated Legal Systems, Inc. network must meet minimum authentication of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to Federated Legal Systems, Inc. internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
10. Personal equipment that is sued to connect to Federated Legal Systems, Inc.'s networks must meet the requirements of Federated Legal Systems, Inc. owned equipment for remote access.
11. Organizations or individuals who which to implement non-standard Remote Access solutions to the Federated Legal Systems, Inc. production network must obtain prior approval from Remote Access Services and InfoSec.

## 4. Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action, up to an including termination of employment.

## 5. REF: [19].

# XII. VPN ACCESS

## 1. Purpose

The scope of this policy is to define appropriate VPN access and its use by authorized personnel.

## 2. Scope

This Policy pertains to all employees that are authorized to use VPN Access on Federated Legal Systems, Inc. computer systems.

## 3. Policy

Federated Legal Systems, Inc. employees can use VPN connects to gain access to the corporate network. Appropriate measure must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access sensitive information is restricted to authorized persons.

3.4 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

3.5 Federated Legal Systems, Inc. will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.6 Appropriate measures may include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area for an extended period of time to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers in cabinets.
- Complying with Portable Workstation Encryption Policy.
- Complying with the Anti-Virus Policy.
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access Policy.

## 4. Enforcement

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

## 5. REF: [20]

# XIII. CLEAN DESK POLICY

## 1. Purpose

The main reasons for a clean desk policy are:

1. A clean desk can produce a positive image when clients visit the company.
2. It reduces the threat of a security incident as confidential information will be locked away when an employee's desk is unattended.
3. Sensitive documents left in the open can be stolen by a malicious entity.

## 2. Scope

All staff, employees and entities working on behalf of Federated Legal Systems are subject to this policy

- ✓ At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
- ✓ At the end of the working day the employee is expected to tidy their desk and to put away all office papers. Federated Legal Systems provides locking desks and filing cabinets for this purpose.

## 3. Action

- ✓ Allocate time in your calendar to clear away your paperwork.
- ✓ Always clear your workspace before leaving for longer periods of time.
    - If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.
    - Consider scanning paper items and filing them electronically in your workstation or your network drive. Office copiers have been designated as scanners and every employee can create their own personal folders on their local workstations to save such documents.
    - Use the recycling or shredders bins for sensitive documents when they are no longer needed.
    - Lock your desk and filing cabinets at the end of the day.
    - Lock away portable computing devices such as laptops, Digital Cameras or PDA devices.
    - Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

## 4. Enforcement

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

## 5. REF: [22].

# GLOSSARY

**Acceptable Use** An organization's policy that provides specific detail about what users may do with their network access, including email and instant messaging usage for personal purposes, limitations on access times, and the storage space available to each user.

**Antispam** A software program that can add another layer of defense to the infrastructure by filtering out undesirable email.

**Antivirus**
used for protecting the user environment that scans for email and downloadable malicious code.

**Appropriate Measures**
To minimize risks to Federated Legal Systems, Inc. from an outside business connection. Federated Legal Systems, Inc. computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Federated Legal Systems, Inc. corporate information, the amount of information at risk is minimized.

**Approved Electronic File Transmission Methods**
Includes supported FTP clients and Web browsers.
**Approved Electronic Mail**
All mail systems supported by the IT Support Team. These include, but are not necessarily limited to, Federated Legal Systems, Inc.

**Approved Encrypted email and files**
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Federated Legal Systems, Inc. is done via a license. Please contact the appropriate support organization if you require a license.

**Approved Instant Messenger** The Jabber Secure IM Client is the only IM that is approved for use on Federated Legal Systems, Inc. computers.

**Asset** A company or personal resource that has value.

**Authorization** The process of identifying what a give user is allowed to do.

**Availability**
Accessibility to information

**Bluetooth An** industrial specification for wireless personal area networks. Bluethooth provides a way to connect and exchange information between devices such as PDA's.

**CD:** A *compact disc* (sometimes spelled *disk)* is a small, portable, round medium made of molded polymer (close in size to the floppy disc) for electronically recording, storing, and playing back audio, video, text, and other information in digital form

**Chain Email or Letter**
Email sent successive people. Typically the body of the not has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

**Confidentiality** Involves a rigorous set of controls and classifications associated with sensitive information to ensure that such information is neither intentionally nor unintentionally disclosed.

**DVD:** The *digital versatile disc* stores much more than a CD and is used for playing

back or recording movies. The audio quality on a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.

**Domain** A group of computers that share a security policy and a user account database.

**Due Care** Assurance that the necessary steps are followed to satisfy a specific requirement, which can be an internal or external requirement, as in an agency regulation.

**Email** The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.

**Environment** The physical conditions that affect and influence growth, development, and survival.

**Extranet** A special internetwork architecture wherein a company's or organization's external partners and customers are granted access to some parts of its intranet and the services it provides in a secure, controlled fashion.

**Encryption** A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

**Ethics** Business ethics can be defined as written and unwritten codes of principles and values that govern decisions and actions within a company. In the business world, the organization's culture sets standards for determining the difference between good and bad decision making and behavior.

**Forwarded email** Email resent to successive people.

**Hacking** Sites that provide content about breaking or subverting computer security controls.

**Handheld wireless device:** A communication device small enough to be carried in the hand or pocket and is also known as a Personal Digital Assistant (PDA). Various brands are available, and each performs some similar or some distinct functions. It can provide access to other internet services, can be centrally managed via a server, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and for maintaining a built-in address book and personal schedule.

**Individual Access Controls** Individual Access Controls are methods of electronically protecting files from being access by people other than those specifically designated by the owner.

**Insecure Internet Links** Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Federated Legal Systems, Inc.

**Incident** Any violation or threatened violation of a security policy.

**Incident Response** A clear action plan on what each response team member needs to do and when it has to be done in the event of an emergency or a security incident.

**Integrity** Involves a monitoring and management system that performs integrity checks and protects systems from unauthorized modifications to data, system, and application files. When applied to messages or data in transit, integrity checks rely on calculating hash digest values before and after transmission to ensure nothing changed between the time the data was sent and the time it was received.

**Intranet** A portion of the information technology infrastructure that belongs to and is controlled by the company in question.

**IP Address** Unique network address assigned to each device to allow it to communicate with other

devices on the network or internet.

**Malware** Software of malicious intent/impact such as viruses, worms, and spyware.

**Media Type Model:** Refers to the brand of media device such as Sony, Treo, or IBM.

**Media Type:** For the purpose of this policy, the term "media type" is interchangeable with "mobile device." Not to be confused with media makes, models, or brands.

**Message** The content and format a sender chooses to use to communicate with some receiver across a network, an intranet, an extranet, or the Internet.

**Misuse** Misuse is typically used to refer to unauthorized access by internal parties.

**Mobile Devices:** Mobile media devices include, but are not limited to: PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

**Modems:** A device that modulates and demodulates information so that two computers can communicate over a phone line, cable line, or wireless connection. The connection talks to the modem, which connects to another modem that in turn talks to the computer on its side of the connection. The two modems talk back and forth until the two computers have no further need of either modem's translation services.

**Network** Two or more computers connect for the purpose of sharing resources.

**OPSEC** "Operational Security or OPSEC is defined as the implementation of standardized operational procedures that define the nature and frequency of interaction between users, systems and system resources, the purpose of which is to: maintain a system in a known secure state at all times and to prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources.

**PDA:** The *Personal Digital Assistant* is also known as a handheld. It is any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. Many people use the name of one of the popular PDA products as a generic term, such as Hewlett-Packard's Palmtop and 3Com's PalmPilot.

**Peer to Peer File Sharing** Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

**Phishing** attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

**Policy** is a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization.

**Pop-up blocker** A program used to block a common method for Internet advertising, using a window that pops up in the middle of your screen to display a message when you click a link or button a website.

**Procedure** A procedure specifies how policies will be put into practice in an environment (that is, it provides necessary how-to instructions).

**Remote Access Service** Allows user to connect from remote access locations and access their

networks for file and printer sharing and e-mail.

**Removable Media** Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Federated Legal Systems, Inc.

**Retention Policy** Documentation of the amount of time an organization will retain information.

**Risk** The potential that a threat might exploit some vulnerability.

**Sensitive Information** Information that if made available to unauthorized persons is considered sensitive if it can be damaging to Federated Legal Systems, Inc. or its clients and or both parties reputation.

**Social Networking Services** Internet sites such as Myspace and Facebook that allow users to post content, chat, and interace in online communities.

**SPAM** Unsolicited Internet Email. SPAM sites are websites linked to and from unsolicited Internet mail messages.

**Secure Shell (SSH)** A protocol designed to support secure remote login, along with secure access to other services across an unsecure network. SSH includes a secure transport layer protocol that provides server authentication, confidentiality (encryption), and integrity (message digest functions), along with a user-authentication protocol and a connection protocol that runs on top of the user-authentication protocol.

**Threat** A danger to a computer network or system.

**Third Party** A business that is not a formal or subsidiary part of Federated Legal Information Systems, Inc.

**Unauthorized Disclosure** The intentional or unintentional revealing of restricted information to people, both inside and outside Federated Legal Systems, Inc. who does not have a need to know that information.

**User ID** User Name or other identifier used when an associate logs into the corporate network.

**Virtual Private Network (VPN)** A popular technology that supports reasonably secure, logical, private network links across some unsecure public network infrastructure, such as the internet.

**Virus** A piece of malicious code that spreads to other computers by design.

**Wireless Networking Cards:** Mobile device for wireless internet connectivity from a laptop. This card allows mobile users the ability to access a secured connection to the internet via a specified vendor.

# WORKS CITED


[1] Harris, Shon. *ALL-IN-ONE CISSP EXAM GUIDE, FOURTH EDITION.* McGRAW-HILL OSBORNE COMPANIES. 2008

[2] Whitman, Michael E. and Mattord, Herbert J. *Principles of Information Security.* Thomson Course Technology, 2005.

[3] Herrmann, Debra S. *A Practical Guide to Security Engineering and Information Assurance.* Auerbach CRC Press LLC, 2002

[4] Information Week Magazine article; Dec. 11, 2006 by Larry Greenemeier; "*Insider Threats*."

[5] Acceptable Use Policy- Retrieved June, 2009, from SANS.org website: http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

[6] Ethics Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Ethics Policy.pdf

[7] Information Sensitivity Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf

[8] Password Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Password_Policy.pdf

[9] Workstation Security Policy – Retrieved June 2, 2009 from SANS Institute website: http://www.sans.edu/resources/student_projects/200802_002.doc

[10] Email Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Email Policy.pdf

[11] Automatically Forwarded Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Automatically_Forwarded_Email_Policy.pdf

[12] Email Retention – Retrieved May 23, 2009 from SANS Institute website: http://www.sans.org/resources/policies/email_retention.pdf

[13] Software Installation Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.edu/resources/student_projects/200711_002.pdf

[14] Employee Internet Use Monitoring and Filtering Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.edu/resources/student_projects/200711_004.pdf

[15] Guidelines on Anti Virus Process - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Anti-virus Guidelines.pdf

[16] AntiVirus Process Anti-Virus Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Lab_Anti-Virus_Policy.pdf

[17] Personal Communication Device Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Personal_Communication_Device.pdf

[18] Removable Media - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Removable_Media.pdf

[19] Remote Access Policy - Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Remote_Access_Policy.pdf

[20] Virtual Private Network (VPN) Policy – Retrieved May 13, 2009 from SANS Institute website: http://www.sans.org/resources/policies/Virtual_Private_Network.pdf

[21] Clean Desk Policy - Retrieved May 23, 2009 from SANS Institute website: http://search.sans.org/search?q=cache:q_0E4x-RbP4J:www.sans.org/info/27959+clean&access=p&


555 S. Union Blvd. • 7th Floor
Phone 555.866.7890 • Fax 555.456.7890