

Implementing a Security Awareness Program for a Non-Profit Organization

Nancy A. Kolb
68-595: Information Security Project
Fall 2008

Table of Contents

I. Confidentiality, Integrity, Availability (CIA).....	3
Protection of Information Assets.....	4
II. Risks	5
Financial Loss.....	5
Cost of Investigative Process	5
Loss of Reputation.....	5
Fractured or Weakened Relationships.....	5
Employee Defections.....	5
Donor Disenchantment and Loss	6
Litigation	6
Damaged Morale	6
III. Defense in Depth.....	6
A. Risk Assessment.....	7
B. Security policy	7
C. Organizational Security	7
D. Asset Management - inventory and classification of information assets	8
E. Human Resources Security.....	8
F. Physical and Environmental Security	9
G. Communications and Operations Management	9
H. Access Control.....	10
I. Information Systems Acquisition, Development and Maintenance	10
J. Information Security Incident Management	11
K. Business Continuity Management.....	11
L. Compliance	12
IV. Information Security Awareness	12
V. Implementing a Security Awareness Program	12
Get buy-in from the top	13
Assemble a Team.....	13
Assess the Environment	13
Survey Employees.....	13
Educate the User.....	14
On-going Monthly Awareness Campaigns	16
Conclusion	19
Acceptable Use Policy	20
Appendix B – Password Policy.....	25
Appendix C – Email Use Policy	29
Appendix D - Free Resources:	31
Works Cited:.....	32

In the non-profit world, raising funds is a major factor in the key to success. Although many non-profit organizations focus their time and money on strategies of fundraising and operations, technology and protecting their data is usually not high on the priority list. Furthermore, non-profit organizations are not required by law to follow IT Federal regulations or rules, such as the Public Company Accounting Reform and Investor Protection Act of 2002 (SOX). However, if their data is compromised, there is a potential for them to lose their value or tarnish their reputations with their constituents.

A good example of tarnished reputations is United Way scandal of 2002. According to the Chronicle of Philanthropy [1], the United Way of Washington experienced immeasurable damage due to their Chief Executive Officer inappropriately taking funds in excess of \$500,000.00. The next fundraising campaign following the scandal received \$38 million opposed to the \$90 million they received before the scandal. The organization's employee size shrunk from 90 to 35. If good policies and procedures were in place, the CEO would have had a very difficult or almost impossible time at getting at the funds.

Regardless of the organization type, continuity of operations and accurate functioning of information systems are vital to all businesses. Threats to information systems and processes are threats to business quality and effectiveness. The objective of information security is to put measures in place which eliminate or reduce significant threats to an acceptable level.

This paper will outline the importance of protecting data, identify the potential risks, and include a brief introduction to a highly recognized information security program. Lastly this paper will provide an easy-to-follow guide on how to implement an information security awareness program including sample templates and reusable information to be adopted in any organization.

Implementing an Information Security Awareness (ISA) Program is not as complicated as one may seem to believe. With a simple structure and careful planning, the ISA program can save immeasurable costs.

I. Confidentiality, Integrity, Availability (CIA)

CIA in the Information Security world is an acronym for Confidentiality, Integrity, and Availability. A key aspect of Information Security is to preserve the confidentiality, integrity and availability of an organization's information.

Confidentiality is the concept of keeping private information private. It is accomplished by restricting access to the information where it is stored. Donors will expect the privacy of their information such as their addresses, phone numbers and credit card numbers.

Integrity is the notion of data consistency: the data is as it should be.

Availability is the idea of having the right data accessible to the right people at the right time, and in the right place.

Protection of Information Assets

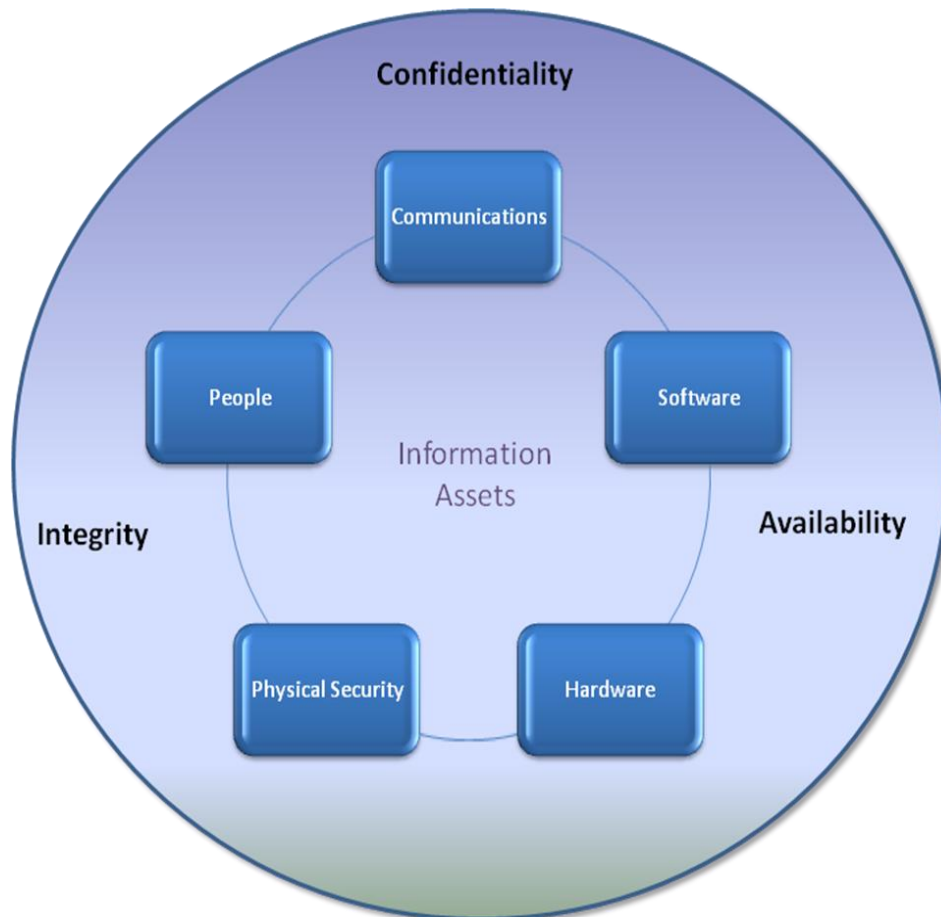


Figure 1 – CIA

Figure 1 is a graphical representation of the CIA model. Each part offers some level of protection, but the combination of them will give an organization a high level of CIA.

The components identified in this graphic include:

Communications The organization's policies and procedures.

People Equip employees with the knowledge of how to protect information

Hardware: Implementing good firewalls and network security protocols

Software: Installing software to protect data such as, up to date virus protection

Physical security: Ensuring hardware i.e., computers, laptops, and mobile devices are protected by lock and key, passwords, etc.

II. Risks

Below is a list of some of the risks that may be incurred in the event of a security breach or fraud.

Financial Loss

Cash or other assets or materials that are stolen or obtained illegally can all be assigned a dollar value to define or assess the total financial value of any asset, cash or equivalent value. Actual frauds that have been perpetrated around the world have reached loss amounts from hundreds to millions of dollars.

Cost of Investigative Process

Every breach or attempted breach should be reviewed, analyzed and fully investigated to help in estimating or determining the “who, what, where, when, how” of the breach and its extent. At a minimum, an organization must be able to determine the dollar amount of the loss, the activities that were undertaken to carry out the breach, and who was involved in assisting in and the carrying out of the actual breach.

Loss of Reputation

The loss of public trust and loss or deterioration of the majority of a non-profit organization’s public reputation will be the outcome the majority of the time. Non-profit organizations that suffer any type of security breach or fraud will suffer a decrease in the public’s confidence that the organization has strong management which can also undermine the organizations overall credibility.

Fractured or Weakened Relationships

Previous organizational relationships that had been developed with grantors, employees, other non-profits and other governments will be questioned and reevaluated.

Employee Defections

Serious and high visibility frauds, especially when committed by a member of the senior management team can cause such a decrease in employee trust, personal and organizational pride that ultimately cause current employees to look outside the organization for advancement or employment.

Donor Disenchantment and Loss

Organizations that have serious frauds committed against them may be excluded from consideration from all types of members of the donor community.

Litigation

Most often, organizations hide security breaches so as to not tarnish their reputations. However, if a non-profit decides to pursue legal actions, the cost to go to court can be considerably expensive.

Damaged Morale

In my experience working for a non-profit, most employees are extremely dedicated to the mission and work tirelessly for the mission. In the wake of an incident, employees will most likely question management and may not perform at the same level they used to work.

Given the risks outlined above, how does an organization plan a strategy to protect its data? The National Security Agency (NSA) addresses those issues in its plan named "Defense in Depth." It is defined as an Information Assurance (IA) strategy in which multiple layers of defense are placed throughout an Information Technology (IT) system. It addresses security vulnerabilities in personnel, technology and operations for the duration of the system's lifecycle [3].

III. Defense in Depth

There are many layers to an information security program. Below are twelve items outlined by the ISO (International Organization for Standardization), the world's largest developer and publisher of international standards [4]. The ISO has listed these factors as part of its latest standard (ISO/IEC 27002:2005), appropriately named "Security techniques – Code of practice for information security management." It is important to point out that not all organizations can implement a complete information security program quickly, easily and with minimal cost. Implementing a strong, cohesive program by using the recommendations listed below can cost thousands of dollars and man hours. Nevertheless, it is essential for organizations to assess their own security and work to improve it.

A. Risk Assessment

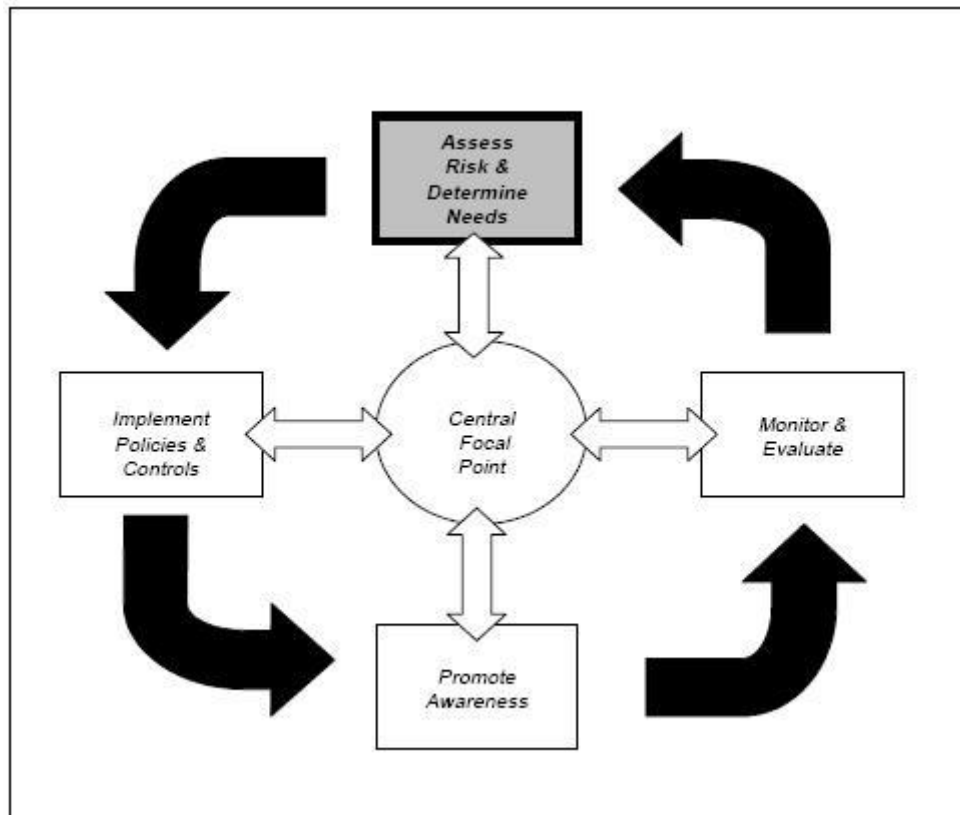


Figure 2 - Risk Management Cycle [6]

Per the GAO: “Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk.” [5]

B. Security policy

Creating security policies sounds like a daunting task; however, a security policy simply defines an organization’s business rules for protecting its data. Policy documents can vary in size. For instance, a password policy document can be as short as one page, whereas an acceptable use policy can span over several pages. Although non-profit’s rarely have IT staff, there are many resources available on the Internet to assist in this process. See the appendices in this paper for example templates.

C. Organizational Security

Information security is not just for the IT department to be concerned about. It relates to managing a business and the challenge of governing information security policies and

enforcing adequate risk management, reporting and accountability. As stated earlier, without IT staff, much can be accomplished with help from free resources.

D. Asset Management - inventory and classification of information assets

How can an organization protect data if they don't know what they have? All information resources belonging to a non-profit organization should be identified, inventoried, and labeled for critical and/or sensitive information elements. A good exercise is to go through a Business Impact Analysis. The process is comprised of five phases: Project initiation, collection of information, information analysis, documentation, and reporting. The process will help identify the critical applications and the corresponding business owners.

Links to BIA instruction and checklists are included in the appendices at the end of this paper. Also note the BIA analysis is the foundation step for item number 11 – Business Continuity (below).

E. Human Resources Security

It is extremely important to have effective policies and procedures for different types of employees, such as new, terminated, and transfer employees, vendors, temporary employees and contract employees. Ensure only the appropriate people have the correct access and remove access when necessary.

A procedure should be in place for all staff managers to understand and follow. It should include the following items:

1. Notify the appropriate Technology department personnel as soon as a hire, transfer, and departure date is known so appropriate security measures can be taken. The notification must include the date and time when all of the employee's accounts (network, e-mail, voice, PDA/Blackberry, etc.) will need to be activated/deactivated. If an employee is being involuntarily terminated, deactivation should take place while the employee is being notified of his or her termination.
2. List in advance all equipment and files in the employee's possession that must be returned.
3. Have all work-related computer files, including existing emails transferred to a temporary location for secure review by the departing employee's successor or supervisor.
4. Arrange for the departing employee's e-mail and phone calls to be temporarily forwarded to the employee's supervisor.

F. Physical and Environmental Security

Protecting data from unauthorized access requires locks, storage facilities, etc. However it is equally important for the hardware to be protected of environmental issues as well, such as floods, fires, etc.

Physical security involves restricting physical access to the computer hardware. This is achieved usually by limiting access to the buildings, areas and rooms where the hardware is housed.

All servers should be protected by lock and key. Servers should be put in a private room, with card/key access. Also, for extra measures servers can be placed in server cages, as shown in Figure 3 below.



Figure 3 – Server Security Cages

(Courtesy of <http://www.cisco-eagle.com/>)

Large IT shops are rare in the non-profit arena, however, the points mentioned in this section should be reviewed when selecting outside vendors that house the data.

G. Communications and Operations Management

Network Operations management is critical for any organization. The items listed below are a great starting point to review internally or with the outside vendor.

1. **Documented Operating Procedures** - All documentation should be complete and available to appropriate users. It is important to include items such as system start ups, backups and maintenance.
2. **System Change Management** - Changes to information systems, using the appropriate planning and testing of changes, authorization, advance communication of changes, and detailed documentation.

3. **Segregation of Duties** - Duties should be segregated to the degree possible in an effort to reduce opportunities for unauthorized changes.
4. **Separation of Development, Test and Production** - Development, test and production environments should be separated to reduce the risk of unauthorized access or changes to the production environment.
5. **Capacity Management** - Information on facility resources should be monitored, and projections made of future capacity requirements to ensure adequate systems performance.
6. **Information Backup** – Backup copies of information and software should be made, and tested at appropriate intervals
7. **Network Controls** - Networks should be managed and controlled, to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
8. **Security of Network Services** - Security features, service levels and management requirements for all network services should be identified in detail, and included in a network services agreement. This includes services are provided in-house or outsourced.

H. Access Control

An organization should ensure that employees have the appropriate access to data, networks, programs and applications, and enterprise-wide systems.

Regular review of network folders and applications are necessary to ensure the right employees have access. The internal or external IT system administrator should conduct quarterly review of access. Typical procedures might include the following:

1. IT Administrator runs user access report to display all users and corresponding access to network directories/folders.
2. IT Administrator sends list of users and corresponding access levels to staff managers.
3. Managers of the various business lines review their staff and corresponding access levels, if any changes are necessary; managers are to specify those changes on the list, sign and return to IT Administrator.
4. IT Administrator receives signed approvals and implements any requested changes.
5. IT Administrator sends final list to VP/Technology to review and obtain approval signature.
6. IT Administrator saves all history of user access review electronic or hardcopy for 3 years.

I. Information Systems Acquisition, Development and Maintenance

When building or buying a software application, it is critical the appropriate security is built into the product. Non-profit organizations usually have little budget for Information

Technology, and it is very common for these organizations to take advantage of open source software (free software). However, with open source software there is always a chance for code vulnerabilities. A notable website to review is <http://www.scan.coverity.com/>, launched as a joint venture with support from the U.S. Department of Homeland Security; this site provides source code analysis and utilizes the latest innovations in automated defect detection to uncover some of the most critical types of bugs found in software.

Another software security item to be aware of when selecting software is to ensure the product includes role-based security which assists in unauthorized access.

J. Information Security Incident Management

An organization should document a plan to anticipate and respond appropriately to information security breaches/incidents. Security incident is defined as a computer or network based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources [6].

Incidents can include the following:

- A laptop computer containing private data is lost or stolen.
- An employee abuses the access they have to private data for their job to look at private data not related to their job, for personal or other reasons or simple curiosity.
- A secure room containing server and network hardware that stores private data is left unattended and unlocked.
- An attacker runs an exploit tool to gain access to the organization's server's password file.
- A worm uses open file shares to infect from one to hundreds of desktop and laptop computers within the organization.

A recommended process and procedure to use when responding to incidents can be found in Appendix A.

K. Business Continuity Management

The term "business continuity" refers to an organization's ability to stay in operation in the event of an incident. Incidents can include security breaches, natural disasters, or national disasters including pandemic illnesses. Creating a business continuity plan has become more popular in recent years. It requires careful planning and a dedicated staff. There are many options for organizations to adopt, please refer to the appendices for more information.

L. Compliance

Make certain the organization follows the information security policies, standards, laws and regulations. Most organizations have internal compliance or audit departments; however, as a cost alternative, hire an accounting firm to perform regular audits for governance and compliance review. Due to the fiduciary responsibilities of non-profit board members, it is a common practice to bring in an audit firm to perform the following:

- Review and appraise the soundness, adequacy and application of accounting, financial and other controls to promote effective and efficient internal control at reasonable cost
- Determine the level of compliance with established policies, plans and procedures
- Conduct special analysis

IV. Information Security Awareness

Security awareness is a great investment. Any organization can have an exceptional state-of-the-art hardware and network security protection, and all it takes is one uneducated user to download a virus from the Internet to compromise an organization's system. Each year, news stories about stolen U.S. Government issued laptops create fears about identity theft. As noted by the Washington Post [7], in May 2006, "a laptop and external hard drive was stolen from a VA data analyst's home in Aspen Hill. It contained the names, birth dates and Social Security numbers of millions of current and former service members. The theft was the largest information security breach in government history and raised fears of potential mass identity theft."

Although the laptop was returned, the point is that with all the high security of Federal Government Agencies, they were unable to keep data safe. Regardless of how secure your network may be, it's only as secure as its weakest link.

Implementing a security awareness program is an essential piece of the overall information security program. It is the best way to communicate security information policies, tips, and best practices to the entire organization. However, it is important to note that Information security awareness is not about training; the overall security awareness objective was designed to change behavior [8].

V. Implementing a Security Awareness Program

A successful security awareness program gives details to users on the proper rules of behavior for the use information technology systems and information. The program should be designed to publicize the information security policies and procedures that must be followed. This must come first and be the foundation and starting point for any

penalties in the event of noncompliance. All users should be well-informed of the expectations.

Get buy-in from the top

Having senior management champion the program will set the tone. Employees are acutely aware of the rules followed by senior management. The executive leadership team affect an organization's ethical culture by implementing practices, policies, and procedures and, equally importantly, by following them. Carefully positioning the program sponsorship sends a clear message emphasizing the importance of the information security program.

Assemble a Team

Create a team with the following areas of expertise: Human Resources, Legal, Technology, and key business lines. The HR, Legal, and Technology team members will have a good understanding of the current policies related to information security; however, the team should be a fair representation of each area of the organization. Information Security Awareness needs to be an organizational-wide effort and presented in the same manner. It is everyone's responsibility.

Assess the Environment

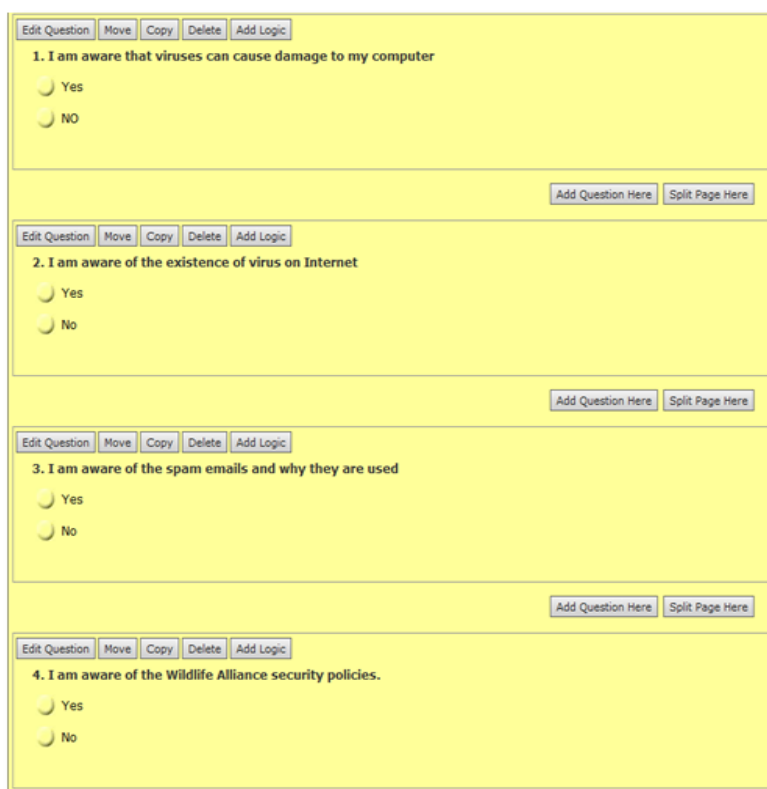
The team should review current policies and procedures. Ensure they are in order and up to date. Assess their strengths and weaknesses. Ensure your policies have a scope, intended audience, a clear instruction, and also include levels of sanctions. For example, first offense, second offense, etc.

Survey Employees

Survey the employees with questions relating to the current policies and procedures. The purpose of this survey is for the project team to assess the level of knowledge the users possess in terms of the policies. The results will determine level of effort the team must perform in an effort to educate the users. Sample questions can be similar to the following:

- Am I aware that viruses can cause damage to my computer?
- Am I aware of the existence of viruses on the Internet?
- Am I aware of spam e-mails and why they are used?
- Am I aware of the current security policies?

Using an online free survey tool called Survey Monkey will save costs. The tool is easy to use and can be found at <http://www.surveymonkey.com/> . The sample survey shown in Figure 3 took less than five minutes to create, but the data it can provide the organization could be invaluable.



The image shows a screenshot of a Survey Monkey survey interface. It consists of four vertically stacked question blocks, each with a yellow background. Each block contains a question, two radio button options (Yes and No), and a set of control buttons (Edit Question, Move, Copy, Delete, Add Logic) at the top. Additionally, each block has 'Add Question Here' and 'Split Page Here' buttons at the bottom right.

1. I am aware that viruses can cause damage to my computer

Yes

NO

Add Question Here Split Page Here

2. I am aware of the existence of virus on Internet

Yes

No

Add Question Here Split Page Here

3. I am aware of the spam emails and why they are used

Yes

No

Add Question Here Split Page Here

4. I am aware of the Wildlife Alliance security policies.

Yes

No

Figure 4 – Sample Survey

Educate the User

Training Sessions

Educating users begins with a kickoff training session. The session should be at least two hours. **An agenda for the training session might** look like the following:

Discussion of the Information Security Awareness Program

- Organization commitment to Information Security
- Discuss Recent Survey Results
- Review the Information Security Awareness Policy
- Ongoing Awareness Campaign

Review current policies and procedures

- E-Mail

- Acceptable Use
- Password
- Code of Conduct

Q & A

Current Policies

The following is a list of four example policies that can be used to implement a Security Awareness Program:

1. E-mail Use Policy

The purpose is to protect the public image of the organization. The scope of the policy is to cover appropriate use of any e-mail sent from the organization e-mail address and applies to all employees, vendors, and agents operating on behalf of the organization.

2. Acceptable Use Policy

The purpose of the policy is to outline the acceptable use of computer equipment of the organization. These rules are in place to protect the employee and organization. Inappropriate use exposes the organization to risks including virus attacks, compromise of network systems and services, and legal liability.

The scope of this policy applies to employees, contractors, consultants, temporary workers, and other workers of the organizations, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the organization.

3. Password Policy

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

The scope of this policy is to include 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 the organization, has access to the organization network, or stores any non-public organization information.

4. Code of Conduct Policy

This policy provides guidance to officers, management, employees, volunteers and staff members having administrative responsibilities as to the organization's underlying ethical philosophy and the standards of conduct expected throughout the organization and its member organization. This code of conduct will help to protect the assets of the organization and the individuals associated with the organization and will also facilitate the protection of the organization's tax-exempt status, its public reputation, and guard against actions that would result in criminal prosecution and/or civil litigation. For

instance, a section of the Code of Conduct policy may include specific details for the method by which donations are processed. If the organization finds out an internal employee mishandled donations and embezzled money, the organization may take legal action against that individual.

Certificate of Completion

Issue a certificate of completion for each attendee. These can be easily created using a template, such as the one shown in Figure 5 below.

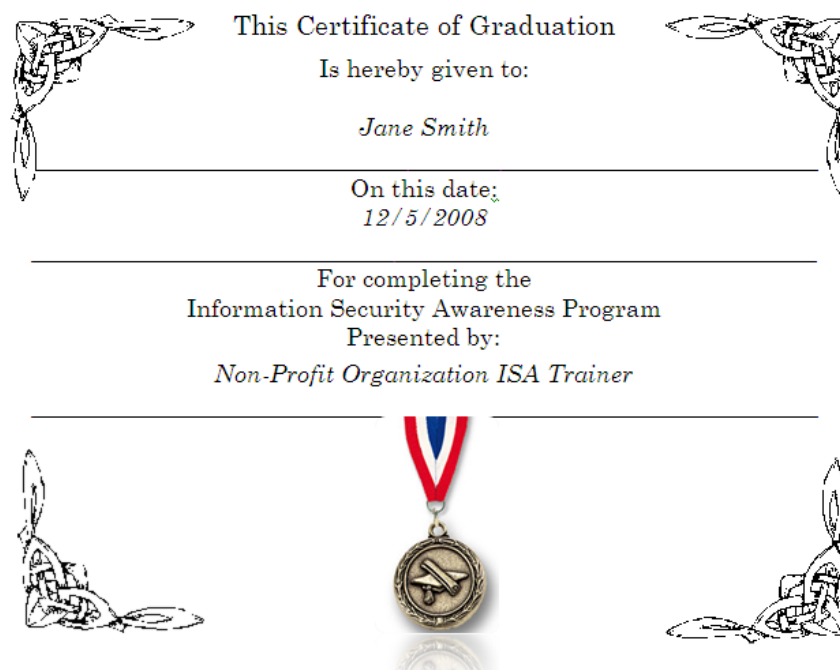


Figure 5 - Sample Security Awareness Certificate

On-going Monthly Awareness Campaigns

A one-time training session is not enough to promote security awareness. Constant reminders will continue throughout the campaign.

To remind personnel of the importance and practice of information security, place posters on the bulletin boards, elevators, and high traffic areas. A good source for such posters is: <http://www.ussecurityawareness.org/highres/security-awareness.html>, which offers free and timely security-related posters. An example of a poster is shown in Figure 6 below.



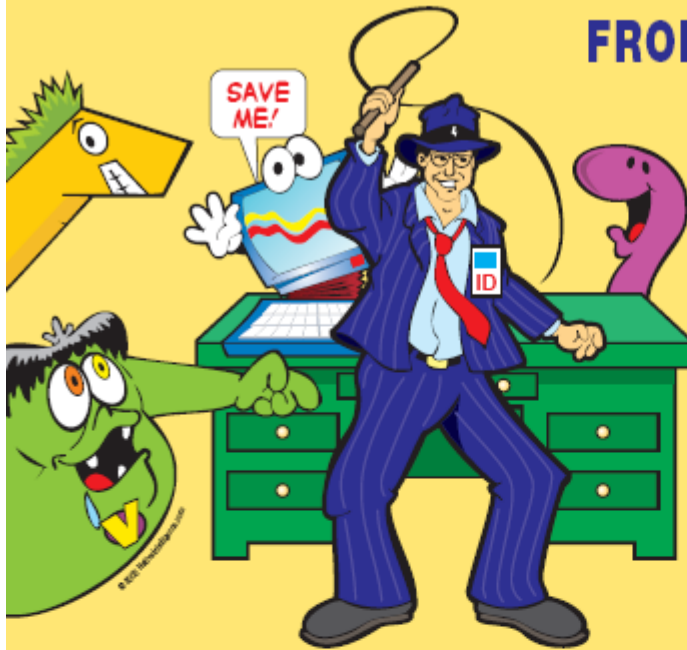
Figure 6 – Sample Security Awareness Posters

Additional monthly newsletters, annual calendars with security awareness tips also prove beneficial. See figures 7 and 8 below for ideas.

Date	September 1, 2008
To:	All employees
From:	Information Security Awareness Team
Subject:	Monthly Newsletter: Traveling with your laptop
	<ul style="list-style-type: none"> • Never leave your laptop unattended. This may seem basic, but unattended also includes the trunk of your car, your hotel room, others' offices or in your luggage. • Encrypt stored files. Software can do this for you. Ask a member of your company's information security staff for advice. • Beware of shoulder surfers. When people peer over your shoulder in the airport, they may be trying to see the sports scores that you have scrolling on streaming video, but they may also be trying to steal the data off your confidential company earnings report. Use a polarizing screen cover. Better yet, use your laptop in a more private location. • Change passwords often. It's hard to remember them all, let alone change them. But it only takes a minute, and it's effective. • Before your laptop is stolen, take preventive measures by adding tracking software. Visit these sites for information: www.sentryinc.com and www.computrace.com. • Finally, if your laptop is stolen, report it to the local police.

Figure 7 – Sample Monthly Newsletter

YOU CAN STOP MALICIOUS SOFTWARE FROM SPREADING...



**DON'T
OPEN
ATTACHMENTS
THAT YOU
ARE NOT
EXPECTING.**

2009

JANUARY							FEBRUARY							MARCH							APRIL						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
				1	2	3	1	2	3	4	5	6	7	1	2	3	4	5	6	7				1	2	3	4
4	5	6	7	8	9	10	8	9	10	11	12	13	14	8	9	10	11	12	13	14	5	6	7	8	9	10	11
11	12	13	14	15	16	17	15	16	17	18	19	20	21	15	16	17	18	19	20	21	12	13	14	15	16	17	18
18	19	20	21	22	23	24	22	23	24	25	26	27	28	22	23	24	25	26	27	28	19	20	21	22	23	24	25
25	26	27	28	29	30	31								29	30	31					26	27	28	29	30		
MAY							JUNE							JULY							AUGUST						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
				1	2		1	2	3	4	5	6				1	2	3	4								1
3	4	5	6	7	8	9	7	8	9	10	11	12	13	5	6	7	8	9	10	11	2	3	4	5	6	7	8
10	11	12	13	14	15	16	14	15	16	17	18	19	20	12	13	14	15	16	17	18	9	10	11	12	13	14	15
17	18	19	20	21	22	23	21	22	23	24	25	26	27	19	20	21	22	23	24	25	16	17	18	19	20	21	22
24	25	26	27	28	29	30	28	29	30					26	27	28	29	30	31	23	24	25	26	27	28	29	
31																					30	31					
SEPTEMBER							OCTOBER							NOVEMBER							DECEMBER						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
		1	2	3	4	5			1	2	3		1	2	3	4	5	6	7			1	2	3	4	5	
6	7	8	9	10	11	12	4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12
13	14	15	16	17	18	19	11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19
20	21	22	23	24	25	26	18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26
27	28	29	30				25	26	27	28	29	30	31	29	30	31					27	28	29	30	31		
COMPUTER SECURITY DAY — NOVEMBER 30																											

<http://www.nativeintelligence.com/ni-free/NI-CSD-Cal-2009.pdf>

Figure 8 - Security Awareness Calendar

Conclusion

As this paper provided evidence that while possessing the finest hardware, software, and other security controls in an IT environment, it is still possible for any organization to be subjected to a security breach. I believe that an organization's best security defense is to implement and continue to support an information security awareness program. A program which consists of surveying your audience, holding training sessions to educate your users, and finally, using ongoing awareness using tools such as monthly newsletters, posters, calendars, etc.

It is important to note the difference in attitude between the non-profit and for-profit organizations as it relates to information security in general. The key distinction is their lackadaisical opinion. Non-profit organizations are notorious for being a very trusting society, as they perceive general information security as preventing an attack from a really bad person trying to break into their systems. It is common for them to have the mindset their systems will always be safe because no one would want to hurt a 'do-good' organization. Unfortunately their own employees can be end up being the honest or dishonest offender. Therefore, continuous security awareness is a necessary approach to educate and change behavior.

Appendix A - Sample Policies

This appendix provides several examples of documents developed by the SANS Institute (www.sans.org). The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs reach over 165,000 security professionals around the world. SANS is exceptionally well known in the Information Security field. Sans also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security. These sample policies have been included and may be freely adopted in any organization.

Acceptable Use Policy

1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. InfoSec is committed to protecting <Company 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, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company 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 <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

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

4.0 Policy

4.1 General Use and Ownership

1. While <Company Name>'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 <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company 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 be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.
5. <Company Name> reserves the right to audit networks 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 not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. 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. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company

Name>, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

8. 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.

4.3. Unacceptable Use

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

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. 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.
15. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging

1. Blogging by employees, whether using <Company Name>'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>'s systems is also subject to monitoring.
2. <Company Name>'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>'s Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

5.0 Enforcement

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

6.0 Definitions

Term	Definition
-------------	-------------------

<i> Blogging </i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
-------------------	--

<i> Spam </i>	Unauthorized and/or unsolicited electronic mass mailings.
---------------	---

7.0 Revision History

Appendix B – Password Policy

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 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.

3.0 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 <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All 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 six months. The recommended change interval is every four 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 forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at <Company Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router 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, weak passwords have the following characteristics:

- The password contains less than fifteen 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, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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).
- Are 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 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.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.).

Where possible, don't use the same password for various <Company Name> access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "dont's":

- 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.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.

- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

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

6.0 Definitions

Terms

Application Administration Account

Definitions

Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Appendix C – Email Use Policy

<COMPANY NAME> Email Use Policy

1.0 Purpose

To prevent tarnishing the public image of <COMPANY NAME> when email goes out from <COMPANY NAME> the general public will tend to view that message as an official policy statement from the <COMPANY NAME>.

2.0 Scope

This policy covers appropriate use of any email sent from a <COMPANY NAME> email address and applies to all employees, vendors, and agents operating on behalf of <COMPANY NAME>.

3.0 Policy

3.1 Prohibited Use. The <COMPANY NAME> email system shall not to 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 from any <COMPANY NAME> employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of <COMPANY NAME> 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 <COMPANY NAME> email account is prohibited. Virus or other malware warnings and mass mailings from <COMPANY NAME> shall be approved by <COMPANY NAME> VP Operations before sending. These restrictions also apply to the forwarding of mail received by a <COMPANY NAME> employee.

3.3 Monitoring

<COMPANY NAME> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. <COMPANY NAME> may monitor messages without prior notice. <COMPANY NAME> is not obliged to monitor email messages.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
------	------------

Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to <COMPANY NAME> or its customers' reputation or market standing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside <COMPANY NAME>, who do not have a need to know that information.

6.0 Revision History

Appendix D - Free Resources:

Information Security Awareness Posters

<http://www.ussecurityawareness.org/highres/security-awareness.html>

<http://www.iwar.org.uk/comsec/resources/ia-awareness-posters/index.htm>

Information Security Policies

Developed by a group of experienced security professionals with more than 80 years of combined experience in government and commercial organizations, and each policy went through a vigorous approval process.

<http://www.sans.org/resources/policies/?ref=3731#template>

Security Awareness Toolbox

<http://www.iwar.org.uk/comsec/resources/sa-tools/>

Security Awareness Yahoo Group

<http://tech.groups.yahoo.com/group/security-awareness/>

IT Governance Institute –

“ITGI is a research think tank that exists to be the leading reference on IT governance for the global business community. ITGI aims to benefit enterprises by assisting enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. By conducting original research on IT governance and related topics, ITGI helps enterprise leaders understand and have the tools to ensure effective governance over IT within their enterprise.”

[http://www.itgi.org/template_ITGI.cfm?Section=Security, Control and Assurance&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=60&ContentID=10609](http://www.itgi.org/template_ITGI.cfm?Section=Security,_Control_and_Assurance&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=60&ContentID=10609)

Security Awareness Monthly Newsletter

<http://www.noticebored.com/html/nbnewsletter.html>

National Institute of Standards and Technology (NIST) - Building an Information Technology Security Awareness and Training Program

<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

Business Impact Analysis

http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bcp_14.html

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci880054,00.html

<http://web.arizona.edu/~ccit/fileadmin/templates/content/security/pdf/BIAChecklist.pdf>

Responding to IT Security Incidents

<http://technet.microsoft.com/en-us/library/cc700825.aspx>

Works Cited:

- [1] The Chronicle of Philanthropy. May 17, 2004. Retrieved November 10, 2008
<http://philanthropy.com/free/update/2004/05/2004051701.htm>
- [2] Wikipedia. January 15, 2008. Wikimedia Foundation, Inc. Retrieved, October 25, 2008
http://en.wikipedia.org/wiki/Image:Information_security_components_JMK.png
- [3] National Security Agency. Retrieved October 25, 2008
<http://www.nsa.gov/snac/support/defenseindepth.pdf>
- [4] International Organization for Standardization. Retrieved October 26, 2008
<http://www.iso.org/iso/about.htm>
- [5] GAO – The United States Government Accountability Office, November, 1999. Retrieved October 22, 2008
<http://www.gao.gov/special.pubs/ai00033.pdf>
- [6] University of Minnesota – Office of Information Technology, September 17, 2007. Retrieved December 1, 2008
http://www1.umn.edu/oit/security/incident/OIT_12654_REGION1.html
- [7] Washington Post. June 30, 2006. Retrieved November 1, 2008
<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/29/AR2006062900352.html>
- [8] The National Institute of Standards and Technology (NIST), October, 2003. Retrieved October 26, 2008
<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>