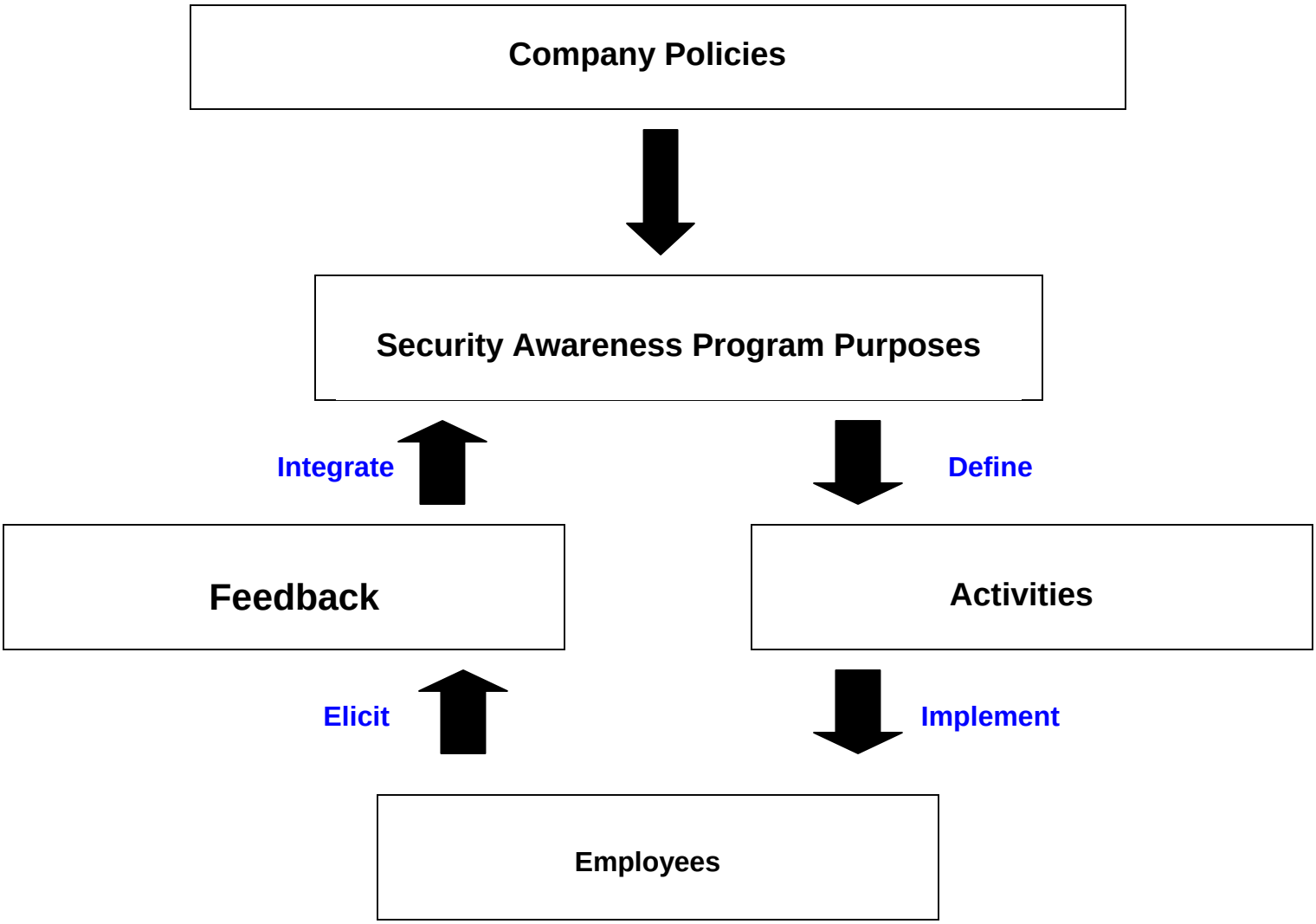
(Company Name)
SECURITY AWARENESS PROGRAM

INFORMATION, PHYSICAL AND PERSONAL SECURITY



Model 1 - The Security Awareness Program Flow

Whether it's checking e-mail, answering a telephone, or logging off for the day, employees must be encouraged to think security into every action they take and every decision they make. Only when security becomes second nature will it become truly effective.

Activities have been developed that meet the purposes of the Security Awareness Program (i.e., heighten your awareness, develop your skills and remind you of Company policies and procedures). Because the awareness program is dynamic and designed to evolve in order to meet the future needs of the Company and employees, and to address the issues that arise due to rapidly advancing information technology, current activities will be modified or new activities will be developed to maintain program relevancy
Employees are more likely to forget or ignore advice that has no relevance to their job, and "one lesson for all" just doesn't work. It's therefore important that employees make the connection between the lessons taught and the task at hand. For example, employees involved in accounting or transaction processing in a business that takes on-line credit card orders are far more likely to remember security lessons focused on protecting credit card files and personal customer information and on privacy issues.
That important security information might not seem so important or relevant to a telephonist, receptionist, or delivery driver, who are more likely to meet or speak with an intruder and be much more susceptible to social engineering.

The Security Awareness Handbook describes the Security Awareness program, documents the security procedures and provides security resources. You will be provided with a handbook at your initial Security awareness briefing. The Security Awareness handbook is designed to be a "living" handbook and it will change as the program evolves.

For further information or future updates to this training handbook, please check the Security Awareness web page on the intranet.

Security Alerts

Security Alerts will be issued periodically to serve as early warnings of threats and vulnerabilities to Company resources. Procedures for these alerts are still being developed. All employee communications resources will be used to announce security preventative measures, changing security issues and requirements, and enhancements to the Security Awareness program. The announcements will provide high-level information and then direct you to where you can obtain additional information from your desktop.

Security Alerts serve as early warnings of threats and vulnerabilities to Company resources.

Security Sense

The **Security Sense** is a monthly mass e-mail that contains relevant tips on security issues. Some articles that will be addressed include, but are not limited to, Viruses and Worms, Guest Procedures, Password Reminder, E-mail Etiquette, Trusted Sources of Info, Safe Web Browsing, Laptop Theft, Photo-ID Badges, Workstation Security, etc.

Lunch and Learn

The Security Department holds ongoing **'Lunch & Learn'** sessions periodically. The purpose is to have an informal get-together during lunch hour and cover a variety of security-oriented issues. These sessions will be on new Security Policies and Procedures, Operating System security, Intrusion Detection, Viruses, and a host of other issues.

Security Presentations/CBT Course

The Security Presentations are 30 to 45 minute mini-briefing and training sessions that have been designed to increase your security skills and knowledge. The presentations are compact enough to facilitate the time constraints of department or group meetings and yet rich enough to provide meaningful information.

The Security Awareness CBT is a 5 Sessions training course with illustrations, activities, examples, how to instructions, and case studies. Sessions address general topics, such as: Social Engineering, Office Security, Identity Theft, Facility and After Hour Access, Employee Identification, Visitor Control, PC Security, Telephone Fraud, Software Piracy, Data Backups,

Laptop Security, Proper/Improper Internet Use, Security Basics, Palm Pilots / PDAs / Cell Phones, Disaster Recovery, Incident Reporting, Passwords, Password Protected Screensavers, Data Classification Guidelines, Internet Security, E-mail Usage, Viruses, Physical Security, Personnel Security, Information Operations Fundamentals, Network and Information Sharing, Incident Handling, Risk Assessment, Data Classification. Test scores are tracked and retained.

Contact the Security Awareness program Coordinator by email or at extension (_____) to schedule a security presentation.

The security presentations are described below:

New Hire Orientation
(COMPANY NAME) maintains a highly visible Security environment that provides for the safety of the Company and our employees. However, no one can be totally risk free in today's society. To lessen the chances of security incidents occurring, everyone's cooperation and vigilance is needed. All members of the (COMPANY NAME) community (employees, contractors, venders and other business partners) are encouraged to immediately report all suspected crimes, unusual or suspicious activities, and emergencies to the Security Department. The purpose of this presentation is to provide new hires and other (COMPANY NAME) business partners' basic security information that prepares them to protection of resources, detection of security breaches and reaction to a potential or actual security incident. The following elements of our security awareness program will be covered:
1.What is Information Security?
2.What Information Needs to be Protected?
3.How Information Security Affects You
4.Viruses
5.Be on Your Guard
6.Passwords
7.Software and Copyright Law
8. Incident Reponse
9.Information Security Policies
The case for action for the new hire orientation is designed with to prevent common consequences, such as:
The inability of both you and other employees to perform assigned responsibilities and provide needed services.
The waste, loss, or abuse of company resources.
The loss of credibility or embarrassment to the company.

Comprehensive Security Awareness
The purpose of this presentation is to introduce participants opportunity to physical, personal and information threats and countermeasures.

Password Construction and Management
The purpose of this presentation is to help you understand the requirements for utilizing passwords when accessing Company information resources and to assist you in creating and maintaining secure passwords

Social engineering
Employees must be able to spot the warning signs of social engineering -- when an intruder poses as a legitimate party like a customer, network administrator, or vendor representative and attempts to bluff sensitive information from an employee. Just as an antivirus product scans incoming files for suspect virus signatures based on its library of definitions, employees must have a library of warnings to detect the telltale signature of the social engineer.

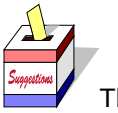
Introduction to Safe Computing Practices
The purpose of this presentation is to help you become familiar with some of the practices that will help to ensure the safe and proper utilization of Company computing resources.

Safeguarding Company Resources
The purpose of this presentation is to help you understand the requirements for accessing Company resources and the way in which they are accessed. It also presents additional information related to your responsibilities in the area of document security.

Feedback Elements

Feedback Elements have been created to maintain the security awareness program by ensuring that the awareness activities remain both timely and relevant to meet both the security needs of the Company and individual employees. In addition, you are more likely to support the program if you actively participate in its development. Your feedback will help identify gaps in the Security Awareness program and the Company's security needs. Your feedback will also be used in the evaluation of overall program quality and effectiveness.

Security Awareness Program Suggestion Form



The **Security Awareness Suggestion Form** allows you to participate in the ongoing design and maintenance of the Security Awareness Program. Suggestions regarding either additions or changes to the program are welcome. You are also encouraged to make suggestions for topics for current program activities. Special recognition is given to employees who make suggestions that are implemented. To submit a suggestion:

1. Make a copy of the form found at the end of this document.
2. Fill out the form.
3. Submit form to the Security Awareness program Coordinator at mail stop ____.

Awareness Presentation Evaluation Form

The **Security Awareness Presentation Evaluation** form measures the effectiveness of the Security Awareness presentation and solicits your suggestions for additional security presentation topics. Evaluation forms are distributed at the beginning of each security presentation and collected at the conclusion of the presentation. A sample evaluation is included at the end of this document.

Suspicious or Unusual Event Report

Employees are asked to report suspicious or unusual events. Events may include (but are not limited to) unauthorized access of the network (from both internal and external sources), compromise of sensitive data, destroying hardware or software, and malicious code such as viruses, worms, Trojan horses, or any other uninvited software. Immediate reporting events will help mitigate any adverse impact and minimize current and future vulnerability. You should report those events that even seem trivial.

To report an event immediately, contact the security Department at ext. (_____). Department personnel will document the report on a **Suspicious or Unusual Events Form**. A sample form is included at the end of this document.

When you first notice a suspicious or unusual event, use a copy of the sample form to collect all relevant and important details.

Suspicious or Unusual Event Report

This form is completed when an employee reports a suspicious or unusual event related to (COMPANY) resources. Events may include (but are not limited to) unauthorized access of the network (from both internal and external sources), compromise of sensitive data, destroying hardware or software, and malicious code such as viruses, worms, Trojan horses, or any other uninvited software.

Information Provided by the Security Department

Report Number: _____

Date: _____

Call received by (Name): _____

Information Collected From Reporting Employee

Collect ALL Information on this section of the form.

Employee Name*:* _____

Employee phone Number: _____

Employee email: _____

Employee mail stop: _____

Description of the Problem:
(e.g., Received an email from Joe Friendly with an attachment (happy99.exe) Now computer doesn't work right. Etc.)

Name of Computer
_____
(Include information on how to locate the name of the computer)

Physical location of computer: _____

Type of computer: _____

Applications that were running at the time:

Names of other employees who were involved in or witnessed the event:

Security Awareness Program Suggestion Form

Please fill out and submit this form with your program and suggestion to the Security Awareness Program Coordinator at mailstop _____.

Name(s):

Phone Number(s):

E-mail:

Mail Stop:

Describe your suggestion:

In what way(s) will this improve the Security Awareness program?

Thank you for your suggestions!