January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Purpose of the Security Awareness and Training Plan 3](#_Toc335914342)

[II. Overview of the Security Awareness and Training Plan 3](#_Toc335914343)

[III. Security Awareness and Training Lifecycle 4](#_Toc335914344)

[IV. Designing the Security Awareness and Training Program 5](#_Toc335914345)

[V. Developing Material for the Security Awareness and Training Program 8](#_Toc335914346)

[VI. Implementing a Security Awareness and Training Program 10](#_Toc335914347)

[VII. Security Awareness and Training Program Post-Implementation 11](#_Toc335914348)

[Appendix A – Distribution List 12](#_Toc335914349)

[Appendix B – Receipt and Acknowledgement 13](#_Toc335914350)

# I. Purpose of the Security Awareness and Training Plan

ABC Company understands that "people", not technology vulnerabilities, can be the biggest threat to our Information Resources. The purpose of this Security Awareness and Training Plan (Plan) is to ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.

# II. Overview of the Security Awareness and Training Plan

A strong security program requires Staff to be trained on security policies, procedures, and technical security controls. ABC Company Staff who manage Information Resources need to have the necessary skills to carry out their assigned duties.

The Chief Security Officer (CSO) is responsible for developing, implementing, and maintaining this Plan. This Plan documents the process for Staff security training, education, and awareness and ensures that ABC Company Staff understands its role in protecting the confidentiality, integrity, and availability of Information Resources.

This Plan ensures that Staff is provided with regular training, reference materials, and reminders to enable them to appropriately protect ABC Company’s Information Resources. Training shall include, but is not limited to:

* ABC Company’s responsibilities for protecting Information Resources.
* Risks to Information Resources.
* The secure use of Information Resources.
* Information security policies, procedures, and best practices.

This Plan ensures:

* All new users attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any IT resources.
* Staff receives training appropriate for specific job roles and responsibilities. After training, each Staff member verifies that he or she received the training, understood the material presented, and agrees to comply with it.
* Staff is trained on the importance of enabling and utilizing secure authentication.
* Staff is trained on how to identify, report, and prevent security incidents as well as the most common indicators of an incident.
* Staff is aware of causes for unintentional data exposures, such as losing their mobile devices or e-mailing the wrong person due to autocomplete in e-mail.
* Staff is trained on how to identify and properly store, transfer, archive, and destroy sensitive information.
* Security policies, procedures, and manuals are readily available for reference and review by the appropriate Staff.
* Staff attends annual security awareness training sessions.

# III. Security Awareness and Training Lifecycle

ABC Company cannot protect the confidentiality, integrity, and availability of information without ensuring that all Staff involved in using and managing Information Resources:

* Understand their roles and responsibilities.
* Understand ABC Company’s security policies and procedures.
* Have at least adequate knowledge of the various administrative, physical, and technical controls to protect the Information Resources for which they are responsible.

The CSO ensures that ABC Company Staff understands the concepts and strategy of the organization’s security awareness and training program. Security begins with awareness, builds to training, and evolves into education.

* *Awareness*. Security awareness efforts change behavior or reinforce good security practices. Awareness is not training. The purpose of awareness is to focus attention on security. Awareness presentations help individuals identify security issues and the proper response to security threats.
* *Training*. While security awareness relies on reaching broad audiences with attractive presentations, training tends to be more formal, with a goal of building knowledge and skills that enhance the effectiveness of security controls. Training strives to produce relevant and needed security skills and competencies by ABC Company Staff.
* *Education*. Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adding concepts, issues, and principles to produce security specialists and professionals capable of pro-active response to threats.

ABC Company’s security awareness and training program lifecycle consists of the following elements:

1. Designing the Security Awareness and Training Program – an assessment is conducted and a training strategy is developed and approved. This strategic planning process identifies implementation tasks to be performed in support of security training goals.
2. Developing Material for the Security Awareness and Training Program – available training resources are identified as is the scope and content of the training material.
3. Implementing the Security Awareness and Training Program – effective communication and roll out of the awareness and training program including options for delivery of awareness and training material (e.g. web-based, distance learning, video, and on-site).
4. Security Awareness and Training Post-Implementation – guidance on keeping the program current and monitoring its effectiveness including the use of feedback methods (e.g surveys, focus groups, and benchmarking).

# IV. Designing the Security Awareness and Training Program

The awareness and training program helps to support the business needs of the organization. The responsibility and budget for ABC Company’s security awareness and training program is developed, managed, and maintained by the CSO. All directives, strategy development, planning, and scheduling is coordinated through this “security awareness and training” authority.

The CSO communicates to ABC Company’s departments the policy directives regarding security awareness and training, the strategy for conducting the program, and the material and methods of implementation. The Department Heads then provide information requested by the CSO.

The CSO collects data on the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. Department Heads provide feedback on the effectiveness of awareness and training material and on the appropriateness of the methods used to implement the material. Department Head feedback allows the CSO to fine-tune, add or delete material, or modify the implementation methods.

On an annual basis, the CSO conducts a needs assessment that reviews and determines ABC Company’s awareness and training needs. The needs assessment supports management’s decision to allocate adequate resources to meet the identified awareness and training requirements and considers various types of Staff:

* Executive Management – management understands directives and laws that form the basis for the security program. They also understand leadership roles to ensure full compliance by users.
* Security Personnel – security program managers and security officers act as expert consultants and are well educated on security policies and security best practices.
* System Owners – system and data owners have an understanding of security policies and a high degree of understanding security controls and requirements applicable to the systems they manage.
* System Administrators – administrators are critical to a successful information security management system and have a higher degree of security technical knowledge and training.
* Operational Managers and System Users – managers and system users have a high degree of security awareness and training on security controls and rules of behavior for systems they use and manage.

Methods to collect information for the needs assessment include:

* Interview or survey of IT department, system and data owners, and key Staff.
* Review and assessment of available resource material (e.g. current awareness and training materials, training schedules, and lists of attendees).
* Analysis of metrics related to awareness and training (e.g., percentage of Staff completing required awareness session or exposure, percentage of Staff who have significant security responsibilities who have been trained in specific material).
* Review of security plans for general support systems and major applications to identify system and application owners and appointed security representatives.
* Review of application user IDs to identify Staff who have access to Information Resources.
* Review of audit findings and/or recommendations related to the security of Information Resources.
* Analysis of events (e.g. denial of service attacks, virus damage, Ransomware, and website defacements).
* Security trends and metrics.

Metrics are an important tool used to help determine the effectiveness of ABC Company’s security awareness and training program. Metrics monitor the program goals and objectives by:

* Quantifying the level of program implementation.
* Identifying the effectiveness and efficiency of the program.
* Analyzing the adequacy of awareness and training efforts
* Identifying possible improvements.

The needs assessment identifies:

* The awareness, training, and/or education needs of the organization.
* Tasks currently performed to address the above needs.
* How the training needs are being addressed and the effectiveness of the training.
* Training “gaps” between the needs of the organization and what is currently being provided.
* A prioritized list of critical needs.

The CSO analyzes the needs assessment and develops an awareness and training strategy. The strategy identifies:

* The personnel responsible for designing, developing, implementing, and maintaining the security awareness and training material.
* The personnel responsible for ensuring that the appropriate Staff attend or view the applicable material.
* The goals to be accomplished for each aspect of the program (e.g., awareness, training, education).
* Target audiences for each aspect of the program. Mandatory and optional courses or material for each target audience.
* Learning objectives for each aspect of the program. Topics to be addressed in each session or course.
* Deployment methods to be used for each aspect of the program.
* Documentation, feedback, and evidence of learning for each aspect of the program.
* Processes to evaluate and update the security awareness and training material.
* The frequency that each target audience should be exposed to material.

Once the security awareness and training strategy has been finalized, the CSO develops a prioritized implementation schedule. Key factors to consider include:

* Availability of materials and resources.
* Role and impact on the organization.
* Current situation and “gaps” from needs assessment.
* Critical project dependencies.

# V. Developing Material for the Security Awareness and Training Program

The secure awareness and training material identifies the behavior to be reinforced (awareness). Since the goal of awareness is to focus attention on good security practices, the message is short and simple. The awareness audience includes all users and makes them aware of commonly shared security responsibilities.

Training material identifies the skills the audience should learn and apply. A typical training class is directed at a specific audience and emphasizes what attendees need to know in order to do their jobs. Training material is usually far more in-depth than material used in awareness sessions.

Security awareness topics include:

* Acceptable use and monitoring of user activity
* Access controls, least privilege, and separation of duties
* Bring your own device and technology (BYODT)
* Change management
* Data backup and storage
* Desktop security (e.g. screen savers, time outs)
* E-mail, spam, and attachments
* Encryption and transmitting sensitive information
* Equipment disposal
* Handheld (mobile) devices
* Incident response contacts
* Laptop security
* Malware, viruses, worms, and Ransomware
* Password usage and management
* Patch management
* Physical access
* Security policies and implications of non-compliance
* Shoulder surfing
* Social engineering attacks including phishing, phone scams and impersonation calls
* Software license restrictions
* Supported software

Security awareness material includes both a single theme (e.g. posters) as well as combining a number of themes or messages into a presentation. Sources of material on security awareness include:

* Conferences, seminars, and courses.
* E-mail advisories issued by industry sources.
* Professional organizations and vendors.
* Security magazines and periodicals.
* Security news websites.

The CSO shall identify Staff members who require special security training:

* Acquire. Staff who acquire Information Resources.
* Administrator. Staff who operate (administer) Information Resources.
* Design and Develop. Staff who program, design, and develop systems and applications.
* Manage. Staff who manage Information Resources.
* Review and Evaluate. Staff who review and evaluate (audit) Information Resources.

The CSO determines if training materials will be developed in-house or through the use of outside services. Key factors considered when determining if the material will be developed in-house vs. outsourced include:

* In-house resources, knowledge, and experience to prepare the material.
* Cost of developing the material vs. packaged materials.
* Course content sensitivity.
* Material delivery schedules.

# VI. Implementing a Security Awareness and Training Program

ABC Company’s security awareness and training program includes a needs assessment and gap analysis, a formal program strategy, a plan to prepare program materials, and a plan to implement the strategy.

Communications with management and Staff is an essential part of implementing the program to ensure active support and commitment of necessary resources. The CSO:

* Documents the expected results of the program, anticipated costs, and benefits to the organization.
* Communicates the program schedule and offerings to the organization’s Department Heads.

Techniques for delivering material include:

* Computer based training
* E-mails
* Flyers
* Instructor led sessions
* Message boards
* Newsletters
* Posters
* Teleconferences
* Videos
* Webinars

Programs take advantage of technology that supports the following features:

* Ease of use and access.
* Scalability for small to large audience sizes and locations.
* Accountability and ability to track attendance and participation.

# VII. Security Awareness and Training Program Post-Implementation

Once the program has been implemented, processes monitor Staff attendance and effectiveness. A tracking system captures key information and program activity (e.g., courses, dates, audience, costs, and training sources). The tracking system captures data by department so that it can be used to provide enterprise wide analysis and reporting regarding awareness, training, and education initiatives.

Compliance tracking maps program activities to standards established by the CSO. Reports are generated and used to identify gaps or problems so that the appropriate corrective action can be taken.

Formal evaluation and feedback mechanisms are critical components of the security awareness, training, and education program. Continuous improvement and feedback processes ensure the program is working as desired.

Feedback mechanisms include:

* Evaluation forms and questionnaires.
* Focus groups.
* Formal status reports.
* Independent observation and analysis.
* Security program benchmarking (external view).
* Selective Interviews.

The CSO and Department Heads are the primary advocates for continuous improvement and support of ABC Company’s security awareness, training, and education program. Listed below are key indicators that gauge the support for, and acceptance of, the program:

* Sufficient funding by ABC Company senior management.
* Support for broad distribution and posting of security awareness items.
* Senior management messages to staff regarding security.
* Use of metrics to identify security trends.
* Managers do not use their position to avoid security controls.
* Required attendance at security awareness and training sessions.
* Recognition of security contributions through awards and contests.

Corrective action is taken and includes formal reminders, additional awareness, training, or education offerings, and external social engineering evaluations by independent auditors.

# Appendix A – Distribution List

President

Chief Operating Officer

IT Director

All Department Heads

# Appendix B – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) Security Awareness and Training Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)