Security Awareness and Training Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

People, not technology vulnerabilities, can be the biggest threat to our Information Resources. Staff must receive security awareness and education training appropriate for their job duties and responsibilities.

# II. Purpose

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 purpose of this Security Awareness and Training Policy is to ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.

# III. Scope

This policy applies to all ABC Company Staff who use Information Resources.

# IV. Policy

ABC Company management must ensure that high priority is given to effective security awareness and training. This includes implementing a viable security program with a strong awareness and training component. ABC Company management shall designate a Chief Security Officer (CSO) responsible for the security of Information Resources. The CSO shall ensure that a well-supported (e.g. resources and budget) and effective security program is implemented and maintained.

ABC Company’s CSO shall be responsible for developing, implementing, and maintaining a Security Awareness and Training Plan (Plan). This Plan shall document the process for Staff security training, education, and awareness and ensure that ABC Company Staff understand their role and responsibility in protecting the confidentiality, integrity, and availability of Information Resources. Communications relevant to the information security management system (ISMS) include what to communicate, when to communicate, with whom to communicate, who shall communicate, and the process by which communication shall be affected. Communications shall be issued in a continuous and engaging manner.

The Plan shall ensure 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
* How to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls
* The secure use of Information Resources
* Information security policies, procedures, and best practices

The Plan shall ensure:

* All new users attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Information Resources.
* Staff receives training appropriate for specific job roles and responsibilities. After such training, each Staff member must verify that he or she received the training, understood the material presented, and agrees to comply with it.
* Staff are trained on how to identify, report, and prevent security incidents. Staff are aware of the most common indicators of an incident.
* Staff understand the importance of enabling and utilizing secure authentication.
* Staff 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 attend annual security awareness training.
* Staff sign an acknowledgement stating they have read and understand ABC Company requirements regarding computer and information security policies and procedures.
* Staff are provided with sufficient training and supporting reference materials to allow them to properly protect Information Resources.
* The IT Department prepares, maintains, and distributes one or more information security manuals that concisely describe information security policies and procedures.
* Cloud computing security awareness training programs address multi-tenant, nationality, and cloud delivery models. Conflicts of interest shall be established for all Staff and Tenants.
* Staff are made aware of the risks and responsibilities related to bring your own device and technologies (BYODT).
* Staff are aware of causes of unintentional data exposures, such as losing their mobile devices or e-mailing the wrong person due to autocomplete in e-mail.

The CSO shall:

* Ensure a skills gap analysis is performed to understand the skills and behaviors Staff are not adhering to and use of this information to build a baseline education roadmap.
* Develop and maintain a communications process to communicate new security program, security bulletin, and security items of interest.
* Ensure that Staff responsible for implementing Information Resources safeguards receives formal training in security best practices.
* Ensure periodic security reminders (flyers or posters, e-mails, verbal updates at meetings) keep Staff up-to-date on new and emerging threats and security best practices. The frequency and method of delivery of such reminders shall be determined by the CSO.

# V. Enforcement

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

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.03, APO02.08, APO07.12-13, APO12.02, APO12.07, APO13.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(D)

ISO 27001:2013 7.2(b), 7.3, A.7.2.2, A.12.2.1

NIST SP 800-37 3.3, 3.4, 3.5, 3.7

NIST SP 800-53 AT-2, AT-3, CP-3, IR-2, PM-13, SI-3, SI-4(24)

NIST Cybersecurity Framework DE.DP-1, ID.GV-1, PR.AT-1-5, RS.RP-1, RS.MI-2

PCI 6.5, 9.9, 12.6.1-2, 12.10.4, A3.1.4