Personnel Security 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

Each ABC Company asset must be protected during its lifecycle from its creation through its disposal. Each asset must be classified and protected based on its importance to the organization.

# II. Purpose

This policy defines requirements for the protection of corporate assets from abuse, misuse, or destruction. Each authorized user has an obligation to preserve and protect assets in a consistent and reliable manner. Security controls provide the necessary technical, physical, and operational safeguards to protect assets.

# III. Scope

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

# IV. Policy

Asset protection plays an important role in ensuring information confidentiality, availability, and integrity. Protection measures are introduced at the recruitment or vendor procurement phase, included in the employee handbook and vendor contracts, and monitored during an individual’s employment or use of third party service providers.

All Staff must protect both tangible and intangible corporate assets. Staff are responsible for reporting to the appropriate manager any real or suspected threats to corporate assets.

Information security responsibilities are to be followed by all Staff who have access to ABC Company’s Information Resources. All Staff must acknowledge in writing that they have read the appropriate Confidentiality Agreement.

Specific information security responsibilities must be incorporated into all contracts with Staff who have access to ABC Company assets.

Information security training shall be provided by the IT Department on a regular basis to make Staff aware of information security policies, procedures, and responsibilities. All Staff shall be trained in the security requirements and processes associated with their job duties, services provided, appropriate business controls, and the correct use of IT systems and facilities.

All Staff must acknowledge in writing that they have read and understood ABC Company’s Security Policy. In addition, all Staff shall receive annual security related training.

Prior to hire, all employees must pass a background check that includes examination of criminal conviction records, credit bureau records, and verification of previous employment. On-going annual background checks shall be performed on all staff that have access to sensitive information.

All Staff must be trained to recognize conflicts of interest and the appearance of conflicts of interest during their first week of employment and annually thereafter. All Staff must identify and submit to their immediate supervisor any conflicts of interest. All conflict of interest statements must be reviewed by the Chief Security Officer (CSO). If the CSO identifies a significant conflict of interest, the conflicts must be discussed with the Staff member’s immediate supervisor to determine the appropriate course of action.

All Staff must sign an ABC Company Non-disclosure Agreement prior to beginning work for ABC Company.

The CSO will implement a system for security incident reporting, response, tracking, and resolution. All Staff are responsible for reporting to the appropriate ABC Company manager any violations of this Policy.

The Human Resources Department is responsible for ensuring that background checks are performed on ABC Company employees. The CSO is responsible for implementing and maintaining Staff security education and awareness training programs. Refer to the Security Awareness and Training Policy for more information.

Executive management shall ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Department Heads are responsible for enforcing compliance with this policy.

# 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 Department Heads and those responsible for information system security.

**Policy History**

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

**References:**

COBIT APO07.12-13, APO08.05-06, APO09.05, APO10.05, APO12.02, APO13.07, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i)

ISO 27001:2013 8.1, A.6.2.2, A.7.1, A.9

NIST SP 800-37 3.4, 3.6, 3.7

NIST SP 800-53 AC-1-3, AC-17, PE-17, PL-4, PS-6, PS-7, SA-9

NIST Cybersecurity Framework ID.AM-6, ID.RA-6, PR.AC-1-4, PR.AC-6-7, PR.AT-1, DE.DP-2

PCI 7.1-3, 8.1-2, 8.4-5, 8.8