Staffing 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

ABC Company must have appropriately supervised professional Staff sufficient to maintain business processes. The staffing level should be appropriate to the environment considering the amount and type of information for which they are responsible as well as the level of risk.

# II. Purpose

This policy ensures sufficient Staffing resources are allocated to supporting and managing ABC Company business processes.

# III. Scope

This policy applies to all ABC Company Department Heads.

# IV. Policy

ABC Company departments are responsible for having appropriately supervised professional staffing sufficient to maintain business processes. The staffing level should be appropriate to the environment considering the amount and type of information for which they are responsible as well as the level of risk.

Staffing processes generally involve the following four steps which apply equally to general users as well as to managers, System Administrators, and security personnel.

1. Position definition - early in the process of defining a position, security issues must be identified and addressed. Once a position has been broadly defined, the responsible Department Head must determine the type of computer access needed for the position. Security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for a particular information system shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the information system, and the classification level of data processed or stored. There are two general security rules to apply when granting access:

* Separation of duties. Refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.
* Least privilege access. This means of granting access refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have a need to run E-mail utilization reports.
* Competency. Management shall determine the necessary competency of Staff that affects information security performance and determine the competency needed based on the appropriate education, training, or experience.

2. Position sensitivity – the responsible Department Head shall determine the position sensitivity, based on the duties and access levels, so that appropriate cost effective screening can be completed.

3. Screening – management shall take actions to acquire and maintain Staff with the necessary competence. Background screening helps determine whether a particular individual is suitable for a given position. Generally, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening alone to reduce the risk to ABC Company. Pursuant to local laws, regulations, ethics, and contractual constraints all employment candidates, contractors and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Contractual agreements shall state Staff and ABC Company’s responsibilities for information security.

4. Training and awareness – Staff shall be trained in the computer security responsibilities and duties associated with their jobs. Refer to the Security Training Policy for more information.

# 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 Executive Management and Department Heads.

**Policy History**

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

**References:**

COBIT APO07.12-13, APO08.12-13, APO10.05, APO11.09-10, APO12.07, BAI08.11-12

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