Reporting Violations 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 Staff are responsible for notifying IT Help Desk or their supervisor if they suspect there has been a violation of an ABC Company policy or if they suspect there may have been a security incident.

# II. Purpose

Staff are a first line of defense and this policy helps ensure protection of ABC Company Information Resources and their availability, integrity, and confidentiality.

# III. Scope

This policy applies to all Staff that access ABC Company’s Information Resources.

# IV. Policy

Every Staff member is responsible for ensuring that ABC Company maintains the highest professional standards while protecting information confidentiality, integrity, and availability. Staff members are obliged to report any suspected violation of company policies. Reports can be made to any of the following departments as appropriate:

* Information Technology (IT)
* Human Resources (HR)
* Legal
* Executive Management

Staff shall not be disciplined or penalized for reporting honestly and in good faith. All reports shall be kept confidential except as necessary to conduct investigations.

# 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 EDM02.03, APO01.03, APO12.02, APO12.07, DSS01.05, MEA03.01, MEA04.11

GDPR Article 32, 33, 34

HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.314(a)(1)

ISO 27001:2013 9, 10.1, A.12.4, A.16.1.1-3

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AU-6, CA-7, IR-6, IR-8, SI-2, SI-4

NIST Cybersecurity Framework DE.AE-1-3, PR.AT-1, DE.CM-1-2, RS.MI-2

PCI 9.9.3, A3.2.6.1, A3.3.1