Security Monitoring 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

Security monitoring confirms that ABC Company’s security mechanisms and controls are in place, are effective, and are not being bypassed.

# II. Purpose

One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning.

# III. Scope

This policy applies to all Staff responsible for the installation of new IT resources, the operations of existing resources, and charged with IT security.

# IV. Policy

Automated tools provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline shall be developed and tools used to report exceptions. Tools shall be deployed to monitor:

* Internet traffic
* Electronic mail traffic
* LAN traffic, protocols, and device inventory
* Operating system security parameters

The following files shall be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by the Risk Management Officer:

* Automated intrusion detection system logs
* Firewall logs
* User account logs
* Network scanning logs
* System error logs
* Application logs
* Data backup and recovery logs
* Help desk trouble tickets
* Telephone activity (e.g. call detail reports)
* Network printer and fax logs

An evaluation of Information Systems by IT security Staff shall be performed on an annual or more frequent basis as needed. Such evaluations shall include a review of:

* Password strength
* Unauthorized network devices
* Unauthorized personal web servers
* Unsecured sharing of devices
* Unauthorized remote connectivity
* Unauthorized operating systems
* Unauthorized software licenses

Any security issues discovered will be reported to the IT Director for follow-up investigation.

Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) shall monitor network traffic and alert personnel to suspected compromises. IDS and IPS systems shall be maintained and kept up-to-date. Any changes shall be authorized by the appropriate asset Owner and logged. IDS and IPS systems shall be updated in a timely manner with vendor supplied patches. IDS/IPS detection alerts shall be issued if suspected intrusions or other unauthorized activities have occurred.

Procedures shall be developed to monitor and record growth and traffic patterns, bandwidth issues, etc. Appropriate reporting shall be in place to allow IT to anticipate performance issues and delays and react in a timely and proactive manner.

# 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 ABC Company Executive Management, Department Heads, IT Director, Risk Management Officer, and Chief Security Officer.

**Policy History**

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

**References:**

COBIT EDM03.07, APO01.11, APO09.05, APO13.07, DSS01.05, DSS05.02, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(C), 164.312(b)

ISO 27001:2013 9.1, 9.3, A.12.1.3, A.12.4, A.15.2.1

NIST SP 800-37 3.7

NIST SP 800-53 AU-3-4, AU-5(1), AU-6, AU-11-12, AU-14, CP-2(2), SA-9 SC-5(2)

NIST Cybersecurity Framework PR.AC-1-2, PR.AC-4, PR.PT-1, DE.AE-1-5, DE.CM-1-7

PCI 8.1.5, 9.1, 10.2, 10.4.2.b, 10.5.5, 10.6-7