Intrusion Detection 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

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

# II. Purpose

This policy establishes intrusion detection and security monitoring to protect resources and data on ABC Company’s network. It provides intrusion detection implementation guidelines along with associated roles and responsibilities.

# III. Scope

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

# IV. Policy

The objectives of this policy are to:

* Increase the level of security by actively searching for signs of unauthorized intrusion.
* Prevent or detect the confidentiality of organizational data on the network.
* Preserve the integrity of organizational data on the network.
* Prevent unauthorized use of organizational systems.
* Keep hosts and network resources available to authorized users.
* Increase security by detecting weaknesses in systems and network design early.

Intrusion detection provides two important functions in protecting Information Resources:

* Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
* Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

All systems accessible from the Internet or by the public must operate IT approved active intrusion detection software during anytime the public may be able to access the system.

All systems in the DMZ must operate IT approved active intrusion detection software.

All host based and network based intrusion detection systems shall have their log files reviewed on a daily basis.

All intrusion detection logs must be kept for a minimum or 30 days. This provides an audit trail of past events. Operating system, user accounting, and application software audit logging processes are to be enabled on all host and server systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems are to be enabled. Audit logging of any firewalls and other network perimeter access control system are to be enabled and audit logs from the perimeter access control systems will be monitored/reviewed daily by the Chief Security Officer (CSO).

System integrity checks of the firewalls and other network perimeter access control systems will be performed on a routine basis. Audit logs for servers and hosts on the internal, protected, network will be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the CSO.

Host based intrusion tools will be checked on a routine and all trouble reports should be reviewed for symptoms that might indicate intrusive activity.

Incident Response security controls must not be bypassed or disabled. All personnel are responsible for managing their use of incident response and are accountable for their actions relating to incident response security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments shall have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

All suspected and/or confided instances of successful and/or attempted intrusions will be immediately reported according to the Incident Response Plan. Users shall be trained to report any anomalies in system performance and signs of wrong doing to the Help Desk. Any suspected intrusions, suspicious activity, or system unexplained erratic behavior discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour.

The intrusion detection team shall:

* Monitor intrusion detection systems both host based and network based.
* Check intrusion detection logs daily.
* Determine approved intrusion detection systems and software.
* Report suspicious activity or suspected intrusions to the incident response team.

The incident response team shall:

* Act on reported incidents and take action to minimize damage, remove any hostile or unapproved software.
* Recommend changes to prevent future incidents.
* Action shall be based on the approved Incident Response Plan.

# 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 Staff responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with information security.

**Policy History**

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

**References:**

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(C), 164.312(b), 164.312(e)(2)(i)

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

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AU-3, AU-6, AU-9, AU-11, AU-12, AU-14, RA-3, RA-5, SI-2, SI-5

NIST Cybersecurity Framework DE.AE-1-5, DE.CM-1-6, RS.RP-1, RS.MI-2

PCI 10.1-9