Vulnerability and Penetration Testing 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

Vulnerability assessments and penetration tests evaluate systems for security related vulnerabilities.

# II. Purpose

Vulnerability assessments and penetration tests help ensure that security controls are sufficient and effective at providing information confidentiality, availability, and integrity.

# III. Scope

This policy applies to all Staff responsible for the installation and support of IT, individuals charged with IT Security, data owners, Chief Security Officer (CSO), and Risk Management Officer.

# IV. Policy

Vulnerability assessments and penetration tests identify and help reduce risks to ABC Company’s Information Systems.

* Vulnerability assessments search Information Systems for known vulnerabilities. Examples include patches that haven't been installed, weak encryption, etc.
* Penetration tests attempt to actively exploit weaknesses in an environment. Examples include SQL injection attacks, cross site scripting, etc. Penetration tests can also include social engineering to evaluate the effectiveness of Staff security education and awareness training.

The Chief Security Officer (CSO) is responsible for ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The CSO shall:

* Evaluation – identity the type of evaluation(s) to be performed. These include vulnerability assessment, penetration test, or both vulnerability assessment and penetration test.
* Scope – define the scope including systems being evaluated, timeframes, controls to be used, etc. Determine if social engineering is included in the scope.
* Resources – identify resources to perform the evaluation.

Access to vulnerability assessment and penetration testing tools shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. The evaluation shall be carefully planned and agreed to minimize disruptions to business processes.

The CSO shall develop and maintain a program for penetration testing that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks. Such test program shall consider a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production. These include attacks against supervisory control, data acquisition, and other control systems.

Where possible, IT security Staff shall utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify potential vulnerabilities on the organization's systems.

The CSO shall use Certified Information Systems Auditors to perform an independent evaluation. Evaluations shall be performed on an annual basis or more frequently if major changes occur to Information Resources or Staff. The report deliverable shall identify the project scope, findings, and recommendations to enhance security. The CSO shall:

* Review the report to confirm the findings and verify the security recommendations are sufficient and effective.
* Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The CSO shall document important findings in the Audit Log Form and The Risk Management Officer shall provide necessary reporting to ABC Company Executive Management.

# V. Enforcement

Any Staff member 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, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

**Policy History**

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

**References:**

COBIT EDM03.07, APO12.02, APO12.07, APO13.07, BAI10.07, DSS05.07, MEA01.05

GDPR Article 32

HIPAA 164.308(a)(8)

ISO 27001 9.2, A.15.2.1

NIST SP 800-37 3.5

NIST SP 800-53 3.3, AC-5, AU-6, CA-2

NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2

PCI 2.2.a-d, PCI Software Security Framework