Wipro’s

Vulnerability Assessment and

## Penetration Testing Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office (GCISO) |
| Sub-function | - |
| Policy Owner | Lakshminarayanan RS, Group Head - Information Security Policy & Framework |
| Policy Effective Date | January 1, 2022 |

**Purpose**

This policy establishes the requirement that the vulnerabilities in the Organization's information systems are identified, tracked, and remediated.

**Audience**

Organization’s employees, retainers, contractors, and service providers engaged in Vulnerability Assessment and Penetration Testing (VAPT).

**Scope**

This policy applies to:

* Vulnerability Assessment – Intranet and Internet facing information systems.
* Penetration Testing – Internet facing information systems.

**Policy Details**

**VAPT.1** An inventory of the information systems within VAPT scope shall be maintained.

**VAPT.2** VAPT shall be performed as per the periodicity defined in the Vulnerability Assessment and Penetration Testing Standard.

**VAPT.3** VAPT shall be performed with prior approval from the application owners.

**VAPT.4** The information system owners shall provide the prerequisites to perform VAPT.

**VAPT.5** An intrusive and a non-intrusive VAPT scanning shall be performed as per business requirements.

**VAPT.6** A grey box and a black box VAPT shall be performed on the public facing information systems.

**VAPT.7** The identified vulnerabilities, along with remedial actions, shall be documented and reported to the information system owners.

**VAPT.8** Identified vulnerabilities shall be tracked and remediated as per the Vulnerability Assessment and Penetration Testing Standard.

**VAPT.9** The Organization shall receive vulnerability information and threat intelligence reports from authentic external and internal sources.

**VAPT.10** VAPT shall be performed in accordance with the applicable laws, regulations, and business requirements.

**VAPT.11** Thelogging and monitoring of VAPT shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Information Systems | Set of applications, websites, services, information technology assets, or other information handling components. |
| Non-Intrusive | Scanning for vulnerabilities without exploiting them. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Penetration Testing | A testing methodology in which assessors, typically working under specific constraints, attempt to circumvent the security features of the information systems. |
| Threat Intelligence | Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. |
| Vulnerability | A weakness in an information system, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| VAPT | Vulnerability Assessment and Penetration Testing |

**References**

* Logging and Monitoring Standard
* Vulnerability Assessment and Penetration Testing Standard
* Vulnerability Assessment and Baseline Compliance Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 12th July 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Jyotisman Chakrabarty/ Maruthi Kumar | Lakshminarayanan RS | 18th January 2024 |
| 1.1 | 23rd April 2024 | Updated Purpose. | Jyotisman Chakrabarty/ Maruthi Kumar | Lakshminarayanan RS | 23rd April 2024 |