Document Control

Document Publication History	
Document Prepared by	
Document Reviewed by	
Document Approved by	
Document Owned by	
Effective Date	
Review Date	
Document Approved Date	
Document Classification	Internal

Document Distribution List			
#	Name	Organization	Purpose
1.	All Employees and affiliates		Initial version
2.			
3.			
4.			

Document Approval History				
Version	Date	Name	Role	Comments
1.0			CISO	Initial version

Contents

1. Objective

This policy establishes the framework for periodic vulnerability assessment and penetration testing (VAPT) on BESSEGGEN INFOTECH LLP critical IT assets and infrastructure. Its primary objective is to proactively identify security vulnerabilities within the IT environment and evaluate the overall security posture through simulated cyberattacks.

2. Scope

This policy applies to all critical IT assets and infrastructure components of BESSEGGEN INFOTECH LLP. This includes, but is not limited to, servers, networking systems, security devices, load balancers, and all other IT systems directly supporting business operations.

3. VAPT Frequency

VAPT shall be conducted at least once per financial year. No audit cycle shall be skipped, irrespective of any changes in audit categories. The VAPT process will commence in Q1 of each financial year.

Additionally, VAPT will be performed following major infrastructure or application changes, or as mandated by regulatory bodies.

4. Engagement of CERT-In Empanelled Organizations

BESSEGGEN INFOTECH LLP shall exclusively engage CERT-In empanelled organizations for conducting VAPT services. These organizations are officially authorized by the Indian Computer Emergency Response Team (CERT-In) to provide certified security assessment services.

5. VAPT Process

The VAPT process comprises the following phases:

i. Planning and Scoping

- **Define Scope:** Clearly delineate the systems, networks, applications, and data to be included in the assessment.
- **Establish Objectives:** Set clear goals for the VAPT engagement, including specific methodologies and rules of engagement.
- **Approval:** Obtain formal approval from the Technology Committee for the defined scope and objectives.

ii. Vulnerability Assessment

- **Tool-Based Scanning:** Utilize industry-standard vulnerability scanning tools such as Nessus, Qualys, and OpenVAS.
- **Manual Validation:** Conduct manual validation of identified vulnerabilities to minimize false positives and confirm their exploitability.
- **Prioritization:** Categorize and prioritize vulnerabilities based on their severity and potential impact to BESSEGGEN INFOTECH LLP.

iii. Penetration Testing

- **Attack Simulation:** Simulate real-world attack scenarios to exploit identified vulnerabilities.
- **Exploitation Attempts:** Attempt to gain unauthorized access, escalate privileges, or exfiltrate data to demonstrate the potential impact of vulnerabilities.
- **Documentation:** Thoroughly document all findings, including the techniques used for exploitation and the evidence of successful compromise.

iv. Reporting

- **Comprehensive Report:** Provide a detailed report including an executive summary, methodology, technical findings, and a clear assessment of risks.
- **Technology Committee Approval:** Submit the VAPT report to the Technology Committee for review and approval.
- **Regulatory Submission:** Submit the final report to relevant Exchanges/Depositories within **one month** of the VAPT completion.

6. Pre-Commissioning VAPT

All critical systems must undergo VAPT prior to their live deployment. The results of this pre-commissioning VAPT must be thoroughly reviewed and formally approved by the Technology Committee before the system is moved to a production environment.

7. Reporting Off-the-Shelf Product Vulnerabilities

Vulnerabilities identified in off-the-shelf products shall be reported to both the respective vendors and relevant exchanges/depositories. BESSEGGEN INFOTECH LLP will coordinate mitigation steps with the vendors and implement compensatory controls as necessary until a permanent fix is deployed.

8. Immediate Remediation of Gaps

Identified vulnerabilities and security gaps shall be remediated based on their risk severity within the following timelines:

Severity	Maximum Closure Time	Retest Required
Critical	15 days	Yes
High	30 days	Yes
Medium	45 days	Optional
Low	90 days	Optional

Remediation efforts shall adhere to established incident response and change management procedures.

9. Vulnerability Severity Classification

S. No	Risk Rating	Description
1	Critical	This level of vulnerabilities can allow attackers to take complete control of mobile applications and application servers. By exploiting these vulnerabilities, attackers could carry a range of acts including information stealing, application defacing and tricking users to do unwanted activities. The vulnerability marked as "***Critical***" is recommended to be handled with utmost priority.
2	High	This level of vulnerabilities indicates maximum risk associated with a vulnerability instance. Such vulnerability can allow attackers to completely compromise mobile applications and their data. Attackers can modify applications in such a way that they behave other than it is intended to do. The vulnerability marked as "***High***" should be mitigated at the earliest after "Critical risk" vulnerabilities are mitigated.
3	Medium	Such vulnerability may enable an attacker to exploit the application and its data to a particular level so that the attacker can gain low level information about the application. Such information can be used by an attacker to craft more specific attacks based on the information collected. The vulnerability marked with "***Medium Risk***" should be mitigated at the earliest after "High Risk" vulnerabilities are mitigated.
4	Low	Such vulnerability may allow an attacker to gain some information about the application which was not intended to be known otherwise. The attacker may not have exploiting techniques available at that instance based on the information revealed by the system. The vulnerability marked with "***Low Risk***" can be mitigated soon after high and medium risk vulnerabilities are mitigated.

10. **Closure of Findings and Compliance Reporting**

An action plan for addressing all VAPT findings shall be developed promptly. A compliance report detailing the remediation status must be submitted within three months of the VAPT completion. Revalidation of remediated findings shall occur within five months of the VAPT completion. Any open findings beyond three months require explicit approval from the Technology Committee with a justified explanation and a revised remediation timeline.

11. **Compliance and Review**

This policy shall be reviewed annually, or upon any significant changes to the IT infrastructure or regulatory landscape. The VAPT process will be continuously adjusted to align with the evolving threat landscape. VAPT for the application has been conducted once year as per SEBI CSCRF.

12. **Training and Awareness**

- **Technical Teams:** Semi-annual training sessions will be conducted for technology teams to enhance their understanding of emerging threats and secure development practices.
- **All Staff:** Annual security awareness sessions will be provided to all staff members, covering general security best practices.
- **Simulated Drills:** Regular simulated exploit-based drills will be conducted to test the effectiveness of incident response procedures and staff readiness.

13. **Policy Exceptions**

Any exceptions to this policy must be formally approved by the Technology Committee, accompanied by a comprehensive justification.

14. **Policy Review**

This policy will undergo a formal review by management at least annually.

15. **Enforcement**

Violations of this policy may result in disciplinary action, up to and including termination of employment.

Annexure A: Vapt Tracking Register

Vulnerability	Severity	Owner	Date Detected	Planned Closure	Actual Closure	Status	Comments