Security Testing Plan Document for Cloud-Based Solutions

1. Introduction

This Security Testing Plan outlines the approach, scope, objectives, responsibilities, and methodologies to assess and validate the security posture of the cloud-based solution.

2. Objectives

- Identify potential security vulnerabilities in the cloud solution.
- Validate compliance with organizational and regulatory security requirements.
- Assess the effectiveness of existing security controls.
- Provide recommendations for remediation.

3. Scope

- Cloud Service Model: [IaaS / PaaS / SaaS]
- Components in Scope: [e.g., API Gateway, Web Application, Storage, Database]
- Out of Scope: [e.g., 3rd Party Integrations, On-premise Networks]

4. Roles and Responsibilities

Role	Responsibility
Security Lead	Plan and oversee security testing activities
Tester	Execute security tests and document findings
System Owner	Coordinate access and facilitate testing
Developer	Implement remediation and updates

5. Security Testing Approach

- Threat Modeling
- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Access Control Review
- Compliance Verification

6. Testing Methodology

1. Information Gathering
2. Identify Assets and Entry Points
3. Manual and Automated Scanning
4. Exploitation (in test environments)
5. Analysis and Reporting

7. Testing Tools

- OWASP ZAP / Burp Suite
- Kali Linux Tools
- Cloud Security Scanners (e.g., ScoutSuite, Prowler)
- CIS Benchmark Tools

8. Reporting & Remediation

- Finding descriptions and evidence
- Risk ratings (e.g., Critical, High, Medium, Low)
- Remediation recommendations
- Timeline for remediation and retesting

9. Schedule

Activity	Start Date	End Date
Preparation	[ ]	[ ]
Execution	[ ]	[ ]
Reporting	[ ]	[ ]

10. Approval

Approved by: _____

Date: _____