

# **Service Level Agreement (SLA)**

**Effective Date: 16/02/2024**

## **Parties:**

1. **Client:** KS Security Solution
2. **Service Provider:** HackersForYou

## **Purpose:**

The purpose of this SLA is to establish clear expectations in regards to service levels, response times, reporting, and remediation support during the penetration testing engagement.

## **1. Service Level Objectives (SLOs):**

### **a. Response Times:**

- **Initial Acknowledgment:**
  - The Provider will acknowledge any communication from the Client within 2 hours during business hours.
  - For urgent matters, the acknowledgment time shall be 30 minutes.
- **Technical Support:**
  - The Provider will respond to technical queries or issues raised by the Client within 24 hours.
  - Urgent technical issues shall receive a response within 4 hours.

### **b. Reporting Timelines:**

- The Provider will deliver the penetration testing report within 5 days after the testing phase.
- The Client will have 7 days to review the report and seek clarifications.

### **c. Remediation Support:**

- The Provider will provide remediation guidance and support for identified vulnerabilities within 7 working days after the report delivery.
- Urgent vulnerabilities shall receive priority attention.

## **2. Consequences for Failing to Meet SLOs:**

- **Response Time Consequences:**
  - If the initial acknowledgment or technical support response time is not met there will be a 20% reduction in pay per month.
  - Repeated action could result in further penalties or the contract being terminated.
- **Reporting Timelines Consequences:**
  - If there are any delays in providing the penetration testing report upon the time agreed, could result in pay reduction.
  - If the delays are significant, this could result in renegotiation of fees or the termination of contract.
- **Remediation Support Consequences:**
  - Remediation support that is delayed or inadequate could impact the overall security posture.
  - The Provider will work diligently to address any shortcomings and rectify the situation.

- **Secure Messaging Platforms:** When exchanging sensitive information, encryption services or platforms with end-to-end encryption should be used.
- **Virtual Meetings:** All findings, remediation strategies and progress updates, should be communicated via video call.
- **Secure File Sharing:** All confidential documents and reports should be shared via a secure file-sharing service that has access controls.
- **Phone Calls:** When necessary, engaging in phone conversations to address urgent matters related to the engagement.

### 3. Alignment with SOW and Engagement Goals:

- This SLA will align with the overall **Statement of Work (SOW)** and the engagement goals that are outlined.
- All conflict or discrepancies that arise between the SOW and this SLA will be promptly addressed by both parties.

## **Acknowledgment and Acceptance:**

Signing this SLA allows, both parties to acknowledge that they understand the terms and agree to follow the specified service levels during the penetration testing engagement.

### **KS Security Solution (Client):**

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Date: \_\_\_\_\_

### **HackersForYou (Penetration Testing Provider):**

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Date: \_\_\_\_\_