INCIDENT RESPONSE PLAN (IRP)

1. Introduction

This Incident Response Plan (IRP) is a critical component of FG-IR ("Company")'s Risk Management Strategy, designed to provide a structured and effective approach to managing and mitigating security incidents. Recognizing the ever-present threat of cyberattacks and data breaches in today's digital landscape, our IRP outlines the procedures for promptly identifying, responding to, and recovering from incidents to minimize their impact on our operations and our clients' trust. This plan ensures that all members of our team are prepared to act swiftly and cohesively, leveraging our collective expertise to safeguard our Company's and clients' information assets. Through preparation, response, and post-incident analysis, we reinforce our commitment to maintaining the highest level of security and resilience against cyber threats.

2. Purpose

The purpose of this IRP is to ensure that any incidents are dealt with in a timely and orderly manner, to minimize impact and restore operations as quickly as possible.

3. Scope

The IRP covers all information systems, data, network infrastructure, and personnel associated with the consultancy firm.

4. Definitions and Severity Levels

- **Incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- **Severity Levels:** Classification of incidents (Low, Medium, High, Critical) based on their impact and urgency.

5. Roles and Responsibilities

- **Incident Response Coordinator (IRC):** Founder or Managing Director, who oversees and coordinate the incident response process and all its steps.
- **Information Security Contact:** Expert who will handle the incident response from the IT side (contact data at the end of this document).
- **Employees/Contractors:** Report any potential security incidents to the IRC.
- **Backup Incident Response Coordinator (IRC):** In the absence of the Founder or Managing Director, employees/contractors should report to the Information Security Contact (contact data at the end of this document).

6. Incident Identification

- Monitor systems and network traffic for unusual activity.
- Implement procedures for employees/contractors to report anomalies.

INCIDENT RESPONSE PLAN (IRP)

7. **Incident Response Procedure**
   i. **Preparation:**
      - Maintain up-to-date emergency contact lists.
   ii. Make all personnel, including contractors, aware of this IRP and ensure they agree to it.
   Detection & Identification:
      - Confirm whether an incident has occurred.
      - Assess the scope and impact of the incident.
   iii. **Containment:**
      - Execute immediate actions to limit the impact.
      - Preserve evidence for potential forensic analysis.
   iv. **Eradication:**
      - Identify and remove the root cause of the incident.
      - Secure systems to prevent recurrence.
   v. **Recovery:**
      - Restore systems to operation in a controlled manner.
      - Monitor for any signs of the threat re-emerging.
   vi. **Post-Incident Analysis:**
      - Conduct a debrief to document the incident's cause and impact.
      - Update IRP and security measures based on lessons learned.

8. **Communication Plan**
   - **Internal Communication:** Keep all team members informed about the incident status and their expected roles.
   - **External Communication:** Establish protocols for communicating with clients, stakeholders, and authorities if necessary. See Communication Plan for Security Breach Disclosure.

9. **Documentation and Reporting**
   - Keep detailed records of the incident, its management, and resolution.
   - Prepare a final incident report summarizing the response process and outcomes.

10. **Agreement**

All employees are asked to comply with the IRP and must sign an agreement indicating that they understand and agree to this Policy.

11. **Compliance and Enforcement**

Non-compliance or violations to this policy may result in disciplinary action, up to and including termination of contract/employment.

INCIDENT RESPONSE PLAN (IRP)

12. Policy Review
This policy will be reviewed regularly to ensure that it remains up-to-date and effective in addressing evolving security threats and technological advancements.

Designated Information Security Contact:
The following contact is responsible for Information Security, technology devices and protocols:

Las Olas Technologies, Inc.
Attn: Mr. Jeff Mendelson
Email: jeff@lasolastech.com, Phone Number / WhatsApp: +1.954.294.7827

Conclusion:
By adhering to the guidelines outlined in this Incident Response Plan (IRP), employees/ contractors can contribute to the overall security posture of the Company and protect client data from unauthorized access or disclosure, both when working remotely and in public places. Compliance with these procedures is essential for maintaining the trust and confidence of our clients and stakeholders.