INFORMATION SECURITY POLICY (ISP)

1. Introduction

This Information Security Policy (ISP) is the cornerstone of FG-IR ("Company")'s risk management strategy and commitment to safeguard the confidentiality, integrity, and availability of our and our clients' information assets. In the dynamic landscape of consulting, we recognize the critical importance of robust information security practices. Our policy sets forth the responsibilities and guidelines for all employees, contractors, and partners, aiming to mitigate risks, ensure regulatory compliance, and uphold our Company's reputation for trustworthiness and excellence. As we navigate through complex data environments and regulations, this ISP guides our collective efforts to protect sensitive information and maintain the highest standards of security and confidentiality.

2. Purpose

The purpose of this policy is to establish guidelines and procedures for safeguarding client data and other sensitive information. It comprises office work and home-office, as well as remote work in public places. In any of these situations, it is imperative to maintain the confidentiality, integrity, and availability of all company assets to ensure compliance with legal and regulatory requirements and to preserve client trust.

3. Scope

This policy applies to all employees, either full and part-time staff, contractors, freelancers, and other agents, including third-party vendors, who handle or have access to Company and client data, regardless of their location or the devices used for accessing such data.

4. Remote Work Guidelines

- Employees must use company-approved devices and secure network connections when working remotely. For definition of company-approved devices, please access the Bring Your Own Device Policy (BYOD).
- All devices used for remote work must have up-to-date security patches installed.
- All non-Mac devices used for remote work must have up-to-date antivirus installed.
- Employees should only access Company data through secure connections (e.g., own private networks and VPN) and avoid using public Wi-Fi networks.
- Data transmission should be encrypted using approved encryption protocols.
- Employees are responsible for the physical security of their devices and must report any loss or theft immediately.
- Multi-factor authentication (MFA) should be enabled for accessing company systems and applications.

INFORMATION SECURITY POLICY (ISP)

5. Password Security Requirements

All passwords that are generated by the Company for use by our employees/contractors must contain:

- At least 15 characters
- At least one Uppercase letter
- At least one lower case letter
- At least one symbol
- A series of numbers

Where applicable, 2FA authentication is enabled for all software and hardware that support it.

6. Use of Removable Media

All removable media, external hard drives, USB drives, etc. are consistently under 2-layers of lock and key. All external media must be secure after use and not left unattended.

7. Public Places Guidelines

- Employees should exercise caution when working in public places to avoid exposing sensitive information to unauthorized individuals.
- Screen protectors should be used to prevent shoulder surfing.
- Devices should be locked when unattended, and passwords should be strong and not shared with others.
- Public Wi-Fi networks should be avoided when handling sensitive information. Working at public places with a low-security environment in terms of Internet access is strictly forbidden when handling material confidential information from clients.

8. Data Handling Procedures

- Client data should only be accessed on a need-to-know basis and should not be stored locally on personal devices.
- Data should be encrypted both at rest and in transit.
- Secure file sharing mechanisms should be used for transferring sensitive data.

9. Reporting Security Incidents

- Employees must report any suspected security incidents or breaches immediately to the designated security officer or IT department.
- The Incident Response Plan (IRP) should be followed in the event of a security incident, including steps for containment, investigation, and mitigation.

INFORMATION SECURITY POLICY (ISP)

10. Agreement
All employees are asked to comply with the ISP 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.

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 Information Security Policy (ISP), employees 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.