INFOTECH SERVICE FZ-LLC

Security Insurance Plan (SIP) Version 2.1

Status: Validated
Version: 2.1
Date of Approval: 06/06/2024
Approvers:

Summary:

This Security Insurance Plan outlines the necessary technical and organizational security measures that must be adopted by third-party partners when accessing INFOTECH SERVICE FZ-LLC's data or information systems. The purpose is to ensure that the third parties maintain compliance with security best practices, safeguarding sensitive information and ensuring the resilience and effectiveness of the systems. The plan applies to the duration of the agreement and is subject to regular reviews and audits.

Scope and Duration:

- The SIP applies to any third-party accessing INFOTECH SERVICE FZ-LLC's data or systems for services or partnerships.
- It outlines the technical and organizational security controls required for safeguarding data and systems.
- The security measures shall remain effective throughout the duration of the agreement with the third-party and are subject to audits.

Key Areas Covered:

1. **Information Security Organization & Policy:**
    - **Information Security Policy:** Third-party must formalize and communicate their Information Security Policy, addressing governance and security requirements.
    - **Certification:** Provide evidence of compliance with standards such as ISO, NIST.
    - **Subcontracting:** Ensure subcontractors adhere to the same security requirements.
2. **Logical Access:**
    - **Access Control:** Access to systems and data must be restricted based on necessity, using strong authentication methods and password policies.
    - **Privileged Account Management:** Stronger authentication methods for privileged accounts must be enforced.
3. **Infrastructure, Network, and Systems Security:**
    - **Segmentation & Firewalls:** Proper network segmentation and firewall protection are mandatory.

- **Host Security:** Regular monitoring, hardening of servers, and anti-virus deployment.

4. **Data Protection:**
    - **Data Location:** Identify data center locations, and control access to employees.
    - **Encryption:** Data in transit must be encrypted using secure protocols like SFTP, TLS.
    - **Data Destruction:** Formal data destruction procedures are required after contract termination.
5. **Monitoring and Logging:**
    - **Continuous Monitoring:** Security events must be monitored and logged. Logs should be made available to INFOTECH SERVICE FZ-LLC upon request.
6. **Security Incident Management:**
    - **Incident Reporting:** Define the scope and level of information that will be reported to INFOTECH SERVICE FZ-LLC in case of security incidents, including timelines and procedures for notification.
7. **Compliance:**
    - **GDPR Compliance:** Ensure compliance with GDPR and other applicable data protection laws, including protection of personal data.

Review and Audit:

INFOTECH SERVICE FZ-LLC reserves the right to audit the third-party's compliance with the security measures outlined in this plan. Regular reviews will take place to assess compliance and update the SIP as needed.

This plan emphasizes the importance of stringent security controls across all aspects of data handling and system access by third parties. Regular audits, data encryption, and incident reporting are critical elements to ensure the safety and integrity of INFOTECH SERVICE FZ-LLC's information systems.