Global Information System Security Policy (ISSP)

1. Introduction

The **Global ISSP** is established to protect information security within INFOTECH SERVICE FZ-LLC by addressing core security concerns, outlining key objectives, and providing a reference framework for the company's information system.

Key Objectives:

- Ensure **Availability**, **Integrity**, **Confidentiality**, and **Traceability** of all information.
- Protect against accidental or malicious threats affecting the company's information systems.

2. Scope of the ISSP

The **ISSP** applies to:

- All resources (technical, human, and organizational) involved in managing information within the company.
- Subsidiaries, entities, and suppliers who interact with INFOTECH SERVICE FZ-LLC's systems.
- Compliance with relevant regulations, customer contracts, and security requirements.

3. Governance Structure

The policy defines the roles and responsibilities within the governance framework to ensure adherence to security practices across all levels:

- **Global Chief Information Security Officer (CISO)**: Oversees the Information Security Management System (ISMS), ensuring its operational integrity.
- **Operational Group Security Officers (OG SOs)**: Implement and enforce ISS policies within business units and subsidiaries.
- **Local Security Correspondents**: Assist in enforcing security measures at a local level, ensuring alignment with global security strategies.

4. Security Policy Lifecycle

The **ISSP** undergoes continuous improvement through a structured lifecycle:

1. **Plan**: Identify updates and plan actions based on security needs.
2. **Do**: Implement planned updates.
3. **Check**: Monitor impacts on operations and measure compliance.
4. **Act**: Analyze feedback and continuously refine security policies.

5. Policy Implementation and Enforcement

- **Applicability**: All entities must comply with the **Global ISSP**. Non-compliance should be addressed with corrective action plans or derogation procedures.
- **Publication**: The **Global ISSP** is available to all stakeholders, while operational policies are available internally for employees and contractors.
- **Exemptions**: Requests for exceptions are managed through a formal process, requiring approval by the Global CISO or other relevant authorities.

6. Appendices and Supporting Documents

The **Global ISSP** is supported by a series of **Operational Policies** that address specific aspects of information security, such as:

- **Human Resource Security**
- **Logical Access Control**
- **Network Security**
- **Cloud Security**
- **Incident Management**
- **Business Continuity**

7. Continuous Improvement and Compliance

The policy highlights the importance of continuous improvement and compliance through periodic reviews, audits, and employee training. These activities are critical for adapting to new security challenges and ensuring ongoing protection of the company's information assets.

8. Roles and Responsibilities

The **Global CISO** and **OG SOs** are key figures in the security governance structure. They are responsible for:

- Approving and enforcing security measures.
- Monitoring compliance within their assigned areas.
- Liaising with external parties, including government agencies and security groups, when necessary.

9. Incident Management and Business Continuity

The **ISSP** outlines procedures for managing security incidents and ensuring business continuity. Regular testing and maintenance of these processes are crucial to the company's resilience against cyber threats.

This policy ensures a robust information security framework that aligns with international standards (such as ISO 27001) and supports the operational needs of INFOTECH SERVICE FZ-LLC. It emphasizes governance, compliance, and continuous improvement to protect the company's digital infrastructure and data.