IT Policy and Procedures for Evertec General Trading Company Ltd

Evertec General Trading Company Ltd recognizes the ever-increasing significance of information technology (IT) in its daily operations. This IT Policy and Procedures document serves as a comprehensive framework that governs the use of IT resources to ensure the security, reliability, and ethical use of technology within the organization.

1. Purpose

The primary purpose of this policy is to establish a robust structure that defines the acceptable usage and management of IT resources, with the overarching objectives of enhancing productivity, minimizing risks, and protecting sensitive information.

2. Scope

This policy is applicable across all aspects of IT, including hardware, software, data management, and network infrastructure. It applies to all employees, contractors, and third parties involved with Evertec General Trading Company Ltd.

3. IT Security

Evertec places the highest importance on securing its IT assets and data. To this end, the policy outlines the following:

- Data Encryption: The encryption of sensitive data in transit and at rest to prevent unauthorized access.
- Password Management: Guidelines for creating strong passwords and enforcing periodic changes.
- Access Controls: Implementing role-based access controls and regular audits to ensure data security.
- Incident Response: Procedures for reporting, addressing, and mitigating cybersecurity incidents in a timely and efficient manner.

4. IT Asset Management

Efficient IT asset management is essential to ensure the optimal performance and longevity of equipment. The policy includes procedures for:

- Procurement: Guidelines for the acquisition of IT assets, including vendor selection and budget considerations.
- Maintenance: Scheduled maintenance, upgrades, and repairs to ensure equipment reliability.
- Disposal: Proper disposal of outdated equipment, including data sanitization to prevent data breaches.

5. Software Usage

Evertec emphasizes legal compliance and protection against malware through guidelines for:

- Software Installation: Procedures for authorized software installation and updates.
- Licensing: Ensuring that all software used is properly licensed.
- Usage: Defining acceptable software usage and the consequences of unlicensed or unauthorized usage.

6. Data Management and Backup

Effective data management is critical for the security and continuity of operations. The policy addresses:

- Data Classification: Categorizing data based on sensitivity and outlining protection measures.
- Storage: Guidelines for secure data storage, with access controls and encryption.
- Backup and Recovery: Regular backup schedules and disaster recovery plans to ensure data integrity and availability.

7. Network and Internet Usage

Acceptable network and internet usage policies are defined to safeguard network integrity, data privacy, and compliance with regulatory requirements. This includes:

- Internet Access: Guidelines for appropriate internet usage, including social media and personal email.
- Network Security: Measures to protect the network from unauthorized access and threats.
- Regulatory Compliance: Ensuring compliance with laws and regulations concerning network usage.

8. IT Training and Awareness

Evertec promotes IT training opportunities for employees and encourages staying updated on emerging IT trends and best practices. An informed workforce is vital for the organization's growth and security.

9. Compliance and Legal Obligations

The policy emphasizes the importance of aligning IT operations with legal and regulatory requirements. This includes:

- Compliance Mechanisms: Outlining how the company will ensure adherence to relevant regulations.
- Consequences of Non-Compliance: Penalties for non-compliance and violations of the IT policy.

10. Monitoring and Audit

Evertec reserves the right to monitor IT resources, conduct audits, and investigate potential violations of this policy to maintain security and compliance. This includes the procedures for auditing, reporting, and addressing violations.