### **Task 4: Risk Management Plan for Viet Phat Transport**

#### **1. Define the Scope & Objectives of Risk Management**

Scope:

The scope of risk management at Viet Phat Transport encompasses all aspects of the company's operations related to transportation and logistics, particularly focusing on IT systems such as fleet management, GPS tracking, transportation management, CRM software, and supply chain management. The primary focus is on safeguarding data integrity, ensuring cybersecurity, and maintaining system reliability.

Objectives:

* To protect sensitive company and customer data from cyber threats.
* To ensure continuous operation and reliability of IT systems.
* To comply with relevant national laws and regulations regarding cybersecurity, personal data protection, and IT standards.
* To prevent unauthorized access and mitigate potential vulnerabilities within the company’s systems.
* To maintain customer trust by ensuring secure electronic transactions and data handling.

#### **2. Identify the Stakeholders & Their Responsibilities**

Stakeholders:

1. Management Team:
   * Responsibilities: Oversee the implementation of risk management strategies, allocate resources, and ensure compliance with laws and regulations.
2. IT Department:
   * Responsibilities: Implement and maintain cybersecurity measures, perform regular updates and security checks on IT systems, and manage data encryption and storage.
3. Compliance Officer:
   * Responsibilities: Monitor adherence to relevant laws and regulations, conduct audits, and ensure all legal requirements are met.
4. Employees:
   * Responsibilities: Follow best practices for cybersecurity, report suspicious activities, and adhere to company policies on data protection.
5. Customers:
   * Responsibilities: Provide accurate information for transactions and follow security protocols advised by the company.

#### **3. Recommendations to Address the Root Causes of Incidents**

Incident 1: Data Leak Incident

* Root Cause: Inadequate cybersecurity measures.
* Recommendation: Implement robust firewalls, intrusion detection systems, and regular security audits. Conduct employee training on data protection and cybersecurity awareness.

Incident 2: System Downtime Due to Cyberattack

* Root Cause: Insufficient protection against DDoS attacks.
* Recommendation: Deploy DDoS protection services, monitor network traffic for unusual patterns, and develop an incident response plan to quickly mitigate attacks.

Incident 3: GPS System Hacked

* Root Cause: Failure to update and secure the software.
* Recommendation: Ensure regular software updates and patches, conduct security assessments on the GPS system, and implement strong encryption protocols.

Incident 4: Unauthorized Access to Fleet Management System

* Root Cause: Weak passwords and lack of multi-factor authentication.
* Recommendation: Enforce the use of strong, unique passwords and implement multi-factor authentication (MFA) for all system access points.

#### **4. Recommendations to Comply with Regulation Requirements**

Law on Cyber Information Security: Data Security

* Requirements: Implement robust cybersecurity measures.
* Recommendation: Establish a comprehensive cybersecurity framework, including firewalls, encryption, and regular vulnerability assessments. Conduct regular training for employees on cybersecurity practices.

Decree 63/2016/ND-CP: Personal Data Protection

* Requirements: Secure customers' personal data in electronic transactions and information storage.
* Recommendation: Encrypt all personal data, implement secure data storage solutions, and conduct regular audits to ensure compliance with data protection standards.

Law on Information Technology: IT Standards Compliance

* Requirements: Adhere to national IT standards for security and efficiency.
* Recommendation: Follow national and international IT standards (e.g., ISO/IEC 27001), regularly review and update IT policies, and ensure all systems are compliant with these standards.

Decree 52/2013/ND-CP on E-commerce: Transaction Security

* Requirements: Secure electronic transactions and protect consumer rights.
* Recommendation: Implement SSL/TLS for all online transactions, ensure secure payment gateways, and educate customers on safe transaction practices.

.