IFS INTERNATIONAL FREIGHT SOLUTIONS

INTERNATIONAL
FREIGHT SOLUTIONS INC

3024 49 Ave SE,
Calgary, AB T2B2X4
☎ 403-971-0085
✉ Info@ifs-transport.com
www.ifs-transport.com

INFORMATION SECURITY POLICY

Version: 1.0
Effective Date:08 Aug, 2023
Approved by: Navjot Singh

1. Introduction

International Freight Solutions (IFS) is committed to maintaining the confidentiality, integrity, and availability of its information assets. This Information Security Policy outlines the principles, responsibilities, and expectations for protecting sensitive company data, customer information, and operational systems from security threats.

2. Purpose

The purpose of this policy is to:

- Ensure the protection of sensitive business, employee, and customer information.
- Safeguard the integrity and confidentiality of data across all business functions.
- Comply with legal, regulatory, and contractual obligations related to information security.
- Minimize risks associated with cyber threats, data breaches, and unauthorized access.

3. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to IFS systems, networks, and data. It covers all IT systems, communication networks, physical documents, and digital records.

4. Policy Statements

4.1 Leadership Commitment

Senior management fully supports and enforces this policy to establish a culture of security within the organization.

4.2 Access Control

- Access to company information and systems will be granted based on job role and business necessity.
- Strong authentication mechanisms (e.g., passwords, multi-factor authentication) must be in place.
- Employees must not share credentials or allow unauthorized access.

4.3 Data Protection

- Sensitive data must be encrypted during transmission and storage.
- Only authorized personnel may handle confidential or restricted data.
- Employees must adhere to data classification guidelines.

4.4 Network and System Security

- Firewalls, intrusion detection systems, and antivirus software must be maintained and updated regularly.
- Unauthorized devices and software are prohibited from connecting to the company network.
- Regular security audits and vulnerability assessments must be conducted.

4.5 Incident Response

- A documented incident response plan must be in place.
- All security incidents must be reported immediately to IT Security.
- Investigations and remediation actions must be conducted promptly.

4.6 Employee Awareness and Training

- All employees must undergo regular security awareness training.
- Employees are responsible for recognizing phishing attempts, social engineering attacks, and other threats.

4.7 Third-Party Security

- Vendors and partners must comply with IFS security requirements.
- Third-party contracts must include information security clauses.

4.8 Compliance and Auditing

- IFS will comply with all relevant industry standards, such as ISO 27001, GDPR, and other transportation regulations.
- Regular audits will be conducted to ensure compliance.
-

5. Policy Enforcement

- Violations of this policy may result in disciplinary actions, including termination of employment.
- Legal action may be taken against individuals or entities that compromise IFS security.

6. Review and Updates
This policy will be reviewed annually or as needed to address emerging security threats and regulatory changes.

Approved By:
Navjot Singh
Director
08 Aug,2023