Policy Guidance Document	Information Security Policy			
Department	Information Technology		Effective Date	Jan 1, 2020
Document Change Status				
Version Number	Date	Change Request By	Change Approver	Change Type
2.0	Jan 01, 2020	IT Team	HR	Revised Documentation

Information Security Policy

1. Overview

Shiprocket, handles customer information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect customer privacy, to ensure compliance with various regulations and to guard the future of the organization. BFRS commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process customer information so that we can meet these promises.

2. Scope

All employees, interns, consultants, and other workers at Shiprocket, including all personnel affiliated with third parties must adhere to this policy.

3. General Requirements

Employees handling Sensitive customer data should ensure:

- Handle Company and customer information in a manner that fits with their sensitivity;
- Limit personal use of Shiprocket information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Shiprocket reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal; ● Do not disclose personnel information unless authorized;
- Protect sensitive customer information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including pen drives, portable disks, hotspot and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive customer data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally/CTO.

4. **Roles and Responsibilities**

Chief Technology Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:
  - Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
  - The IT Administrator shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

5. **System and Application Administrators shall:**

- Monitor and analyze security alerts and information and distribute to appropriate personnel administer user accounts and manage authentication.
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.

The Human Resources Officer (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- Facilitating participation upon hire.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand BFRS's information security policy.

Financial Controller or CS (or equivalent) will ensure that for service providers with whom customer information is shared:

- Written contracts require adherence to PCI-DSS by the service provider.
- Written contracts include acknowledgement or responsibility for the security of customer data by the service provider.

6. **Security Awareness and Procedures:**

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.
- All employees that handle customer information will undergo background checks before they commence their employment with BFRS.
- All third parties with access to customer data are contractually obligated to comply BFRS InfoSec policies.
- Company security policies must be reviewed annually and updated as needed.

7. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious software, a competitor, or a disgruntled employee, and their intention might be to steal information or data, or just to damage our company.

The Incident response plan must be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members and take steps to ensure that they understand it and what is expected of them.

Employees will be expected to report to the CTO for any security related issues. Shiprocket security incident response plan is as follows:

- Each department must report an incident to the IT Administrator (local issue)/DevOps Manager (cloud/platform issue).
- That member of the team receiving the report will advise the Management Team (CTO/CBO/COO) of the incident.
- The Management Team (Response Team) will investigate the incident and assist the potentially compromised department in limiting the exposure of customer data and in mitigating the risks associated with the incident.
- The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (merchant, customer, logistics company, etc.) as necessary.
- The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
- If an unauthorized wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the IT Administrator or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
- A department that reasonably believes it may have an account breach, or a breach of customer information or of systems related to the environment in general, must inform BFRS Incident Response Team. After being notified of a compromise, the Response Team, along with other designated staff, will implement the Incident Response Plan to assist and augment departments' response plans.

8. Shiprocket PCI Security Incident Response Team: (Update as applicable):

- CTO
- Compliance Officer
- IT Admin
- DevOps Manager
- Merchant Services

I. Escalation Members:

- First Level
  - IT Admin
  - DevOps Manager
  - Merchant Services Escalation
- Second Level
  - Compliance Officer
  - CTO
  - CEO
- External Contacts (as needed)
  - Courier SPOC
  - Payment Gateway SPOC
  - Merchant SPOC
  - Internet Service Provider (if applicable)
  - Internet Service Provider of Intruder
  - Partners
  - Insurance Carrier
  - Law Enforcement Agencies as applicable inn local jurisdiction.

9. In response to a systems compromise, the Response Team and designees will:

- Ensure compromised system/s is isolated on/from the network.
- Gather, review and analyze the logs and related information from various central and local safeguards and security controls.
- Conduct appropriate forensic analysis of compromised system.
- Contact internal and external departments and entities as appropriate.
- Make forensic and log analysis available to appropriate law enforcement or security personnel, as required.
- Assist law enforcement and security personnel in investigative processes, including in prosecutions.

The Company reserves the right to amend, suspend or withdraw this policy, guidance and procedure at any time without notice. Further, the Company reserves the right to administer discipline in such a manner as it deems appropriate to the circumstances, and may, in its sole discretion, eliminate any or all the steps.

*** End of Document***