

Information Security Policy

Anjani Finance Limited

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

The Company handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Company 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 cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of Company information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Company 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 authorised;
- Protect sensitive cardholder 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 unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Company's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. The Company will maintain an approved list of technologies and devices and personnel with access to such devices.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they can not be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Protect Stored Data

- All sensitive cardholder data stored and handled by Company and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by Company for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

5. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Company if disclosed or modified. **Confidential data includes cardholder data.**
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

6. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up

tapes, computer hard drive, etc.

- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on Company sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

7. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL,TLS,IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

8. 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 (see Appendix A)
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

9. Network security

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- Stateful Firewall technology must be implemented where the Internet enters the Company Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented
- The Company will have firewalls between any wireless networks and the cardholder data environment.
- The Company will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- The Company have to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

10. Roles and Responsibilities

- Chief Security 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 analysing 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 Information Technology Office (or equivalent) 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).
- System and Application Administrators shall:
 - monitor and analyse 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 Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:
 - Facilitating participation upon hire and at least annually.
 - Ensuring that employees acknowledge in writing at least annually that they have read and understand the Company's information security policy.
- General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:
 - Written contracts require adherence to PCI-DSS by the service provider.
 - Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.