FINANCIAL INFORMATION SECURITY POLICY

Contents

Section	Title
1.	Introduction
2.	Information Security Policy
3.	Network Security
4.	Acceptable Use
5.	Physical Security
6.	Access to the Sensitive Cardholder Data
7.	Protect Data in Transit
8.	Disposal of Stored Data
9.	Security Awareness and Procedures
10.	Credit Card (PCI) Security Incident Response Plan
11.	Transfer of Sensitive Information Policy
12.	User Access Management
13.	Access Control Policy

1. Introduction

This policy sets out Inspectahire Instrument Company Ltd.'s arrangements for protecting confidential financial and payment information. It applies to employees and other authorised persons who handle, process or have access to sensitive financial or cardholder information.

2. Information Security Policy

Inspectahire is committed to protecting financial and cardholder information from unauthorised access, disclosure, alteration, loss or misuse. Appropriate technical, organisational and physical safeguards will be maintained according to the sensitivity of the information and applicable legal, regulatory and contractual requirements.

Inspectahire respects the privacy and confidentiality of its customers and is committed to maintaining a secure environment for the processing and handling of financial and payment information. Access to such information will be restricted to authorised personnel with a legitimate business need.

Employees and authorised personnel are responsible for:

- Protecting confidential financial and payment information from unauthorised access, disclosure, loss or misuse.
- Accessing financial information only where required for their authorised duties.
- Keeping passwords and other authentication credentials secure and not sharing them with others.
- Ensuring sensitive financial information is not left unattended or accessible to unauthorised persons.
- Following Company requirements for the secure storage, transmission, retention and disposal of financial information.
- Using only Company-approved systems, equipment and methods when processing or transmitting sensitive financial information.
- Reporting suspected or actual information security incidents, loss of information, unauthorised access, phishing attempts or other security concerns promptly to their line manager and/or the appropriate Company contact.
- Complying with relevant Company information security, data protection and Information Technology requirements.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. To support this policy compliance to the company Data and Privacy Policy is required.

3. Network Security

Inspectahire maintains appropriate technical security controls to protect Company systems and financial information from unauthorised access, loss, misuse and cyber threats.
Network and Information Technology security is managed with support from the Company's appointed Information Technology service provider. Appropriate controls include firewalls, endpoint protection, access controls, secure authentication, software and security updates, and monitoring appropriate to the Company's systems and level of risk.

Access to systems containing sensitive financial information is restricted according to business need and authorised user access. Changes to network infrastructure, security configurations or connections must be appropriately authorised and managed.
Security vulnerabilities and identified risks are addressed through the Company's Information Technology support and information security arrangements, with appropriate action taken where weaknesses or incidents are identified.

4. Acceptable Use

Company Information Technology systems, equipment, networks and information must be used responsibly and in accordance with Company policies and authorised business purposes.

Employees and other authorised users must:

• Use only Company-approved systems, software, devices and services for processing or accessing sensitive financial information.

• Keep passwords, authentication credentials and security information confidential and must not share them with other persons.

• Take reasonable precautions to prevent unauthorised persons from viewing or accessing confidential financial information.

• Lock or secure devices when left unattended and ensure sensitive information is not unnecessarily displayed, printed or left unsecured.

• Not install unauthorised software, alter security settings or connect unauthorised equipment to Company systems or networks.

• Exercise appropriate caution when opening email attachments, following links or responding to unexpected requests for financial, payment or account information.

• Not transmit sensitive financial or payment information using unapproved communication methods or personal accounts.

• Promptly report suspected phishing, malware, unauthorised access, loss of equipment or information, or any other suspected information security incident.

• Comply with the Company's Information Technology, information security and data protection requirements at all times.
Company systems and equipment may be monitored and managed as necessary to maintain security, investigate suspected misuse and meet legal, regulatory and contractual requirements.

5. Physical Security

Physical access to areas, equipment and records containing sensitive financial information is restricted to authorised personnel as appropriate.

Sensitive financial records must be stored securely when not in use and must not be left unattended where they could be accessed or viewed by unauthorised persons.

Printed financial or payment information must be collected promptly from printers and stored securely where retention is required. Documents containing sensitive information must be disposed of securely when no longer required, using appropriate confidential waste or shredding arrangements.

Company computers and other devices used to access financial information must be appropriately secured when unattended. Employees must take reasonable precautions to prevent loss, theft or unauthorised access to Company equipment and information.

Visitors and other unauthorised persons must not be permitted unsupervised access to sensitive financial information, systems or restricted areas.

Any loss, theft or suspected unauthorised access involving financial information, records or Company equipment must be reported promptly in accordance with the Company's information security incident reporting arrangements.

6. Access to the Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is not to be shared.
- Inspectahire will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.
- Inspectahire will have a process in place to monitor the PCI DSS compliance status of the Service provider.

7. Protect Data in Transit

Sensitive financial and payment information must be protected when transmitted or transferred and only Company-approved methods may be used.

Employees must ensure information is sent only to the intended authorised recipient. Secure or encrypted methods must be used where appropriate or required. Unexpected requests for financial information, bank details or changes to payment arrangements must be independently verified before any information is disclosed or action taken.

Any suspected loss, misdirection or unauthorised disclosure of sensitive financial information must be reported promptly.

8. Disposal of Stored Data

Financial and payment information must be securely disposed of when it is no longer required, in accordance with the Company's data retention requirements.

Paper records containing sensitive information must be securely shredded or disposed of through approved confidential waste arrangements.

Electronic information and storage media must be securely deleted, wiped or destroyed as appropriate to prevent unauthorised recovery of sensitive information.

Information awaiting secure disposal must be appropriately protected from unauthorised access.

This keeps the important controls without committing Inspectahire to unnecessary technical processes that may not reflect what you actually do.

9. Security Awareness and Procedures

Employees are made aware of their responsibilities for protecting financial and payment information through relevant Company policies, procedures, training and communications.

Personnel with access to sensitive financial information must understand the security requirements relevant to their role and promptly report any suspected security concerns or incidents.

Relevant information security policies and procedures will be periodically reviewed and updated where necessary to reflect changes in business activities, risks or applicable requirements.

This is enough for the policy without claiming that you hold specific security awareness meetings or provide formal Payment Card Industry training to everyone.

10. Credit Card (PCI) Security Incident Response Plan

Any actual or suspected loss, unauthorised access, disclosure or compromise of financial or payment information must be reported immediately to the appropriate line manager or senior management.

The incident will be assessed promptly, with appropriate action taken to contain the issue, protect affected information and prevent further unauthorised access or loss.

Relevant internal personnel, the Company's Information Technology provider, payment service provider, bank, insurer, regulatory authorities or law enforcement will be contacted where appropriate to the nature and severity of the incident.

Following an incident, the cause and effectiveness of the response will be reviewed and any necessary corrective actions, procedural changes or additional safeguards implemented.

11. Transfer of Sensitive Information Policy

Sensitive financial and payment information may only be shared with authorised third parties where there is a legitimate business requirement. Before information is shared, appropriate consideration must be given to the security and suitability of the third party and any applicable contractual, legal or regulatory requirements.

Third parties with access to sensitive financial or payment information are expected to maintain appropriate security controls and use the information only for the authorised purpose. Any concerns regarding the security or handling of information by a third party must be reported to management and investigated as appropriate.

12. User Access Management

Access to Company systems and financial information is provided according to an individual's role and legitimate business requirements. New user access and any additional permissions must be appropriately authorised by management and implemented through the Company's Information Technology support provider. Each user must have their own unique account and authentication credentials. User accounts and passwords must not be shared.

Access rights must be amended where an employee's role or responsibilities change and removed promptly when access is no longer required. When an employee leaves the Company, relevant management will ensure that the Information Technology support provider is notified so that system access can be revoked.

13. Access Control Policy

Access to Company systems and information must be appropriately controlled to prevent unauthorised access, disclosure, alteration or loss.

Access rights will be based on the principles of least privilege and business need, with users provided only with the level of access necessary to perform their authorised duties. Privileged or administrative access must be restricted to appropriately authorised personnel and managed with support from the Company's Information Technology service provider.

Users must authenticate using their own authorised account and must keep passwords and other authentication credentials secure. Remote access to Company systems must use approved and appropriately secured methods.

Access rights will be reviewed and amended where necessary to reflect changes in roles, responsibilities or business requirements. Any suspected unauthorised access or misuse of Company systems must be reported promptly.

Authorised by:

Cailean Forrester (Sep 8, 2026 13:57:48 GMT+1)

Name: Cailean Forrester
Title: Managing Director
Date: 08/09/2026 (Review period 13 Months)

Financial Information Security Policy 2026 - 2027 - POL 14 Rev 02

Final Audit Report 2026-09-08

Created:	2026-09-07
By:	Lillian Paterson (lillianpaterson@inspectahire.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA948dXOk6DPMioAK0wBI1EmHrl8LeljPt

"Financial Information Security Policy 2026 - 2027 - POL 14 Rev 02" History

Document created by Lillian Paterson (lillianpaterson@inspectahire.com)
2026-09-07 - 10:32:15 AM GMT

Document emailed to Cailean Forrester (caileanforrester@inspectahire.com) for signature
2026-09-07 - 10:32:20 AM GMT

Email viewed by Cailean Forrester (caileanforrester@inspectahire.com)
2026-09-08 - 12:57:24 PM GMT

Document e-signed by Cailean Forrester (caileanforrester@inspectahire.com)
Signature Date: 2026-09-08 - 12:57:48 PM GMT - Time Source: server - Signature Appearance Selected: DRAW

Agreement completed.
2026-09-08 - 12:57:48 PM GMT