GCI FINANCIAL LIMITED

Cyber Security Policy

Contents

1. Introduction

GCI Financial Limited is committed to maintaining a secure and protected environment for its operations, clients, and employees. This Cyber Security Policy outlines the measures and guidelines that all employees, contractors, and third-party vendors must adhere to in order to safeguard our information systems and data assets from cyber threats.

2. Objective

The objective of this policy is to establish a comprehensive framework to identify, prevent, detect, and respond to cyber security risks. It aims to protect the confidentiality, integrity, and availability of information assets, maintain business continuity, and ensure compliance with applicable laws and regulations.

3. Roles and Responsibilities

3.1 Management Responsibilities

Executives and senior management will provide clear direction and support for cyber security initiatives. Designated individuals will be responsible for overseeing the implementation, monitoring, and review of the policy.

Adequate resources will be allocated to maintain an effective cyber security program.

3.2 Employee Responsibilities

All employees must familiarize themselves with this policy and comply with its provisions.

Employees are responsible for reporting any suspected or actual cyber security incidents promptly to the designated authority.

Awareness training will be provided to employees to ensure they understand their role in maintaining a secure environment.

4. Risk Assessment and Management

Regular risk assessments will be conducted to identify vulnerabilities, threats, and potential impacts on information assets.

Appropriate controls and safeguards will be implemented to mitigate identified risks.

Risk management strategies will be reviewed periodically and updated to reflect emerging threats.

The company has identified the following vulnerabilities, threats, and potential impacts:

Access Control

Access to information systems, networks, and data will be granted based on the principle of least privilege.

User access rights will be regularly reviewed, modified, and revoked when necessary.

Multi-factor authentication will be implemented for privileged accounts and sensitive systems.

Information Security

Information assets, including client data, will be classified based on their sensitivity and appropriate security controls will be implemented. Please refer to the Information Security Policy.

Encryption will be used to protect data in transit and at rest.

Secure coding practices will be adopted in software development processes.

Incident Response and Reporting

An incident response plan will be established to ensure timely identification, containment, eradication, and recovery from cyber security incidents. All employees must report any suspected or actual security incidents immediately.

Incident response procedures will be tested periodically through simulations and drills.

Data Privacy

GCI Financial Limited will comply with all applicable data protection laws and regulations.

Client and employee data will be collected, processed, and stored securely and in accordance with the organization's privacy policies.

Vendor Management

Third-party vendors will be assessed for their cyber security capabilities before engaging their services. Contracts with vendors will include provisions that address their cyber security responsibilities and data protection obligations.

Employee Awareness and Training

Regular awareness programs and training sessions will be conducted to educate employees about cyber security best practices. Employees will be updated about emerging threats and vulnerabilities through regular communication channels.

Compliance and Audit

Compliance with this policy and related procedures will be thoroughly monitored and enforced.

Periodic audits and assessments will be conducted to evaluate the effectiveness of the cyber security program and identify areas for improvement.