Integrated Management System (IMS)

Cyber Security Policy

Table of Contents

1 Introduction

At Red Funnel Ferries, we recognize the importance of cybersecurity in protecting our systems, data, and customers. This Cybersecurity Policy outlines our commitment to maintaining a secure environment and the responsibilities of employees and stakeholders in safeguarding our digital assets.

2 Scope

This policy applies to all employees, contractors, and third parties who have access to Red Funnel Ferries' information systems, networks, and data.

3 Security Controls

3.1 Access Control

- Access to information systems and data will be granted on a need-to-know basis.
- User access privileges will be regularly reviewed and updated as necessary.
- Strong authentication mechanisms, such as multi-factor authentication, will be implemented where appropriate.

3.2 Data Protection

- Data will be classified based on its sensitivity and criticality.
- Encryption will be used to protect data both in transit and at rest.
- Data backups will be performed regularly, and backup copies will be stored securely.

3.3 Network Security

- Firewalls, intrusion detection/prevention systems, and other security controls will be implemented to protect our network infrastructure.
- Wireless networks will be secured using encryption and access controls.

3.4 Endpoint Security

- Antivirus software and endpoint detection and response (EDR) solutions will be deployed on all devices.
- Devices will be regularly patched and updated to address security vulnerabilities.

4 Incident Response

4.1 Reporting

- All employees are responsible for promptly reporting any cybersecurity incidents or suspicious activities to the IT department or designated security personnel.

4.2 Incident Handling

- An incident response plan will be developed and maintained to guide the response to cybersecurity incidents.
- The IT department will lead the response efforts, coordinating with relevant stakeholders and authorities as necessary.

5 Security Awareness

5.1 Training

- All employees will receive cybersecurity awareness training upon hire and periodically thereafter.
- Training will cover topics such as phishing awareness, password security, and data handling best practices.

5.2 Communication

- Regular communications will be issued to employees to reinforce cybersecurity policies and promote awareness of emerging threats.

6 Compliance and Governance

6.1 Compliance

- This policy will comply with relevant cybersecurity laws, regulations, and industry standards.
- Regular audits and assessments will be conducted to ensure compliance with this policy and other applicable requirements

6.2 Governance

- A cybersecurity governance framework will be established to provide oversight and accountability for cybersecurity initiatives.
- The Head of IT will lead the governance efforts and report to senior management on cybersecurity matters.

7 Responsibilities

7.1 Management

- Senior management will provide support and resources to ensure the effective implementation of this policy.

- Management will lead by example in adhering to cybersecurity best practices and promoting a culture of security awareness.

7.2 Employees

- All employees are responsible for complying with this policy and maintaining the security of Red Funnel Ferries' digital assets.

- Employees should report any security concerns or potential vulnerabilities to the appropriate channels.

8 Review and Revision

This policy will be reviewed periodically and updated as necessary to address evolving cybersecurity threats and changes in business operations.

9 Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

9 Contact Information

For questions or concerns regarding this Cybersecurity Policy, please contact the IT department.