SOUTH COAST
PORT SERVICES

Security Policy.

1. Overview.
The purpose of this policy is to establish and promote the security practices necessary to protect the confidentiality, integrity, and availability of the company's information assets.

1.2 This policy applies to all employees, contractors, consultants, temporary staff, and third-party vendors / customers who have access to the company's information systems and data.

1.3 The company is committed to safeguarding its information assets against unauthorised access, disclosure, alteration, destruction, or theft. All personnel must adhere to this policy to ensure the security and privacy of company data.

2. Roles and Responsibilities.
2.1 Management: Ensure the resources and support for security initiatives.

2.2 Divisional Operation Manager's incorporate the role of Security Officer and are accountable for the implementation / monitoring / Auditing of all company security initiatives and compliance. Additionally, to customer / client system resources.

2.3 IT Department: Implement security controls, monitor systems, and respond to incidents.
This includes the company's external professional support – IT Consultant
(Online Facilities Management LTD. Company Registration 07122430)

2.4 Employees and Users: Follow security policies and report security incidents, and complete the annual refresher training pertaining to own areas of security / data integrity.

2.5 GDPR Company Controller and Divisional GDPR Officers – Manage, maintain, and Audit GDPR protection practices and security, as well as investigating breaches and carrying out DSAR compliance.

2.6 HR Business Partner: provides security - HR governance, stewardship of policies and procedures, cross over Workflow of secured information / data in conjunction with customer on behalf of the company.

3. Information Classification.
3.1 All information must be classified into categories such as:

- Public: Information that can be shared freely. Published on company website and Customs House.
- Internal Use Only: Information intended for internal staff.
- Confidential: Sensitive information requiring strict access controls.
- Restricted: Highly sensitive information requiring the highest level of security.

4. Access Control.
4.1 Access to information systems shall be granted based on the principle of least privilege.

4.2 User accounts must be unique, and passwords must meet complexity requirements.

4.3 Access rights shall be reviewed regularly.

5. Data Protection.
5.1 Sensitive data must be encrypted both in transit and at rest.

5.2 The company use Data flows into and out of devices through what we call ports. A firewall is what controls what is - and more importantly isn't - allowed to pass through those ports. The firewall allows very little, if any, inbound traffic. There's rarely any legitimate reason for other devices to connect to any company device, or home network, unsolicited.

5.3 Data backups shall be performed regularly and stored securely.

5.4 Data retention and disposal procedures must comply with legal and company requirements.

6. Incident Management.
6.1 All security incidents must be reported immediately to the IT/security team.

6.2 Incidents will be documented, investigated, and remediated promptly.

6.3 Lessons learned will be integrated into security practices.

7. Physical Security.
7.1 Access to physical facilities shall be restricted to authorised personnel.

7.2 Sensitive hardware and storage devices must be secured and monitored.

8. Security Awareness and Training.
8.1 All staff shall receive regular security awareness training.

8.2 Employees should be aware of phishing, social engineering, and other common threats.

9. Compliance.
9.1 The company shall comply with relevant laws, regulations, and contractual obligations.

9.2 Regular audits and assessments shall be conducted to ensure compliance.

10. Summary.
10.1 Violations of this policy may result in disciplinary action, including termination of employment or legal action.

10.2 This policy shall be reviewed annually or upon significant changes within the company security practices, or regulatory requirements.

11. Additional Security Information Guidance / Reference points.
- Business Continuity Policy and Procedure.
- Criminal Finances ACT 2017 Policy and Procedure.
- Cyber Security Policy and Procedure.
- Controlled Security Measure - Confidentiality Statement / Email / Security Disclaimer for IT and Email.
- Anti-Virus protection emailware.

- Contract of Employment / Terms and Conditions / Job Description/ Confidentiality Agreements.
- Due Diligence Policy and Procedure.
- External Security / IT / Company Safeguarding – (Online Facilities Management Ltd, Company Registration 07122430)
- Internal – Security / IT Safeguarding GDPR Officer – Accountability / Role Responsibility. Annual Audit.
- General Data Protection Regulations 2018 Policy and Procedure.
- General Data Protection – Data Subject Access Request – Policy and Procedure.
- General Data Protection Privacy Policy and Procedure.
- General Data Protection Privacy and use of Cookies Policy and Procedure. /
- General Data Protection Data Retention Policy and Procedure.
- General Data Protection Special Category Data Privacy Policy and Procedure.
- Occupational Health -Medical Surveillance confidentiality / Security of Records Agreement.
- 2012 Health and Social Care Act – IT Protection of Medical Information.
- Remote Working - Security Measures & Audit / IT Protection / Working Agreement.
- Risk Management / Internal
- Social Media Policy and Procedure.
- Service Level Agreement.
- Terminal and Port Security Policy and Procedure.
- Use of Mobile Phone Policy and Procedure.

Approved by: Martin Eardley.
Managing Director.
Effective Date: 01.04.2025
Review Date: 27.03.2026