INFORMATION SECURITY POLICY

INTRODUCTION

Tayside Contracts recognise that information is a valuable asset, essential in supporting the organisation's vision and the delivery of business functions and customer services and must be adequately protected against loss or compromise.

Effective information security management is vital to safeguarding our information from unauthorised use, modification, disclosure or destruction, thereby maintaining Tayside Contracts' reputation and demonstrating integrity in dealing with employees, business partners, regulators and the public.

This Policy is a core part of our Information Governance Framework and sets out Tayside Contracts' commitment and approach to protecting our information from security threats, whether internal or external, deliberate or accidental.

SCOPE

This policy applies to:

- all employees of Tayside Contracts, third party organisations or contractors and anyone else who is authorised to access and use Tayside Contracts' information and related physical and ICT facilities, systems or services;

- all information held by Tayside Contracts which includes information stored in the following formats - on printed media (e.g. forms, reports, documents, records, books), on computers and networks, on magnetic or optical storage media (e.g. hard drive, tape, CD, USB), in physical storage environments (e.g. offices, filing cabinets, drawers), on CCTV or other video and audio formats; and

- information accessed on or from any Tayside Contracts' premises, accessed off-site, for example when travelling, working from home, in a public area or on third party premises and accessed using Tayside Contracts' computer equipment or on an individual's own devices.

EMPLOYEE RESPONSIBILITIES

All employees and contractors are responsible for ensuring that they are familiar with and comply with all relevant policies, procedures and guidance. They are expected to take all reasonable steps to protect Tayside Contracts' information from unauthorised use, modification, disclosure or destruction and must report any suspected or actual security weakness, threats, events or incidents in line with the Tayside Contracts' breach management procedure.

POLICY COMMITMENT

Tayside Contracts is committed to protecting its information assets in line with the three principles of information security. These are:

- **Confidentiality:** protection of information from unauthorised disclosure.
- **Integrity:** safeguarding the accuracy and completeness of information.
- **Availability:** ensuring that information and associated services are available to users when required.

IMPLEMENTATION

To deliver on this commitment in practice, Tayside Contracts will establish and maintain adequate technical and organisational information security measures and controls, taking a proportionate, risk-based approach, e.g.;

- Information security risks will be identified for all information assets and control(s) put in place to prevent and minimise the impact of information security incidents.
- ICT systems and information use will be monitored to protect the confidentiality, integrity and availability of information assets.
- Physical access to buildings and facilities will be monitored and a clear desk policy adopted.
- Information assets vital to the business continuity of Tayside Contracts will be identified in information asset registers and included in Business Continuity plans.
- All breaches of information security will be reported, investigated and appropriate action taken where required.
- Clearly documented information security requirements will be specified and delivered as part of any major change to IT systems and business processes.
- Contractors will be made aware of their responsibilities to adequately protect information through relevant contractual clauses and service level agreements.
- Employee will be made aware of their responsibilities to adequately protect information through their employment contract and Employee Code of Practice.
- Employees will be given the necessary skills and knowledge required to meet these responsibilities through the provision of relevant guidance and training at induction and through employment.

POLICY VIOLATIONS

Failure to comply with this policy may result in individuals being investigated and disciplinary action taken against them in accordance with Tayside Contracts' Disciplinary Policy.

EXTERNAL OPERATING ENVIRONMENT

Compliance with this policy will help us meet the information security requirements and obligations of our external operating environment including:

- Compliance with statutory and regulatory obligations of all organisational functions, for example Health, Safety and Environmental legislation and Financial and Procurement regulations.
- Maintaining relevant security accreditation and certification.
- Contractual requirements with our public and private customers.
- Effective, efficient and compliant information sharing and Partnership working.

Compliance with this policy will help us meet our obligations under the following legislation:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright Patents and Designs Act 1988
- Freedom of Information (Scotland) Act 2002
- General Data Protection Regulation
- Human Rights Act 1998
- Payment Card Industry (PCI) Data Security Standard 3.1
- Surveillance Camera Code of Practice.

RELATED POLICIES

The Information Security Policy links to the following policies which can be accessed on the Intranet, or requested from your line manager or from the HR Admin Team:

- Acceptable use of Social Media Policy
- Data Breach Management Procedure
- Data Protection Policy
- Data Quality Policy
- Employee Code of Conduct
- Information Governance Strategy
- Internet and Email Use Policy
- IT Security Policy
- Records Management Policy.

The above list is not exhaustive.

MONITORING AND COMPLIANCE

Policy compliance and performance improvement will be monitored by the Information Governance Lead, based on an agreed set of key performance indicators, and reported to the Corporate Management Team on an annual basis.

POLICY REVIEW

The Information Security Policy will be reviewed at 3 yearly intervals or sooner if required by legislative or operational changes.

Should you have any queries or require further clarification regarding any aspects of this policy or if you would like this document translated into another language or in another format such as audio or large print then please contact Angie Thompson, Equalities and Communications Manager on 01382 834165 or angie.thompson@tayside-contracts.co.uk