

Information Security Policy

**CONTENTS**

**PAGE**

1. Introduction 3
2. Scope 3
3. Organisational Roles and Responsibilities 4

3.1 Organisational Roles 4

3.2 Organisational Responsibilities 4

1. Policy Framework 5

4.1 Management of Security 5

4.2 Asset Control and Classification 5

4.3 Personnel Security 6

4.4 Physical & Environmental Security 6

4.5 Systems Operational Management 7

4.6 ICT Access Control 7

4.7 Incident Reporting 7

4.8 Business Continuity and Disaster Recovery Plans 8

4.9 Compliance and Audit 8

4.10 Further Information 8

5. Appendix 1 – Information Security Policy Framework 9

1. **Introduction**

This Information Security Policy is a key component of East Ayrshire Leisure’s overall Information Security Management framework and should be considered alongside more detailed information security documentation including: system level security policies, security guidance and protocols or procedures.

The objectives of East Ayrshire Leisure’s Information Security Policy are to preserve:

* **Confidentiality** – access to data will be confined to those with appropriate authority.
* **Integrity** – information will be complete and accurate. All systems, assets and networks will operate correctly, according to specification.
* **Availability** – information will be available and delivered to the right person, at the required time.

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by East Ayrshire Leisure by:

* ensuring that a consistent level of security standards are applied by all employees in order to protect the confidentiality, integrity or availability of the information processed
* ensuring that the processing and security of information complies with statutory obligations and that all East Ayrshire Leisure employees, Trustees etc. are aware of and fully comply with the relevant legislation as described in this and other policies
* describing the principals of security and explaining how they will be implemented within East Ayrshire Leisure, ensuring that all employees, Trustees etc. fully understand their own responsibilities
* creating and maintaining a level of awareness of the need for information security within East Ayrshire Leisure as an integral part of the day to day business, providing a framework to facilitate the application of a standardised approach to security
* ensuring that data compromises or security incidents are quickly identified, impact minimised and the event quickly resolved and repaired
* providing customers with a level of assurance that security of their personal details is regarded as paramount at all times
* protecting information assets under the control and direction of East Ayrshire Leisure and thereby also protecting its reputation

1. **Scope**

This policy describes the information security management principles that are applied to the hardware, software and information assets of East Ayrshire Leisure, access by any party connecting to East Ayrshire Leisure or any party processing or storing information that originates from East Ayrshire Leisure, or is to be fed into it, irrespective of the format. It is supported by asset or task specific policies and procedures which identify the standards to be met in more detail.

This policy follows the general principles outlined within the ISO27000 standards for Information Security Management and relevant legislation such as the Data Protection Act 1998. Asset and task specific policies will be based on guidelines from recognised best practice sources including Communications-Electronics Security Group (CESG), the Cabinet Office and the Scottish Government.

For the purposes of this policy the term ‘employee’ refers to any person who is given access to East Ayrshire Leisure information assets. This includes (but is not restricted to) permanent or temporary employees directly contracted by East Ayrshire Leisure (such as trainees, modern apprentices), or indirectly contracted (such as contractors, consultants, temps, agency staff or volunteers). It also includes Trustees. It is irrespective of whether the work carried out is within East Ayrshire Leisure premises or remotely from a non-authority site.

1. **Organisational Roles and Responsibilities**

**3.1 Organisational Roles**

East Ayrshire Council will establish a Corporate Information Governance Group in order to:

* maintain this policy
* schedule regular independent security health checks, review reports and make recommendations to improve security as necessary
* review requests and risk reports for the addition of a new service or facility or for the upgrade of an existing one
* investigate significant security breaches with the aim of minimising impact and recovering as quickly as possible
* carry out an annual review of security incidents to establish potential trends or security weaknesses and determine corrective action solutions
* review new legislation to identify any areas of non-compliance and produce a corrective action plan to redress as appropriate
* carry out a review of this policy every 2 years to maintain relevance and security levels

The Corporate Information Governance Group will consist of the Data Controller from East Ayrshire Leisure or a nominated individual and any contracted security consultants. The team will meet quarterly to review security in general, special meetings may be held to examine a specific security problem or review a request for a new business system to be implemented within East Ayrshire Leisure.

**3.2 Organisational Responsibilities**

Ultimate responsibility for information security rests with the Chief Executive of East Ayrshire Leisure, but on a day-to-day basis the Data Controller or a nominated individual will be responsible for communicating this policy and related procedures and specifically:

* reporting security breaches to the Corporate Information Governance Group
* working with the Corporate Information Governance Group or their nominated representatives in the investigation and recovery from a security breach or data compromise
* discussing any potential gaps in their ability to comply with this policy with the Corporate Information Governance Group
* submit requests and risk reports for the addition of a new service or facility or for the upgrade of an existing one
* ensuring that the principals of this policy are explicitly incorporated into any outsourcing or third party contract, where it involves assets or information belonging to East Ayrshire Leisure
* maintaining an Information Asset Register which is used by staff to support parts of East Ayrshire Leisure or its business systems

Line managers will be individually responsible for the security of their physical environments where information is processed or stored. Line managers are also responsible for ensuring that their permanent, temporary employees and contractors are aware of:

* the information security policies applicable in their work areas
* their personal responsibilities for information security
* how to access advice on information security matters

All employees will comply with information security procedures including the maintenance of data confidentiality and data integrity. Users who fail to comply with or uphold this policy may be subject to disciplinary action, as set out in East Ayrshire Leisure’s Disciplinary Policy and Procedures appropriate to the employee group concerned.

Each employee will be responsible for the operational security of the information systems they use.

Each system user will comply with the security requirements that are currently in force and will ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to East Ayrshire Leisure’s information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

1. **Policy Framework**

**4.1 Management of Security**

Responsibility for Information Security will reside with the Chief Executive. East Ayrshire Council’s Corporate Information Governance Group will be responsible for implementing, monitoring, documenting and communicating information security requirements for the organisation.

**4.2 Asset Control and Classification**

* + 1. Asset Ownership

Each information asset (hardware, software, application or data) will have a named custodian who will be responsible for the information security of that asset. The Information Asset Register will list all East Ayrshire Leisure information assets and associated risks. The register must record information and/or supporting hardware or software infrastructure and include formal, documented risk management procedures in order to:

* manage the threat of a compromise of confidentiality, integrity or availability of information held on systems or manual records and a strategy to address the threat or reduce the impact
* manage compliance with Data Protection obligations in use of personal data
* manage the risk of removal of information from controlled environments or exchanges of data with third parties
* protect against loss, damage or theft of equipment and/or data therein
* ensure a Risk Register is maintained for each business system

The core principle of risk assessment requires the identification and economic control of risk. The existing methodology requires:

* a general narrative description of the risk including, where possible, a financial assessment of the worst case scenario
* an assessment of the impact of the risk coming to fruition i.e. the immediate difficulties would create (high, medium or low risk) with a narrative to back up the decision reached
* an assessment of the consequences of the risk coming to fruition i.e. the medium to longer term difficulties it would create (high, medium or low risk) with a narrative to back up the decision reached
* a value of the likelihood of the risk coming to fruition (high, medium or low) with a narrative to back up the decision reached
* a value of the risk rating, taking into account all of the foregoing, (high, medium or low) with a narrative to back up the decision reached

Once identified, information security risk will be managed on a formal prioritised basis with action plans put in place to effectively manage those risks. Identified risks will be recorded in the relevant departmental risk register.

Identified risks will be regularly reviewed to identify any emerging threats and/or opportunities for improvement.

* + 1. Classification of Sensitive information

A consistent system for the classification of information within East Ayrshire Leisure enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with other bodies. The Information Classification and Protection Policy defines the baseline standards to be applied to classification of information and information assets with varying degrees of sensitivity and criticality to manage the need for increased protection or handling measures. East Ayrshire Leisure will implement appropriate information classification controls, based upon the results of formal risk assessment and guidance from best practice sources, including CESG, the Cabinet Office and the Scottish Government.

The Data Retention Policy defines how long records are to be held live and archived, environmental conditions for storage areas and approved methods of destruction.

**4.3 Personnel Security**

4.3.1 User Training/Awareness

An Information Security Awareness Training Programme will be included in East Ayrshire Leisure’s induction process. An Information Security Awareness Training Programme will be established and maintained in order to ensure that employee awareness is refreshed and updated as necessary.

**4.4 Physical and Environmental Security**

The Physical and Environmental Policy defines the baseline standards to be applied in order to ensure that information processing facilities, backup and archive storage areas are protected to prevent unauthorised access or avoidable damage to equipment or records.

**4.5 Systems Operational Management**

System operating policies and procedures define the baseline standards to be applied in order to ensure that the information processing facilities, backup and paper record storage areas are built and maintained to prevent unauthorised access or damage to equipment or paper records including:

* Malicious Software and Hacking Policy
* Information Governance Guidelines
  + Remote and Homeworking policy
  + Use of Removable Media Policy
  + Use of Email Policy
  + Data Transfer Policy
* Clear Desk Policy
* Network Security Policy
* Change Management Policy
* Development and Testing Environment Policy
* Disposal/Decommissioning Policy
* Information and Software Exchange Policy
* Firewall Policy

**4.6 ICT Access Control**

The ICT Access Control Policy defines the baseline standards to be applied in order to restrict access for employees and visitors to East Ayrshire Leisure to prevent unauthorised or fraudulent access including:

* only authorised personnel who have a justified and approved business need will be given access to restricted areas containing information systems or stored data
* access to information will be restricted to authorised users who have a bona-fide business need to access that information
* access to computer facilities will be restricted to authorised users who have business needs to use these facilities
* access to data, system utilities and programme source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators
* authorisation to use an application will depend on the availability of a licence from the supplier

The ICT Access Control Policy will be supported by other key policies, including:

* Password Management Policy
* Physical and Environmental Policy
* User Account Control Policy

**4.7 Incident Reporting**

All information security events and suspected weaknesses are to be reported to the Corporate Information Governance Group, as defined in the Incident Reporting Policy. All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

**4.8 Business Continuity and Disaster Recovery Plans**

East Ayrshire Leisure will ensure that business impact assessment, Business Continuity and Disaster Recovery Plans are produced for all mission critical information, applications, systems and networks.

**4.9 Compliance and Audit**

A range of policies define the baseline standards to be applied in order to ensure that East Ayrshire Leisure complies with legislation, that standards are being applied to identify and manage misuse or compromise of information or systems.

These include:

* Information Governance Guidelines
* Data Handling Policy
* Acceptable Use Policy Governing the use of Communication Systems
* Code of Conduct

Summary of relevant legislation:

1. Data Protection Act 1998
2. Freedom of Information (Scotland) Act 2002
3. Copyright, Designs and Patents Act 1988
4. Computer Misuse Act 1990
5. Regulation of Investigatory Powers Act 2000
6. Anti-Terrorism, Crime & Security Act 2001
7. Defamation Act 1996
8. Health & Safety at Work Act 1994 (Computers)
9. Re-use of Public Sector Information Regulations 2005
10. Civil Contingencies Act 2004

**4.10 Further Information**

Further information about this policy should be directed to East Ayrshire Leisure’s Data Controller:

Tel : 01563 554057

Email : [EALInformationgovernance@eastayrshireleisure.com](mailto:EALInformationgovernance@eastayrshireleisure.com)

**Record of Change**

|  |  |
| --- | --- |
| **Date Reviewed** | **Date of next review** |
| Aug 2019 | Aug 2020 |

Appendix 1

**Information Security Policy Framework**

Information Security Policy

* Information Asset Inventory
* Information Asset Ownership
* Risk Assessments

Information Asset Register

* Password Management Policy
* User Account & Control Policy
* Malicious Software & Hacking Policy
* Information Governance Guidelines
* Network Security Policy
* Change Management Policy
* Development & Testing Environment Policy
* Disposal/Decommissioning Policy
* Incident Management
* Develop Training Programme
* Develop ongoing Training Programme
* Information Governance Guidelines
* Acceptable Use Policy
* Freedom of Information Act
* Data Protection Act
* Clear Desk Policy
* Information Governance Guidelines
* Classification Procedure
* Storage of Classified Data

Compliance & Audit

Business Continuity & Disaster Recovery Plans

Incident Reporting Policy

ICT Access Control Policy

Systems Operational Management Policies

Physical & Environmental Policy

Information Security Awareness

Information Classification Policy