Information Security Policy

Version: V1_0
Owner: Corporate Governance / Corporate Services

Document Control Sheet

Title	Information Security Policy
Prepared By	Allyson Blue
Approved By	Jaki Carnegie
Date Effective From	2014/04/01
Version Number	V1_0
Review Frequency	Annual
Next Review Date	2015/04/01
Contact	ICT Manager

Revision History:

Version:	Date:	Summary of Changes:	Name:	Changes Marked:
V0_1	2013/12/03	New policy	Allyson Blue	N/A
V0_2	2014/01/17	Reviewed and updated	Stevie Thomson	Yes

Approvals: This document requires the following signed approvals.

Name/Title	Date	Version
Jaki Carnegie	2014/03/28	V1_0

Distribution: This document has been distributed to

Name:	Title/Division:	Date of Issue:	Version:
	All Staff	2014/04/01	V1_0

Table of Contents

1. Introduction

The Park Authority relies on information to fulfil our outcomes, obligations and statutory responsibilities and functions. Information and the systems we hold and use represent an extremely valuable asset both to the Park Authority and potentially to others. The

increasing reliance on information technology for the delivery of the services provided by the Park Authority make it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure way.

Threats to information security are becoming more widespread, ambitious and increasingly sophisticated. The consequences of the loss and misuse of confidential and sensitive information cannot only be significant to the organisation but can be devastating to individuals. It is essential, therefore, that all information processing systems within the Park Authority in whatever format, are protected to an adequate and effective level from disruption or loss of service or compromise whether through accidental or malicious damage.

This policy provides the guidelines and framework for ensuring the confidentiality, security and integrity of information held by the Park Authority, its services and officers is maintained.

2. Purpose, Aim & Scope

This policy applies to all employees of the Park Authority, our board members and employees/agents of external organisations who have access to Park Authority information systems.

Information covered by this policy includes that which is:

- Stored on computers or mobile devices
- Transmitted across networks – both internally and externally
- Printed
- Written
- Sent by fax
- Stored in electronic format on an external device or media eg. CD, DVD, USB drive etc
- Sent/Received via email
- Stored in databases
- Held on microfiche
- Held on CCTV Tapes
- Audio and video recordings

The policy also recognises that some aspects of information security are governed by legislation. The most notable Acts are:

- The Data Protection Act 1998
- Copyright, Designs & Patents Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers (Scotland) Act 2000
- Regulation of investigatory Powers Act 2000
- Freedom of Information (Scotland) Act 2002
- Electronic Communications Act 2000
- Telecommunications Act 2003
- Health & Safety at Work Act (1974)

- Environmental Information (Scotland) Regulation 2004

3. Objectives of Policy

- Ensure that staff and all Board members have an appropriate awareness and concern for information security and an understanding of their personal responsibility for information security;
- Ensure that all contractors, their agents and employees have a proper awareness and understanding of their responsibility towards our systems and information ;
- Provide a framework giving guidance for the establishment of standards and procedures for implementing information security;
- To meet the general objectives of BS7799-2 Code of Practice for Information Systems Security;
- To ensure that all employees and Board members ; are aware of the legislation surrounding information and information systems security;

4. Responsibilities

Our Director of Corporate Services and ICT Manager are ultimately responsible for Information Security Management within the Park Authority.

Directors and Heads of Service are responsible for:

- Ensuring that this policy is communicated to all individuals, including third parties, who are authorised to use information facilities;
- Ensuring that the information security principles and standards of operation are consistently enforced, in line with the terms of this policy, across all service areas;

Operational Managers are responsible for:

- Information created, held, stored, processed and destroyed in their service;
- Owning and managing risks associated with information in their service;
- Ensuring that business continuity plans are in place that cover the loss of information and systems within their service;
- Determining, on the basis of business needs, those staff who require access to information to assist them in the performance of their duties;
- Ensuring that appropriate local access controls are in place (eg. application passwords, lockable storage etc)
- Ensuring appropriate resources for the response / investigation / management / resolution of security incidents in their service areas.
- Ensuring that authorised users are given appropriate training and are fully briefed in good practice, legitimate and lawful use of the systems in accordance with the standards set down in this policy;
- New employees are made of this policy during their induction training
- Ensuring that authorised users are made aware of the possible disciplinary and/or legal consequences of any breach of this policy and any associated procedures or codes of practice;
- Reviews are carried out to ensure compliance with the terms of this policy;
- Complying with procedures for removing or amending the access rights of their staff who change jobs or leave the Park Authority;
- Reporting security incidents to the ICT Helpdesk

All authorised users (including all Board members of the Park Authority, staff, consultants, contract and agency staff)

General responsibilities of any and all authorised users

- Comply with the terms of this policy in relation to good practice and legitimate and lawful use of our information systems and physical records;
- Manage the security of their own work in accordance with our Data protection and Information Security Procedures;
- Ensure they exercise security (in line with guidelines) of all personal or sensitive information they handle on behalf of the Park Authority;
- Comply with all other guidelines relating to information security including password use, clear desk/clear screen guidelines, anti-virus guidelines, internet and email use policy etc;
- Must not circumvent or alter security facilities (such as anti virus software), access control facilities (network passwords, firewall rules etc) without prior permission;
- Report all suspected cases of misuse of this policy to their line manager.

Project Managers & Procurement Manager

- Ensuring that information security is specified and included in project plans and contracts;
- Ensuring new implementations and timely upgrades to existing information systems are fully tested and that audit arrangements are put in place;
- Ensuring that project and corporate risk logs are kept up to date with developments;
- Ensuring that all external project staff are aware of the information security responsibilities.

ICT Team

- Maintaining all security issues associated with central system facilities such as servers, databases, software and network facilities;
- Providing all ICT based security facilities such as firewalls, anti-virus software, intrusion detection, encryption facilities;
- Maintaining internet network security, user accounts and filtered user access, and for monitoring and reporting on inventories and access logs;
- Providing backup and disaster recovery facilities for systems
- Providing backup and disaster recovery as well as business continuity facilities for all central systems including email, internet, electronic file storage, firewalls etc;
- Reviewing the technical, operational and security aspects of this policy, in consultation with service areas;
- Issuing procedural guidance and codes of practice in support of this policy;
- Assisting with periodic audits and security accreditations.
- Provision and maintenance of the Information Security policy, guidelines and procedures;
- Provision of ICT Security training material and online content (for all users);
- Provision of advice and planning on security issues to the Records Management Working Group, across services, programmes and projects;
- Sign-off authority on firewall and network security changes and updates.

5. Asset Management

- Information Assets e.g. Databases, documents etc will be identified and managed within the Records Management policy;
- Al ICT assets will be clearly identified and included in a central inventory (Asset Log)
- All assets will have an identified "owner" either Head of Service or IT Team (for central systems)

6. Information Classification

All information within the Park Authority will be identified and classified by the criteria set out in our Records Management Policy. Information will be classified and labelled as per each service's file plan and our Business Classification Scheme. This will ensure that appropriate levels of protection are afforded when handling information. Higher levels of protection will be applied to personal or sensitive information or where there is a specific legal agreement.

7. Physical and Environmental Security

Depending upon the function and the nature of use, accommodation that stores information will be equipped with perimeter barriers, walls, gates, manned reception desks, CCTV and entry controls. Public areas, deliveries etc will be isolated from information processing areas.

The HQ office is the only office that deals with personal and/or sensitive information. This office has CCTV installed along with a secure storage facility onsite for the storage of records identified on the retention schedule as either being kept permanently or have a retention assigned which means they are kept for a set period of time. These records are stored in secure moveable filing cabinets which have security cards for access to cabinets which have personal and/or sensitive information. In addition all ICT documentation, data software etc is kept in fireproof safes.

8. User Access Management

All users will be granted/revoked access to systems via a formal user registration and de-registration process.

User access rights will be reviewed and audited on an annual basis.

9. Equipment Security

In order to mitigate the risks of loss, damage, theft or compromise of equipment and to protect equipment from environmental threats and hazards, and opportunities for unauthorised access:

- Central equipment (servers, network equipment, storage etc) will be protected from power failures and disruptions caused by failures in supporting services;
- Power and telecommunications cabling shall be protected from interception or damage;

- All equipment shall correctly be maintained to ensure correct (specified) operation and uptime;
- Secure disposal of equipment – all items containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Note: We use a third party facility to destroy IT equipment;
- Security settings are locked down by our ICT Staff ensuring they cannot be altered.
- Equipment, information or software shall not be taken off-site without prior authorisation;
- Security shall be applied to off-site equipment taking into account the different risks of working outside our premises; and
- Specific guidance and procedures will be issued by IT Services.

10. Network Security Management

IT Services will specify, implement, manage and maintain central network management facilities eg, cabling, switches, wireless devices, hubs, firewalls and intrusion detection systems.

Networks will be adequately managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or by a third party.

Appropriate authentication methods will be used to control access of remote users.

Automatic equipment identified will be maintained as a means of authenticating connections. Physical and logical access to diagnostic and configuration ports will be controlled. Networks will be segregated to ensure security between groups of users.

Routing controls will be maintained to ensure security of business applications.

All network connections and third party access must comply with this policy and have been approved by IT Services.

11. Mobile Computing and Teleworking

Mobile working and teleworking is supported and but is also subject to prior approval from your Line Manager.

12. Publicly Available Information

The integrity of information being made available on publicly available systems (e.g. our website) will be protected to prevent unauthorised modification or loss. Information published on behalf of the Park Authority must follow agreed publishing procedures.

13. External Parties

To maintain the security of our information and information processing facilities that are accessed, processed, communicated to or managed by external parties;

- The risks the our information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
- All identified security requirements shall be addressed before giving the third party access to our information or assets;
- A documented third party access agreement will be required of all service providers providing any aspect of information management and must cover all security arrangements
- Service delivery agreements will be regularly monitored and reviewed and will cover the security controls and standards required. All services will be reviewed upon significant change or upgrade.

14. Human Resources

Managers will ensure that all staff, contractors and third party users understand their responsibilities with regard to information security.

Line managers must ensure that all employees complete appropriate awareness training and regular updates as relevant to their job function. Upon termination of employment line managers must ensure the return of assets and inform the ICT Manager in order to remove all access rights.

15. Disciplinary Process

Any misuse of information or information systems will be investigated under our Disciplinary Procedure.

16. Protection against Malicious Code (Viruses)

A central anti-virus security system will be managed by IT Services. This will ensure the running of anti-virus updates, monitoring, alerting and responding. This will include all security patching on central servers and systems as well as PC based anti-virus.

17. Information Handling

Information that is subject to the Data Protection Act (1998) must not be stored or transmitted on USB memory drives, removable drives, CD's and DVD's. Only our approved methods of information transit will be permitted in limited circumstances with line manager prior approval.

Electronic data devices such as laptops, CD's Memory Sticks and other removable memory devices must be protected; using our approved encryption methods, from unauthorised disclosure, loss or misuse.

High risk areas will be identified, recorded on our corporate risk register and additional procedures, staff training and awareness will be applied.(where necessary)

18. Exchange of Information/Information Sharing

Formal agreements must be in place to protect the exchange of information of the Park Authority and external bodies. Individual Data Sharing Agreements must be in place for each instance. These agreements will detail our information security requirements.

19. Electronic Commerce Services

Information involved in electronic commerce (such as online payments, electronic purchasing etc), passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification using secure servers and encryption.

20. ICT Operational Management

Access and areas of responsibility including network equipment, central servers, back up facilities, central databases, central storage and web facilities will be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the system. System and administrator passwords will be issued on an individual basis, changed regularly and used in a secure manner to maintain least privilege access control.

The capacity of these facilities will be managed and optimised – the use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure required system performance.

Audit logs of activities on servers etc will be maintained to assist in security monitoring and investigations.

Incidents and system faults will be logged with the IT Helpdesk.

Development, test and operational facilities shall be separated to reduce the risks of unauthorised access. System acceptance criteria will be drawn up to ensure consistent criteria for the testing of new systems/changes/upgrades.

Back-up copies of information, databases, configurations and software shall be taken and tested regularly in accordance with the agreed back up plan.

21. Business Continuity

Facilities and systems shall be in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters and to ensure their timely resumption

Business Continuity plans, procedures and facilities shall be in place for all of our critical systems. A disaster recovery facility shall be put in place and maintained by IT Services that allows for the full or partial recovery of critical business systems in the event of a disaster at the HQ Building.

All backup, business continuity and disaster recovery systems will be reviewed and tested on an annual basis and after each significant change or upgrade.

22. Information Security Incident Management

All staff, contractors and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services. All must comply with the subsequent requirements and directives in order to rectify or eliminate the security risk.

Security incidents must be logged with the IT Helpdesk who will ensure the timely notification to management.

IT Services will give security incidents priority over normal service work until an agreed and acceptable level of security is restored.

All on-going security risks must be recorded on the LLTNPA's Corporate Risk Register.

23. Monitoring and Review

Monitoring activities will be carried out by Working Group members on an annual basis. Where non-compliance to this policy is discovered, this will be escalated to the Steering Group by way of an exception report outlining the current status together with recommendations for suitable action to be implemented to ensure resolution.

24. Related policies, procedures and Templates

- Disciplinary Procedure
- Data Sharing Agreement Template
- Remote Access to NP Systems
- Mobile Phone procedure
- IT Policy
- Mail Procedure