

Plymouth City Council

Information Security Policy

March 2007



This document is copyright to Plymouth City Council and should not be used or adapted for any purpose without the agreement of the Council.

Contents

Authorisation Statement.....	3
Document Control.....	4
Document Amendment History.....	4
1. Purpose.....	5
2. Scope.....	5
3. Risks to Plymouth City Council.....	5
4. Statement of Management Intent.....	6
5. Responsibilities.....	6
6. Review.....	7
7. Communication.....	7
8. Policy Standards.....	7
8.1 Organisation of Information Security.....	7
8.2 Asset Management.....	7
8.3 Human Resources Security.....	8
8.4 Physical and Environmental Security.....	8
8.5 Communications and Operations Management.....	8
8.6 Access Control.....	8
8.7 Information Systems Acquisition, Development and Maintenance.....	8
8.8 Information Security Incident Management.....	8
8.9 Business Continuity Management.....	8
8.10 Compliance.....	9
Appendix A: Glossary.....	10
Appendix B: Standards.....	11
Appendix C: Implications for the Council.....	12
Appendix D: Equalities Impact Assessment.....	14
Comments and Observations.....	16

Authorisation Statement

Information Security Policy

The purpose and objective of this Policy is to enable the Council's information assets to be held, used, stored and where appropriate disposed of in a secure manner. So that any internal or external threats to personal or business confidentiality, or to the integrity and availability of Council information are controlled. So that Council information and data are available for their intended purposes and unavailable for illegitimate purposes.

All Councillors, staff and others who collect information on behalf of the Council, or are provided with access to Council data, are directed to implement corporate standards so that decision making, reporting and communications are based on trusted knowledge resources.

Detailed standards and associated procedures will be produced to support the implementation of this policy and to achieve compliance with regulatory and legislative requirements.

This policy arises from the Information Communication and Technology Strategy and replaces the Information Security Policy & Guidelines March 2000

The implementation of this policy is the responsibility of the Head of ICT

This policy has been authorised by:

Signature Date
Mr B Keel
Chief Executive
Plymouth City Council

Document Control

Organisation	Plymouth City Council
Title	Information Security Policy
Creator	Devon Information Security Group
Source	Review of policies produced by other Local Authorities.
Approvals	MISF; CMT
Distribution	ICT managers and CMT
Filename	S V2.0 Information Security Policy.doc
Owner	Head of ICT
Subject	The Security Policy formalises Information security within Plymouth City Council.
Rights	Public
Review date	Annually

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
1.0	John Finch	27/02/2007	Compiled with Devon local authority colleagues and provided to Plymouth ICT managers for review
1.1	Richard Woodfield	02/03/2007	Format and content changes made after ICT managers review. Change of 'Authority to Council.
2.0	Richard Woodfield	06/3/2007	PDF created for CMT consultation.
2.1	John Finch	15/03/2007	Grammatical corrections, 1 section split into two paragraphs.

1. Introduction

- 1.1 Information is a major asset that Plymouth City Council has a duty and responsibility to protect.
- 1.2 The purpose and objective of this Information Security Policy is to set out a framework for the protection of the Council's information assets:
 - From all threats, whether internal or external, deliberate or accidental
 - To ensure business continuity and minimise business damage
 - In order to deliver strategic and operational objectives
- 1.3 The Information Security Policy is a high level document, and adopts:
 - **Standards:** mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. The standards are derived from the international security standard ISO 27001
 - **Baselines:** descriptions of how to implement security packages so as to ensure consistency throughout the Council
 - **Procedures:** which define the details of how the policy, standards and guidelines will be implemented in an operating environment
 - **Guidelines:** General statements designed to achieve the policy's objectives by providing a framework within which to implement controls not covered by procedures

2. Scope

- 2.1 This Information Security Policy outlines the framework for the management of information security within Plymouth City Council.
- 2.2 The Information Security Policy, Standards, Baselines and Procedures apply to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Plymouth City Council purposes.
- 2.3 Information takes many forms and includes:
 - hard copy data printed or written on paper
 - data stored electronically
 - communications sent by post / courier or using electronic means
 - stored tape or video
 - speech

3. Risks to Plymouth City Council

- 3.1 Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.
- 3.2 Poor education and training, misuse, and breach of security controls of information systems may result in data and information being put at risk, may be used to misrepresent the Council and result in the ineffective use of Council resources

- 3.3 Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements against the Council.

4. Statement of Management Intent

4.1 It is the policy of Plymouth City Council to ensure that:

4.1.1 Information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorised users have access to relevant information when required.

4.1.2 The Council will appoint a Management Information Security Forum (MISF) to review and make recommendations on security policy, policy standards, directives, procedures, incident management and security awareness education.

4.1.3 Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, Standards, Baselines and Procedures.

4.1.4 The requirements of the Information Security Policy, Standards, Baselines and Procedures will be incorporated into the Council's operational procedures and contractual arrangements.

4.1.5 The Council will work towards the ISO27000 series, the International Standards for Information Security.

4.1.6 The MISF will define Information Security Incidents, including a definition of breach.

4.1.7 All breaches of information security, actual or suspected, must be reported and will be investigated.

4.1.8 Business continuity plans will be produced, maintained and tested.

4.1.9 Information security education and training will be available to all Councillors and employees.

4.1.10 Information stored by the Council is appropriate to the business requirements.

5. Responsibilities

5.1 The Head of ICT is the designated Council owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, Standards, Baselines and Procedures.

5.2 Chief Officers are responsible for ensuring that Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council are made aware of and comply with the Information Security Policy, Standards, Baselines and Procedures.

- 5.3 The Council's Internal Audit Service will review the adequacy of the controls that are implemented to protect the Council's information and recommend improvements where deficiencies are found.
- 5.4 Each Councillor, Committee, Department, Partner, Employee of the Council, contractual third party and agent of the Council accessing Plymouth City Council information is required to adhere to the Information Security Policy, Standards, Baselines and Procedures.
- 5.5 Failure to comply with the Information Security Policy, Standards, Baselines and Procedures will lead to disciplinary or remedial action.

6. Review

- 6.1 The security requirements for the Council will be reviewed by the MISF and formal requests for changes will be raised for incorporation into the Information Security Policy, Standards, Baselines and Procedures.
- 6.2 Where the change impacts the Information Security Policy, these changes will be co-ordinated through the Devon Information Security Partnership.
- 6.3 Where agreement cannot be reached or the Devon Information Security Partnership is unable to coordinate the changes, the Council's Head of ICT will manage the changes.

7. Communication

- 7.1 The Information Security Policy, Standards, Baselines and Procedures will be communicated to each Councillor, Committee, Department, Partner, Employee of the Council, contractual third party and agent of the Council accessing Plymouth City Council information.

8. Policy Standards

8.1 Organisation of Information Security

- 8.1.1 The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the Council and in its dealings with third parties.
- 8.1.2 Specialist external advice will be drawn upon where necessary so as to maintain the Information Security Policy, Standards, Baselines and Procedures to address new and emerging threats and standards.

8.2 Asset Management

- 8.2.1 All assets (data, information, software, computer and communications equipment, service utilities and people) are accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset/s concerned.

8.3 Human Resources Security

- 8.3.1 Employee, contractor and third party terms and conditions of employment/working and any supporting documents, e.g. role profiles, must set out security responsibilities and show adequate screening and declaration processes in place.

8.4 Physical and Environmental Security

- 8.4.1 Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

8.5 Communications and Operations Management

- 8.5.1 Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established.
- 8.5.2 The Retention and Disposition Policy must be implemented for all information holding systems both manual and electronic.

8.6 Access Control

- 8.6.1 Access to information and information systems must be driven by business requirements. Access shall be granted or arrangements made for Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council according to their role, only to a level that will allow them to carry out their duties.
- 8.6.2 A formal user registration and de-registration procedure is required for access to all information systems and services.

8.7 Information Systems Acquisition, Development and Maintenance

- 8.7.1 Information security risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems.
- 8.7.2 Controls to mitigate the risks must be identified and implemented where appropriate.

8.8 Information Security Incident Management

- 8.8.1 Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner.

8.9 Business Continuity Management

- 8.9.1 Arrangements must be in place to protect business processes from the effects of failure or disasters and to ensure the timely resumption of business information systems.

8.10 Compliance

8.10.1 The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements.

Appendix A: Glossary

Term	Description
Baselines	Establishes the implementation methods for security mechanisms and products.
Chief Officers	Directors / Heads of Service / Head teachers / Principals
Data	A specific fact or characteristic
Devon Information Security Partnership	Representatives of the Local Authorities and other Governmental organisations in the County of Devon. This group initiates and supports good information security practice.
Guidelines	General statements designed to achieve the objectives of the policy by providing a framework within which to implement controls
ICT	Information Communications Technology
ISO	International Standards Organisation
Information	Data being used in context and for decision making
MISF	Management Information Security Forum are representatives from each Directorate that monitor the implementation of this policy and recommend how the policy should apply to Council activities
Procedures	Step by step instructions detailing how policy and standards will be implemented in an operating environment
Retention and Disposition Policy	This policy controls how long records are kept and whether at the end of this period the record is then permanently archived or destroyed
Standards	Mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. The standards are derived from the international security standard ISO 27001

Appendix B: Standard Summary

Reference	Standard Summary
8.1	Responsibility for implementing the policy is assigned
8.2	All assets holding or conveying information have an identified owner who is accountable for the maintenance and protection of those assets
8.3	All those employed by the Council have had screening to determine whether they are a risk to any information held by the Council
8.4	Appropriate security barriers and/or entry controls are in place for all information assets
8.5	Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities are in place
8.6	Access to information and information systems to be according to role and only to a level that will allow responsibilities to be fulfilled
8.7	Information security risks are identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems and controls implemented where appropriate
8.8	Information security incidents and weaknesses are recorded and mitigating action taken in a consistent and timely manner.
8.9	Arrangements are in place to protect critical business processes from the effects of failure or disasters and to ensure the timely resumption of business information systems
8.10	Statutory, regulatory and contractual security requirements are identified and implemented for all information systems and information transfers

Appendix C: Implications for the Council

Human Resources	
2.2, 4.1.4, 8.3.1	Employee, contractor and third party terms and conditions of employment/working and any supporting documents, e.g. role profiles, must set out security responsibilities and show adequate screening and declaration processes in place
5.4	Each Councillor, employee, partner and third party accessing Plymouth City Council information is required to adhere to the Information Security Policy, Standards, Baselines and Procedures
5.5	Failure to comply with the Information Security Policy, Standards, Baselines and Procedures must lead to disciplinary action
Staff Development	
3.2	Training is required for all Councillors and staff
4.1.8	Information security education and training will be available to all Councillors and employees.
Asset Management	
8.2.1	All assets (data, information, software, computer and communications equipment, service utilities and people) are to be accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset/s concerned.
8.4.1	Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls
8.5.1	Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established
8.6.1	Access to information and information systems must be driven by business requirements. Access shall be granted or arrangements made for Councillors, employees, partner agencies and third parties according to their role, only to a level that will allow them to carry out their duties
Business Continuity	
4.1.7, 8.9.1	Business continuity plans will be produced, maintained and tested for all systems that obtain, produce, hold or transfer information
Procurement	
2.2, 4.1.4,	The requirements of this policy must be incorporated in all arrangements with providers and suppliers of services to the Council
5.5	Failure to comply with the Information Security Policy, Standards, Baselines and Procedures must lead to breach of contract action
Information and Communications Technology	
5.1	The Head of ICT will maintain and review the Policy, Standards, Baselines and Procedures
6.1	The security requirements for the Council will be reviewed by the MISF and formal requests for changes will be raised
6.3	Where agreement over changes to the policy cannot be reached or the Devon Information Security Partnership is unable to coordinate the changes, the Head of ICT will manage the changes
7.1	Will identify those accessing Plymouth City Council information and

Information Security Policy

	communicate this Policy, Standards, Baselines and Procedures
8.1.2	Will obtain specialist external advice where necessary in order to address new and emerging threats and standards
8.7.2, 8.8.1	Controls to mitigate risks must be identified and implemented where appropriate
Directorates	
2.2	All activities involving data or information must take account of the requirements of this policy
3.2	Inefficiencies will be reduced through complying with this policy
4.1.2, 8.1.1	Will contribute to the Management Information Security Forum and follow its recommendations
4.1.4	The requirements of the Information Security Policy, Standards, Baselines and Procedures will be incorporated into operational procedures
4.1.5	Will cooperate with achieving ISO27001, the International Standard for Information Security
4.1.6, 8.8.1	Will establish procedures for reporting and investigating all breaches of information security
4.1.9	Will only store information appropriate to their business requirements
5.2	Directors and Service Managers are responsible for ensuring that Councillors, employees, partners and third parties are made aware of and comply with the Information Security Policy, Standards, Baselines and Procedures
8.5.2	Will implement the Retention and Disposition Policy for all information holding systems both manual and electronic
8.6.2	Will establish a formal user registration and de-registration procedure for access to all information systems and services
8.7.1	When developing business requirements for new information systems or enhancements to existing information systems will identify information security risks at the earliest stage
8.10.2	When designing, operating, using and managing information systems will take into consideration all statutory, regulatory and contractual security requirements

Appendix D: Equalities Impact Assessment

Policy: Information Security Policy	Date: 06 March 2007
Data used in conducting this assessment: none	Officer conducting this assessment with contact details: Richard Woodfield tel: 304067

Equalities Issue	Positive impact	Negative impact	None	Reasons for decision
Age			X	
Disability		X		Learning Disability group. Tight controls on how information is handled and stored may be a difficulty for those people who are restricted in comprehending the standards that apply to the processing of electronic data and hard copy records.
Faith			X	
Gender			X	
Race			X	
Sexual Orientation			X	
Other	Those who do not have a reasonable use of the English language may require additional assistance in order to implement this Strategy			

The guidance on undertaking a standard EIA ... is also applicable to a basic assessment. This EIA template is suitable for small-scale assessments of delegated decisions

Section B: Action

5. Please complete your action plan below. Issues you are likely to need to address include

What consultation needs to take place with equality groups (bearing in mind any relevant consultation already done and planned corporate consultation exercises)

What monitoring/evaluation will be required to further assess the impact of any changes on equality target groups

Equalities Impact Assessment Implementation Action Plan

Issue to be addressed	Responsible Officer	Action Required	Timescale for completion	Action Taken	Comments
Councillors, Staff and consultants are clear about the requirements and their role and are intellectually able to undertake the requirements of the Information Security Policy	Team Leaders / Line Managers / Head of Democratic Support	Disability assessment as to users ability to fulfil their role in the light of the requirements of the Information Security Policy	ongoing	On start of role and then as part of annual appraisals	<p>The Information Security Policy applies to Councillors, staff, consultants and any other person processing the Council's data or information using the Council's electronic or manual systems.</p> <p>The strategy will not have a direct or indirect affect on service user groups except on the integrity and confidentiality of the information used to make service arrangements.</p>

6. Report and publication

Please record details of the report or file note which records the outcome of the EIA together with any actions / recommendations being pursued (date, type of report etc)	This assessment is an appendix to the Information Security Policy
Please record details of where and when EIA results will be published	None applicable

Name of Officer completing: Richard Woodfield Date: 06 March 2007

Name of Senior Manager Authorising Assessment and Action Plan for publication:

Neville Cannon Signed: _____ Date: _____

Comments and Observations

Please send any comments, observations or suggestions about this strategy to:

John Finch
Information Security Manager
ISD
Floor 2
Civic Centre
Plymouth
PL1 2AA

Fax: 01752 304997

Email: john.finch@plymouth.gov.uk