POLICY: INFORMATION SECURITY POLICY

Author:	Tara Walker
Division:	ICT
Date Created or Reviewed:	12 June 2013
Review Date:	12 June 2014

Contents

1.0 Introduction

As public services look to more collaborative ways of working, recognising information as a valuable shared resource, the necessity for organisations to operate securely and adopt common standards increases.

Threats to information exist both internally through mis-use, accidental or malicious loss or disclosure, and externally by hackers, disgruntled trouble makers or even foreign governments. Our customers expect that their information is held confidentially, is accurate and is available when and where it may be needed for their benefit.

Brighton & Hove City Council ('BHCC') is under various duties to adequately protect the information it holds about its citizens. There are various pieces of legislation that affect the Council such as the Data Protection Act, Freedom of Information Act, the Computer Misuse Act and the Human Rights Act. As well as legal duties the Council has contractual compliance obligations, such as the PSN Code of Connection. In order to comply the Council is committed to ensure these obligations are met and best practice and industry security standards are adopted and embedded throughout the organisation.

The primary tenet of policies, procedures and other mechanisms put in place by ICT is the protection of information and the systems containing information from illicit intrusion, damage, theft, corruption or unauthorised deletion. The Information Security Policy is an overarching policy that comprises information related policies, procedures, standards and other mechanisms, and draws them into one coherent framework. These policies detail the assertions, along with references to relevant guides and other supporting material, that have been enacted to ensure this duty is carried out efficiently and effectively.

Furthermore, these policies add value to the Council's activities by improving and optimising the Council's business processes and as a result increasing its efficiency.

2.0 Purpose

BHCC will define and enforce this Policy Framework as a living document set enabling the Council to have an effective, consistent working environment with the ability to defend against internal and external threats and show due diligence to the people it serves. Effective information security ensures and increases public confidence and avoids any potentially damaging action being taken against the Council such as litigation or large fines from the ICO. The primary aim of the Information Security Policy Framework is to protect the Council from security breaches to its information systems and the information stored on them that might have an adverse effect on its operations, infrastructure financial position and/or reputation.

An Information Security Policy framework creates the working environment in which information is protected in an organisation. As a key dependency of an organisation's success, information security can no longer be miscategorised as an ICT issue; it is not, it is a key business issue. A secure, consistent and reliable working environment operated by all members of staff, Members, partners and contractors is necessary to effectively contribute to enabling an organisation to reach

its corporate objectives. Therefore the secondary objective is to position information as a key business asset and therefore a key business issue; raise awareness and highlight the importance of information security ensuring that all employees, members and third parties are aware of their responsibilities.

3.0 Scope

This policy applies to all information in any format held on any media. This includes but is not limited to paper, electronic documents, email, fax, notes written on paper, audio and video recordings and conversation.

All Brighton & Hove City Council employees and members shall familiarise themselves with this policy. All contractors and third parties should be made aware of this policy during their period with the Council or during the period of access to the Council's systems.

4.0 Policy

4.1 Principles

Information security includes protection of the following:

- Confidentiality: Ensuring that information and information systems are accessible only to authorised users.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorised users have access to information and information systems when required.

4.2 Assertions

Brighton & Hove City Council shall use all reasonable, appropriate and cost-effective measures to protect its information and achieve its security objectives to ensure that information is appropriately protected.

BHCC has created the Information Security Policy Framework which can be visualised as a pyramid. This policy is the corporate overarching information security policy which states the organisations approach and commitment to information security; the top of the pyramid. This policy is underpinned by area specific policies such as Data Protection, information handling and remote working forming the second layer. These policies are based on the various standards the Council must comply with. Policies are further supported by guidance, process and procedure at the third layer. The top 3 layers inform and are supported by the technology environment in which the organisation operates on.

ISO 27001 / BS 7799 (Information Security Management and Records Management standards) will be used as the guide to determine policy and manage security.

The policy will comply with legal and contractual requirements including but not limited to:

- Environmental Information Regulations (2004)
- Freedom of Information Act (2000)
- Regulation of Investigatory Powers Act (2000)
- Data Protection Act (1998)
- Computer Misuse Act (1990)
- PSN Code of Connection (GCSx)
- IG Toolkit (N3)

The policy will not unnecessarily limit business or individual freedom, but take a balanced risk management approach.

4.3 Risk

Non-compliance with this policy may result in financial loss, an inability to provide services to our customers, and adversely impact the Council's reputation.

4.4 Responsibilities

The Executive Leadership Team ('ELT') through the Information Management Board is ultimately responsible and accountable for ensuring that the objectives of the security policy are met.

The Head of ICT is responsible for implementation of the policy and is authorised to commission activities to achieve the policy objectives.

The ICT Security & Standards Manager has the responsibility to coordinate and control all the day-to-day activities associated with protecting the security of Brighton & Hove's City Council information.

The ICT Security & Standards Manager, in association with the Security & Standards Team and the ICT Department, is responsible for advising users on security issues, preventative monitoring of information systems and investigating security incidents.

The Data Protection Manager is the Council's designated Data Protection Officer. The Security & Standards Team will work with these officers to ensure compliance with these areas of legislation.

Key information systems have designated System Owners. These individuals are responsible for the security of their system and the data held on it. The Security & Standards Team will provide further advice.

All users of Council information systems are responsible for protecting information assets. Users must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.

Users must report any breach, or suspected breach, of information security to the Data Protection Manager on 01273 291207. In such an event the procedure contained in the 'Data Protection Guidance in the Event of a Breach' must be followed. The guidance is available on the Wave at BHCC > Cross Directorate > Information Governance > Shared Documents > ICT Policies.

4.5 Awareness

The Security & Standards Team will publicise the information related policies, procedures and guidance to all Council employees and members, and where relevant contractors and third parties.

Information on known vulnerabilities and patches will be made available to relevant users and system owners.

Information security awareness will be provided through workshops, training courses and various publications either on the Wave or through printed material.

5.0 Related Policies, Standards and Guidelines

This policy over pins a set of detailed policies which document specific areas of information security. A detailed list is available at Appendix A.

Supporting guidance and procedures have been produced to provide practical/technical information on how to implement policies for specific environments and environments.

Procedures are obligatory security measures to be followed at all times.

Guidance documents the recommended security measures to be followed unless it is not practical to do so.

6.0 Terms and Definitions

The words data and information are used interchangeably in all information related policies in the policy set detailed at Appendix A.

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given elsewhere can be found here.

The keywords must, must not, will, will not, required, should, should not, recommended, not recommended, may, and optional in this document are to be interpreted as follows:

Must: this word, or the terms **required**, or **will** means that the definition is an absolute requirement of the specification

Must not: this phrase, or the phrase **will not** means that the definition is an absolute prohibition of the specification

Should: this word, or the verb **recommended**, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course of action regarding the specification.

Should not: this phrase, or the phrase **not recommended**, means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications must be understood and the case carefully weighed before implementing any behaviour described with this label.

May: this word, or the adjective **optional**, means that you have a choice, which you must exercise reasonably, lawfully and in accordance with the Council's policies and priorities.

7.0 Enforcement

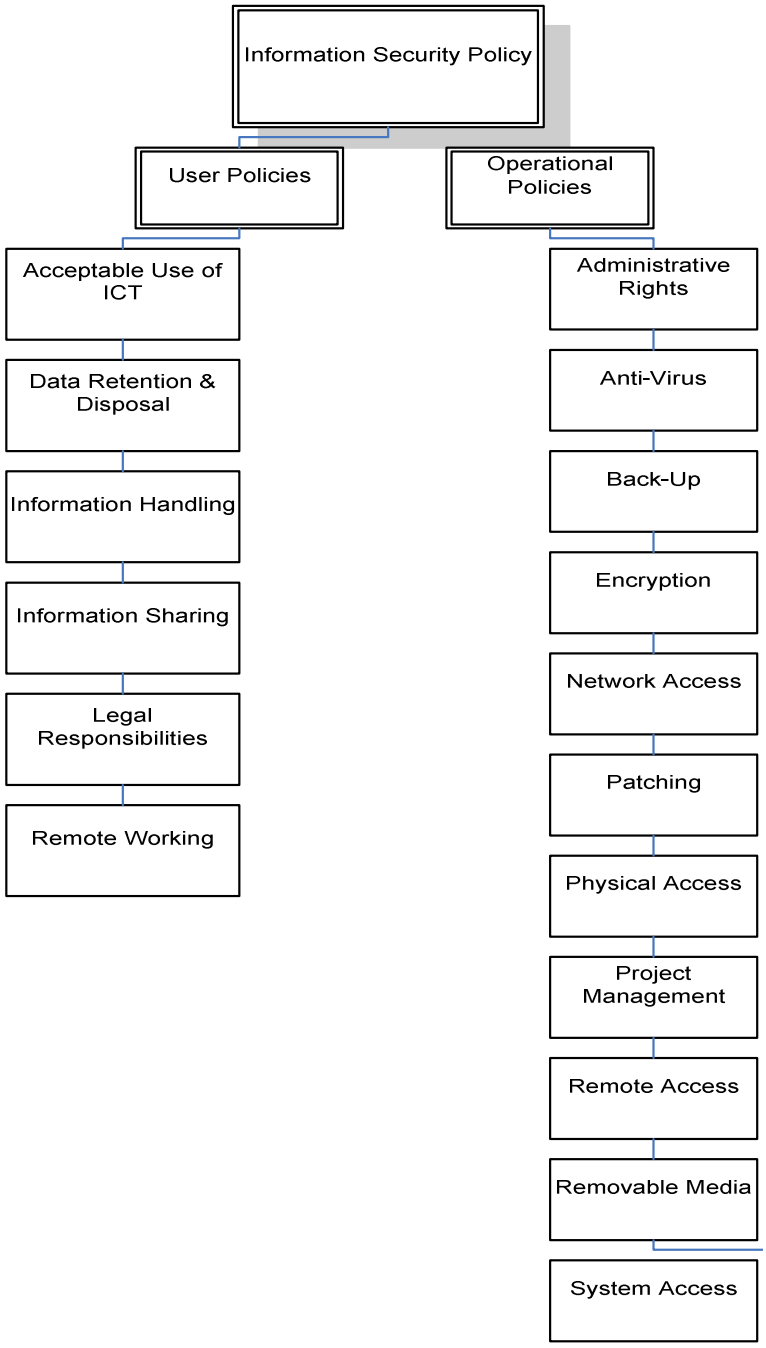
ICT Services will monitor information systems and the network to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents

This policy and compliance with it applies to all employees and those who use Council information systems. Any user or administrator found deliberately contravening this policy or caught jeopardising the security of information that is the property of Brighton & Hove City Council may be subject to disciplinary action and, where appropriate, legal action.

8.0 Review

This document will be reviewed annually as a minimum or wherever there may be a change of influencing circumstances. All major changes should be approved by the Information Management Board.

Appendix A: Table of Information Security Policies



10.0 Document Attributes

Document Information

Title	Information Security Policy
Identifier	Information Security Policy
File Location	ICT > Document Library > Information Management > Documentation > Policy > Published
Description	Details the overarching policy approach to over pin all other information based policies.
Keywords	Information; Security;
Format	MS Word
Author	Tara Walker
Owner	Head of ICT
Classification	UNCLASSIFIED
Date Created	11 July 2012
Last Review Date	12 June 2013
Next Review Date	12 June 2014
Date to Dispose	12 months after later version of policy released

Document History

Date	Summary of Changes	Version
11 July 2012	First Draft by Security & Standards Manager	v0.1
12 June 2013	Third Draft following input from the IMB	V0.3

Document Approval

Date	Name & Job Title of Approver(s)	Version

Distribution

Name / Group	Title

Coverage

Group

End of Document