Birmingham City Council

Information Security Labelling and Handling Standard

If you have any inquiries about this Standard,
Contact the Information and Strategy Team (formerly the Business Policy Team, ICF) on 675 1431 or 464 2877

Standard Owner:	Gerry McMullan Information & Strategy Manager, Performance and Information Division, Birmingham City Council
Author:	Mrs M A Westrop – Information Security Manager, Service Birmingham
Version:	4.0
Date:	20/07/2011
Classification	NOT PROTECTIVELY MARKED

Produced in conjunction with

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version Amendment	Date	Purpose	Author
Draft 0.1	23/05/07	Initial Draft	M Westrop
Draft 0.2	14/06/07	Draft after consultation DT&CH of ICF &NJ (see minutes)	M Westrop
Draft 0.3	05/07/07	Draft after documented comments from Reviewers (see detail below)	M Westrop
Draft 0.4	18/07/07	Draft changes after ICF alterations to draft (see ICF document 0.3 reviewed)	M Westrop
Draft 0.5	26/07/07	Changes incorporated after clarification from ICF (see correspondence)	M Westrop
Draft 0.6	02/08/07	In line with 0.6 Code of Practice	M Westrop
Draft 0.7	08/08/07	Corrections after questions put to ICF	M Westrop
Draft 0.8	16/08/07	Update following CISG review	S Tilley / D Thomas
Draft 0.9	30/08/07	Syntax; reinstate capitalised S in Standard.	M Westrop
v1	04/09/07	Update to v1 following BTAG approval	C Hobbs
1.1	12/03/09	Changes for Government GCSx requirements	M Westrop
1.2	08/04/09	Update from review comments	C Hobbs/J Walker
1.3	15/04/09	Amended page breaks and tables & storage paragraph	C Hobbs
1.4	17/04/09	Amended storage paragraph after meeting with SB	C Hobbs
2.0	22/04/09	Approved by BTAG	C Hobbs
2.1	28/05/10	Reviewed and no changes represented to	

2.1	May 2010	CISG Members	Birmingham City Council & Service Birmingham	

Document Approval by Birmingham City Council

Version	Date	Name	Role
1.0	04/09/2007	BTAG	Approving Body
2.0	22/04/2009	BTAG	Approving Body
3.0	02/06/2010	BTAG	Approving Body
4.0	20/07/2011	BTCG	Approving Body

Overview

Authority[a]	Birmingham City Council – Assistant Director Performance & Information Division
Owner[b]	

2. PURPOSE OF THE LABELLING AND HANDLING STANDARD

The Birmingham City Council Information Security Labelling and Handling Standard contains security rules to protect information controlled by the council, or by a third party on behalf of the council[e]. The council requires all those within the scope of the Standard to follow these rules to protect the confidentiality, integrity and availability of council information.

The handling and labelling rules apply to information classified according to the scheme set out in the Birmingham City Council Information Security Classification Standard. This has been changed to fit in with the 2008 Government Security Policy Framework. From April 2009, Birmingham City Council participates in the Secure Government Intranet 'GCSx' network. This means that the council has harmonised its security classifications to cope with information shared between the Government and the council. RESTRICTED, PROTECT and NOT changed to <<DMCID 4 >>BDC8m A

3. STANDARD PARTICULARS

This Standard should be used in conjunction with the Birmingham City Council Information Security Classification Standard which sets out three specific Information Security Classifications used by the council: RESTRICTED, PROTECT and Not Protectively Marked.

At all stages in its lifecycle, information should be labelled with its Security Classification and handled with the degree of caution necessary for that Security Classification. Practical advice is set out in the Birmingham City Council Information Security Labelling and Handling Code of Practice. Managers are responsible for deciding th e Security Classification of information and the handling procedures in their own business area in line with legislation, financial or audit regulations, Government requi rements (including Government Connect [h]) and the particular requirements of their business area.

Information Lifecycle Summary

Lifecycle stage	Key principles. These are supplemented with practical advice in the Information Security Labelling and Handling Code of Practice.
Acquisition and Creation	When information is acquired or created, it must be given its Information Security Classification and handled appropriately for that Information Security Classification and any additional particular requirements. Birmingham City Council managers have a responsibility to classify information which must be clearly labelled with its security classification. Files must be marked with the highest security level that has been given to any item of information within that file.
Storage	When anyone stores information on any council equipment[i] the stored information must be relevant to their duties and this must only be done in the course of those duties. This restriction does not apply to information temporarily stored as a result of personal use of email or the Internet. The council reserves the right to monitor and investigate any information stored on its systems. All information files must be labelled with the highest level of security classification required within the file. Handling rules for each classification are described in the Information Security Labelling and Handling Code of Practice.

[h] Government Connect is a network between central government and every local authority in England and Wales, known as GCSx (Government Connect Secure Extranet).

[i] This includes personal and shared network drives and local hard drives

Lifecycle stage	Key principles. These are supplemented with practical advice in the Information Security Labelling and Handling Code of Practice.
Access	Access rights to information (manual or computer information systems) should be role-based and not individually-based: that means that a particular individual can access RESTRICTED or PROTECT information in the course of their work only if their job or role within the council justifies this. See the council's Access Control Standard for further guidance. Access to information classified as RESTRICTED and PROTECT, (which will include all sensitive personal information), must be limited to those authorised to view it. RESTRICTED or PROTECT information must always be safeguarded by authentication formalities, whatever storage system is used[j]. Information shared through the GCSx Government Connect network must be Processed only on equipment owned by the council and connected to the council's networks directly[k] and kept on council-controlled premises. Other information, (but never information available to GCSx), may be processed remotely as set out in the Flexible and Remote Access Standard.
Prints, copies or other portable media	Portable information may be held on paper (for example, prints and copies) or other non-digital media or portable electronic memory (for example, CDs and memory sticks). It must be labelled with its Security Classification. Access to portable information must be restricted solely to relevant people and information must be stored securely in order to prevent unauthorised access. Files must be marked with the highest security level that has been given to any item of information in that file. All portable use of RESTRICTED information should be recorded in an audit log[l]. Unless it is deliberately reassessed and re-classified, portable information inherits the same Information Security Classification as the original from which it was copied. Portable information should be appropriately labelled with its Information Security Classification. Information released under the Freedom of Information Act must be classified as Not Protectively Marked. It is the responsibility of the person using copied or portable data to keep it securely. It is a manager's responsibility in their business area to decide what portable handling needs to be specifically authorised.

j Authentication formalities are the procedures used to verify the identity of the person using the information and record and limit their access to the information: for example, the person who gains access must have a unique identity and secret password; they must be formally authorized and granted an identity before t hey gain access; they should have access levels appropriate for their job duties, etc. Full controls are set out in ISO27001.

k Direct connections do not pass through the internet or networks not owned and managed by the council. For example, Blackberry connections to GCSx data are not permitted.

l An audit log template is available on the PSPG database.

Lifecycle stage	Key principles. These are supplemented with practical advice in the Information Security Labelling and Handling Code of Practice.
Retention, Back Up, Archiving and Destruction	When mobile devices and portable memory devices are due to be de-commissioned, the person responsible for the information on those devices must consider if the information should be retained, archived or destroyed. Information which is due to be destroyed is always classified as RESTRICTED. Refer to your Directorate's retention schedules and the Records Management Policy for advice about whether the information should be retained, destroyed or archived.
Transfer and Exchange of Information	It is presumed that all information which not protectively marked will be available to the public under Freedom of Information rules, unless there is a legal obligation not to exchange this information. Protectively marked Information should not be exchanged or transferred unless there is clear justification and authorisation. When information is

4. ROLES AND RESPONSIBILITIES

Role	Organisation	Responsibility
Employees, agency staff, elected members or other public representatives, trustees, third parties under a contract, employees of associated organisations or volunteers	All within Scope	To comply with this Standard & related documents.
Corporate Management Team	Birmingham City Council	To manage and maintain controls which limit access to information as required in this Standard.
Intelligent Client Function – Business Policy Manager	Birmingham City Council	To make sure the Information Security Labelling and Handling Standard meets business needs and is reviewed annually as a minimum; To make managers aware of the requirements of the GCSx Code of Connection.
Birmingham City Council Managers	Birmingham City Council; Service Birmingham on behalf of Birmingham City Council.	To manage information labelling and handling locally within the organisation and to decide the appropriate information security classification for each database; To provide suitable training about the security Standards and Policies and to communicate this Standard and the Code of Practice to Staff; To make third party organisations aware that the council's Information Security Labelling and Handling Standard is the minimum requirement when information is exchanged; To communicate issues and anomalies back to the Corporate Management Team. To understand and follow the requirements of the GCSx code of connection when dealing with Government Connect information.
Head of Records Management Service	Birmingham City Council	To advise on records management within the council.

5. EXCEPTIONS

There are no exceptions to this Standard.

6. ENFORCEMENT

Any member of staff who contravenes this Standard may be investigated under the council's disciplinary procedure and, where appropriate, legal action will be taken.

Third parties, partners and other individuals within the scope[n] of this Standard, who contravene its terms, may have their right to handle council information revoked and may jeopardise their relationship with Birmingham City Council. They may also face legal action.