



Birmingham City Council

Software Control Standard

If you have any enquiries about this Standard, contact the Information and Strategy Team,
Performance and Information Division, Corporate Resources
on 0121 675 1431 or 0121 464 2877.

Policy Owner: Gerry McMullan
Information and Strategy Manager
Performance and Information Division,
Birmingham City Council

Author: Jill Walker
Manager – Security
SP&BS Team, Service Birmingham

Version: 5.0

Date: 26th October 2012

Classification: NOT PROTECTIVELY MARKED

© Birmingham City Council 2012



Produced in conjunction with

TABLE OF CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS	3
2. DEFINITIONS	5
3. PURPOSE OF THE STANDARD.....	5
4. SECURITY RISK	5
STANDARD PARTICULARS	6
5.1 Software acquisition, purchase and approval	6
5.2 Software Registration	7
5.3 Installation and Maintenance and Use of Software.....	8
5.4 Removal or Transfer of Software.....	8
5.5 Malicious Software	9
5.5.1 Computers owned by Birmingham City Council	9
5.5.2 Computers and computer devices not owned by Birmingham City Council.....	9
5.5.3 GCSx connections.....	10
5.5.4 All Peripheral devices connected to the Network	10
5.5.5 Software Control.....	11
6. ROLES AND RESPONSIBILITIES.....	12
7. MONITORING.....	13
8. ENFORCEMENT	13

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose	Author
3.2	September 2011	Amendments following review comments	Jill Walker
4.0	23 September 2011	BTCG Approval	Caroline Hobbs
4.1	10 September 2012	Annual Review: software processing council information on private computers must use approved software; ICF now PI; COTs not available so refer to SB for a copy; s/w transfers must be performed by SB; defined terms defined; SB managers and third parties included; language tightened particularly definition and scope more defined and to cover Users of all city information on any equipment; all city equipment; and all SB managed equipment, updated Related Documents; corrected name of CD&Pact; clarified home workers can patch but otherwise installation by SB, enforcement changed in line with external access practice.	M Westrop
4.3	27 September 2012	Changes to 5.3 to set out responsibility for patching after review by Audit; cross reference to Cascading of Surplus Equipment Policy.	
5.0	26 October	Approved by BTCG	Caroline Hobbs

Document Distribution after Approval

Name	Organisation
All staff	Birmingham City Council
All staff	Service Birmingham

Document Reviewers

Version	Date	Name	Organisation	Role
3.1	09/11	CISG	BCC/SB	Corporate Information Security Group
3.1	09/11	Mark Lyden	Service Birmingham	Asset & Configuration Manager
3.1	09/11	Lesleen Black	Service Birmingham	Software Licensing Manager
3.1	09/11	Sajid Rehman	Service Birmingham	Remote Fix Team Manager
3.1	09/11	Helen Smith	Service Birmingham	Procurement Manager
4.3	09/11	All of the above	BCC/SB	Reviewers

Document Approval by Birmingham City Council

Version	Date	Name
2.0	17/09/2009	BTAG
3.0	01/09/2010	BTAG
4.0	21/09/2011	BTCG
5.0	26/10/2012	BTCG

Authority ^I	Birmingham City Council – Assistant Director Performance and Information Division
Owner ^{II}	Birmingham City Council – Information and Strategy Manager
Scope ^{III}	This Standard applies to all Users when they access council owned information from any equipment in any location; and it applies to all council owned equipment and any equipment managed by Service Birmingham on behalf of Birmingham City Council. It also applies to anyone engaged in council business who has knowledge of lost or found equipment.
Review period ^{IV}	Annual
Related Birmingham City Council documents	Information Security General Standard Malicious Software Guidance Asset Management Joint Standard E-mail Code of Practice Loss of Information or Loss of Equipment Containing Information Standard Disposal of Information Processing Equipment Standard Internet Use Policy Internet Code of Practice Service Birmingham Non-Standard Product Management Process GCSx Code of Connection Flexible and Remote Access Standard Cascading of Surplus Equipment Policy
BS ISO/IEC 27001:2005	<i>Control Reference</i>
BS 7799-2:2005	A.6.1.3 Allocation of Information security responsibilities
control references	A.7 Asset Management A.7.1.1 Inventory of Assets A.7.1.2 Ownership of Assets A.7.1.3 Acceptable Use of Assets A.8.3.2 Return of Assets A.12.4.3 Control of Operational Software A.12.5.3 Restrictions on changes to software packages A.12.5.5 Outsourced software development A.15.1.1 Intellectual Property Rights

^I AUTHORITY: The person or organisation who is responsible for enforcing this Standard.

^{II} OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of, this Standard.

^{III} SCOPE: The organisations or persons to whom the Standard applies.

^{IV} REVIEW PERIOD: How frequently the Standard should be reviewed.

2. DEFINITIONS

A “Budget Holder” is a manager or officer with responsibility for purchases made from a particular cost centre within the accounting structure of Birmingham City Council.

An “Asset Number” is a number given to certain digital equipment within the Scope of this Standard.

The “Definitive Software Library” (DSL) is the repository of master copies of approved software.

The “Network” is a collection of hardware computer devices owned by Birmingham City Council and Service Birmingham, which are interconnected. Access to the Network is controlled.

Information is “Processed” whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: *it is difficult to say there is any activity directed towards the data, which does not amount to processing.*

“Software” consists of sets of computer instructions which act on equipment or information within the Scope of this Standard (see above) or operated by Users within the Scope of this Standard. Software may include paid for commercial products and free software and will usually be supplied with licensing restrictions.

“Two Factor Authentication” is defined in the Information Security Labelling and Handling Standard under ‘Two Levels of Security’.

“Users” are those persons who are authorized by Birmingham City Council management or Service Birmingham management to access council owned information or council owned equipment or equipment managed by Service Birmingham on behalf of Birmingham City Council.

3. PURPOSE OF THE STANDARD

This Standard sets out rules and proper practice for the approval, acquisition, registration and installation, maintenance, removal, transfer and use of all Software within the Scope of this Standard.

The purpose of the rules and practice set out below is to make sure that the council’s Software is compatible with business and security requirements and is compatible with the council’s existing infrastructure; to make sure Software is licensed; to prevent copyright infringement and to prevent the infection from malicious software within Birmingham City Council’s Network.

4. SECURITY RISK

Malicious software would, if not stopped, compromise the confidentiality, integrity and availability of information and systems (see the *Malicious Software Guidance* document for further information).

Birmingham City Council licenses the use of computer software from a variety of third parties. The software developer normally copyrights such software and unless expressly authorised to do so, Birmingham City Council has no right to make copies of the software except to create a backup or archive. Copyright law protects software against copying and distribution, even in the absence of a licence agreement. Under the Copyright, Designs & Patents Act 1988 those illegally reproducing copies of software may be liable for civil damages and subject to criminal penalties including fines and imprisonment. Both the person who made the illegal copy and the council could be prosecuted. Such action could cause damage to Birmingham City Council’s credibility and reputation as well as potentially resulting in significant legal costs.

STANDARD PARTICULARS

Birmingham City Council requires all Users of its equipment and information to respect computer software copyright and to comply with the terms of all software licences.

Service Birmingham manages the acquisition, maintenance, registration, installation, transfer and removal of all Software on behalf of Birmingham City Council, under the terms of their contract with Birmingham City Council. This is done in compliance with copyright legislation and licensing agreements.

Software is approved by both Birmingham City Council and Service Birmingham^V.

5.1 Software acquisition, purchase and approval

All Software must be approved by Birmingham City Council and Service Birmingham before it is purchased or installed.

- Service Birmingham tests the software before it is placed on the approved list^{VI} for compatibility with other City and Service Birmingham systems and equipment.
- Software acquisition is also controlled in order to check that it is purchased from reputable, authorised sources.
- Only Software which is capable of being upgraded and patched with security improvements may be installed.

A complete record of all approved Software for Birmingham City Council use, both standard and non-standard, is maintained by Service Birmingham. Users who have a business need for non-approved Software which is not in the approved list catalogue, must follow the Service Birmingham Non-Standard Product Management Process in order to request it.

Birmingham City Council will not purchase, install or register any software without the approval and authorization of Service Birmingham. Service Birmingham on behalf of Birmingham City Council will also purchase, install and register all Software approved by the City and Service Birmingham.

Service Birmingham will only provide support for software that has been acquired in accordance with the principles in this Standard.

All requests for the acquisition of Software for Users must be passed to an Approved Budget Holder for authorisation. After the costs are authorized, Software requests must be directed to Service Birmingham for approval, further authorization, purchase and installation.

Users must never install unauthorized software, or any software owned or licensed to parties other than the City or Service Birmingham, on equipment owned or managed by Birmingham City Council or Service Birmingham.

When council owned information is Processed on equipment not owned by the city and not managed by Service Birmingham, the Software used on such information must still be approved and authorized by both Service Birmingham and Birmingham City Council.

^V This is carried out in line with the ISO20000 Standard for IT Service Management.

^{VI} An approved list of software is kept by Service Birmingham and is available on request. Telephone the Service Desk (4-4444) and ask for a copy of the "COTS" (Commercial Off-The-Shelf) applications approved catalogue in the repository "SB Docs".

5.2 Software Registration

When software is delivered, it must be delivered to Service Birmingham who will store all software installation media^{vii}. All Users in possession of copies of Software on any medium must make sure the medium is passed to Service Birmingham without delay.

Service Birmingham must complete the registration and inventory requirements for all software. Service Birmingham will complete registration cards or similar formalities and return any information to the software publisher which is required under the terms of any licence, warranty or contract.

All Software must be registered in the name of Birmingham City Council or Service Birmingham, as appropriate.

A copy of all licence agreements (in electronic or hard copy form) must be held by Service Birmingham for the period determined by agreement between Birmingham City Council and Service Birmingham.

Service Birmingham will, where it is available, make manuals, tutorials and other materials available to Users.

Service Birmingham also stores licence keys wherever particular software includes a key as part of its associated access control. Both software and licence key is stored securely and is only accessible to Service Birmingham staff whose job role requires this access.

Service Birmingham on behalf of Birmingham City Council will keep a complete record of Software in the Software Asset Register: for example, this would include application software, system software, development tools and utilities.

The minimum detail that must be documented within the Software Asset Register is:

- A description of the software.
- The date and source of software acquisition.
- The Asset Number of any hardware where a copy of the Software is installed.
- Where the master copy is kept in the DSL.
- The Software product serial or licence number(s).
- Details of any upgrades or modification applied to the software.
- Where the software is supplied to third parties as part of a contract, the contract details and, if appropriate, the period of supply agreed.

^{vii} For example, DVDs, disks, USBs, etc..

5.3 Installation and Maintenance and Use of Software

Service Birmingham will install all software on behalf of Birmingham City Council.

Upon receipt of new software media, Service Birmingham will load the software into the DSL, which will be used as the master source for all installations^{viii}.

Service Birmingham is responsible for providing or commissioning software support and will make sure that upgrades (or “patches”) are received as often as is reasonably necessary for standard approved software on council or Service Birmingham premises. However, Users must take the initiative themselves and ask Service Birmingham to upgrade and patch non-standard software. In the case of agile or home workers using their own equipment, they are themselves responsible for installing new patches for protection against malicious software themselves. Other software on privately owned equipment must be installed by Service Birmingham or under Service Birmingham instructions.

Software installed on Birmingham City Council or Service Birmingham equipment must be used in accordance with the purpose of this Standard. All Users who access council information or equipment must be authorised to do so and must have an individually designated identity within the Network^{ix}.

5.4 Removal or Transfer of Software

Software may be lost if it is installed on equipment that is lost. All council and Service Birmingham staff, volunteers, elected members and anyone else engaged on council business must report all lost, stolen or found digital equipment to the Performance and Information team^x. This team will report the lost kit to Service Birmingham to enable them to update the Software Asset Register.

Anyone who wants to request the removal or transfer of software must contact Service Birmingham Service Desk^{xi}.

Software removal or transfer includes a requirement that Service Birmingham updates the Software Asset Register so that the licensed use is tracked.

Service Birmingham alone will handle all transfers of Software between different pieces of digital equipment^{xii}. Service Birmingham alone will remove Software from digital equipment^{xiii}.

Users who have equipment surplus to requirements should follow the *Cascading of Surplus Equipment Policy* so that software can be recovered and reused.

^{viii} Very occasionally, new software is approved from an Internet source and Service Birmingham will install it directly from the internet; in this case a master copy is not kept but the source is recorded instead.

^{ix} The network identity is the identity managed in Active Directory: Software that centrally controls user identities in one repository as well as policies which determine the access privileges for those identities.

^x Follow the Information or Loss of Equipment Containing Information Standard

^{xi} Telephone 4-4444

^{xii} in line with the software licence agreement and this Standard and updating the Software Asset Register where appropriate..

^{xiii} in accordance with the council's Disposal of Information Processing Equipment Standard.

5.5 Malicious Software

Malicious Software is computer program code which is designed to infiltrate and damage our digital information systems, to stop systems running properly, or to steal information. It includes viruses, spyware and other computer code^{XIV}.

Users must follow the following rules to prevent the infection and spread of malicious software within Birmingham City Council's Network.

5.5.1 Computers owned by Birmingham City Council

Users must connect council owned equipment to the Network at least once a month, so that it receives the latest security software automatically; unless they have an agreed absence from work. If Users are absent by agreement they must immediately connect to the council Network to update their anti-virus software on their return.

Users must not change the settings on any security software managed by Service Birmingham. Users (except the general public) should contact the Service Desk^{XV} if they need a change to their security settings.

All council equipment used remotely^{XVI} to access information governed by the GCSx Code of Connection, must have personal firewalls (security software that stops malicious software infection) installed locally. Users must not alter the settings on these firewalls. (Note that GCSx information must, under current rules, only be accessed by council equipment located within the council's Network).

5.5.2 Computers and computer devices not owned by Birmingham City Council

Whenever any equipment, regardless of who owns it, is connected to the council's Network, it must have anti-virus defences provided by the approved supplier^{XVII} and must be up to date. All software must be patched (see 5.3 above). Service Birmingham Service Desk will not support non-compliant equipment or software.

Home and agile workers who are permitted to use their own equipment are personally responsible for keeping the approved supplier anti-virus software up to date.

Any manager within Birmingham City Council or Service Birmingham, who authorises an external party to access equipment or Networks managed by Service Birmingham or owned by Birmingham City Council, is responsible for making sure that the third party complies with this Standard and that they have up-to-date patches for all software and operating systems^{XVIII}.

Equipment which is not owned by Birmingham City Council must not be connected to any equipment which is used to process information governed by the GCSx Code of Connection.

^{XIV} See the Malicious Software Guidance.

^{XV} Service Desk telephone 4/4444

^{XVI} Remote access includes all mobile access under the terminology of the GCSx Code of Connection. For the definition of remote access, see the Flexible and Remote Access Standard.

^{XVII} Approved Anti-Virus supplier is Sophos as at September 2011; or an alternative if authorized in writing by Management.

^{XVIII} See the third party compliance requirements set out in the Flexible and Remote Access Standard and ask Service Birmingham to review the arrangements.

5.5.3 GCSx connections

If a User has any remote access^{XIX} to information shared with the Government and governed by the GCSx Code of Connection, they must always use Birmingham City Council owned equipment and cannot use their own, or third party owned, equipment. The equipment used to connect to the Government information must be protected by Two Factor Authentication, where one factor is encryption from an approved encryption service^{XX}. Remote equipment connecting remotely to Government information must be locked down (this means that local functionality including use of the local hard drive (longer term storage within the equipment) and sockets for connections to disks or memory sticks and other connections must be disabled). Mobile equipment must include a personal firewall.

Any requests for unlocked equipment or user-configured desktops will be denied wherever a GCSx connection is in place.

The council reserves the right to deploy network access controls which will check the provenance, antivirus software and security of all devices connected to the council's Network. It reserves the right to disconnect devices which are vulnerable to malicious software, to update the anti-virus protection on all connected devices and to monitor and investigate any unauthorised equipment connections. The council also reserves the right to use intruder detection systems and to disconnect unauthorised devices from the council's Network. Intruder detection and Network access control may be carried out for the council by Service Birmingham.

5.5.4 All Peripheral devices connected to the Network^{XXI}

All digital storage devices in this category, such as memory sticks, ipods, external drives, cameras, palm-held devices, etc, as well as portable computers such as laptops, should all be scanned for malicious software whenever they are connected to any of the council's computers or Networks. This must be done even if the peripheral is brand new.

The User connecting the device must run a scan immediately after connecting it to the Network. Users must right-click on the shield at the bottom-right hand corner of their computer screen in order to run the anti-virus software^{XXII}.

Peripheral devices must be provided by a trusted source and their use must be authorised by Birmingham City Council management. It is therefore not permitted for Users to connect personally owned devices to council computer equipment without express permission from management.

The Network Access Controls described under item 5.5.3 above also apply to peripherals.

^{XIX} Remote access includes all mobile access under the terminology of the GCSx Code of Connection. For the definition of remote access, see the Flexible and Remote Access Standard.

^{XX} Approved encryption includes the Credant encryption software at September 2011. All laptops should have this installed.

^{XXI} ***This category does not include security peripherals provided by Service Birmingham containing an operating system (for example, a secure operating system on a USB stick) which will also have malicious software protection where necessary, but managed by Service Birmingham.***

^{XXII} The scanning process can also happen automatically or can be initiated by Service Birmingham.

5.5.5 Software Control

Many malicious software programs lie hidden within other computer information: usually within software instructions, but possibly within pictures or documents. Software can unwittingly be downloaded by users who open file attachments on e-mails or visit website addresses. The rules that prevent infection in this way are set out in addition to this standard in the *E-mail Use Code of Practice* and the *Internet Use Policy and Code of Practice*.

Where GCSx information is processed, any unauthorised software must be prevented from executing. If unauthorised software is detected, this must be reported as a security incident (see the *Malicious Software Guidance*)^{xxiii}.

^{xxiii} Service Birmingham Security 3-4743, will give advice on whether a GCSx connection is sufficiently Secure.

6. ROLES AND RESPONSIBILITIES

Role	Responsibility
Service Birmingham	Contractual responsibility for the management of all Software on behalf of Birmingham City Council.
BCC Corporate Management Team	Overall responsibility for the management of the council's assets.
Birmingham City Council Performance and Information Division – Information & Strategy Manager	<p>Make sure the Software Control Standard meets the business need and is reviewed annually.</p> <p>Carry out or commission audits to monitor compliance with this Standard.</p>
Managers employed by Birmingham City Council	<p>Management of Software at a local level.</p> <p>Make sure all new Software within their section is properly authorised and licensed in line with this Standard.</p> <p>Make sure staff within their control are aware of the Software Control Standard.</p> <p>Use contractual provisions to require third parties and external agencies working in partnership with the council to comply with this Standard where reasonable.</p> <p>Report any breach or suspected breach of this Standard to Service Birmingham Service Desk for investigation.</p>
Birmingham City Council Staff (Permanent, temporary, casual and seconded employees) Elected Members and volunteers	<p>Must not give software used by Birmingham City Council to any third parties, including contractors and customers.</p> <p>Must not use on any Birmingham City Council computer equipment software that has not been provided via Service Birmingham and authorised by Birmingham City Council.</p> <p>Must not install Software on any Birmingham City Council computer system.</p> <p>Must pass any master copies of software in their possession to Service Birmingham without delay.</p> <p>Must report to their management any installation, distribution, use or copying of Software in breach or suspected breach of this Standard.</p> <p>Must report any lost or found *** equipment or Software.</p>

7. MONITORING

To monitor compliance with this Standard, audits will be carried out by council staff or by Service Birmingham.

8. ENFORCEMENT

Any individual member of staff found contravening this Standard or jeopardising the security of information that is the property of Birmingham City Council may be investigated under the council's investigation access procedure or disciplinary procedure and, where appropriate, legal action may be taken.

Third parties or partner organisations found contravening this Standard or jeopardising the security of information that is the property of Birmingham City Council may be investigated and, where appropriate, legal action may be taken. Contractual provisions may allow the access granted to third parties to be terminated without notice for a period reasonably considered necessary to protect systems or information from serious risk of damage or breach of security requirement or statutory obligation from malicious or defective Software.