Information and Cyber Security Standard

Document Owner:	Jackie Woollam Head of Strategy & Governance Team, BCC
Version:	1.0
Date of this version.draft:	December 2015
Policy change in this version.draft:	No policy rule change. The use of the term cyber security is added and defined to address audit requirements but cyber security carried out as before.
Date last version approved:	August 2015
Date version approved	December 2015
Classification	
Contact:	Mr David Thomas
Title	ICF Manager 10 Woodcock Street Birmingham B2 2YY Tel: 454 2877/ 675 1431
Author:	M Westrop, Information & Cyber Security Manager

Table of Contents

1. The purpose of this standard and Information Security and Cyber Security defined

The purpose of the Information and Cyber Security Standard is to protect the information held by Birmingham City Council on behalf of the people it represents and in the national interest and to emphasise the importance of both Information and Cyber Security to the Staff working for the council.

Information Security is the preservation of confidentiality, integrity and availability of information as required by law.

Cyber Security is the defence of both digital information and all the equipment used to hold that information. Cyber security is required continually to fend off constant attack and to reduce vulnerability to future attacks.

2. Scope

This standard applies to all information and all the equipment used to hold that information and to all staff.

See also conditions of use applicable for some services to the public.

3. Definitions

Capitalised terms, acronyms and their origin are explained in the separate document, "*BCC Basic Definitions for Information and Cyber Security Policies and Standards*."

4. Who is responsible for information and cyber security

4.1 Responsibility for practising correct information security

It is the responsibility of all staff to comply with the Standard and the detailed rules and guides.

Additionally, BCC makes all managers directly responsible for implementing information and cyber security policies (see detailed rules and guides, below) within their business areas.

Managers must follow, and also require their staff to follow, these policies. Birmingham City Council undertakes to provide appropriate information security training for all staff including Elected Members.

See also the rules for public groups, below.

4.2 Responsibility for the management of security

Birmingham City Council manages corporate information security and cyber security and put the security strategy, into practice.

The security function is the responsibility of two dedicated areas which work in collaboration with each other and with staff and with third party partners:

1. the Strategy, Policy and Business Security team, within Service Birmingham;
2. and the Intelligent Client Function ("ICF") team within Birmingham City Council.

ICF have overall responsibility for the provision of adequate information security and cyber security on behalf of BCC and work under BCC management.

Strategy, Policy and Business Security are a dedicated resource under Service Birmingham management who work to provide an information security and cyber security service to BCC. This team reports on cyber risks to the separate risk management process.

Information and cyber security management is a requirement of the joint venture between BCC and Service Birmingham and its details are refined in particular collaborative procedures where the demarcation of duties between the two teams is set out[1].

Specific duties and responsibilities are also allocated to particular roles in the council such as system owners, SIROs, IAOs[2]. For example, each system owner must identify and document the availability requirements of their systems and formulate a contingency plan in the event of system failure. These form part of the overall emergency plan determined by senior management and co-ordinated by the chief executive.

BCC's audit team is responsible for independently evaluating information security measures and for reporting upon the effectiveness of the controls in place.

[1] For example, the SB Lost Equipment or Data Procedure available from Service Birmingham.
[2] See the BCC Information Assurance Framework available on the Intranet.

5. Principal policy obligations

The task of security management comprises a mixture of active operations to avert and mitigate attacks, defensive and cautionary planning and operations, strategic appraisal and assurance.

5.1 Cyber-operations and incident management.

- Security management, third party partners and technical staff will deploy cyber security continuously to fend off constant attack, using a Defence in Depth strategy.

- Information and cyber security management will respond to emerging threats in collaboration with other departments in order to defend the council from cyber-attack.

- All staff have a duty to report suspected breaches of information security policies and standards to management[3].

5.2 Defensive planning & collaboration

- It is the council's policy that all staff have a duty to be mindful of information and cyber security rules and principles which are set out in published policies, contractual obligations, management instructions and specialised training courses.

- Security management will work collaboratively with all areas of the council and with third parties on security matters.

- Directorate management are required to work with information and cyber security management to preserve an appropriate level of confidentiality, integrity, availability and security for all information and all digital systems.

5.3 Assurance, governance and risk

- Information and cyber security management are responsible for monitoring compliance with the standards, taking corrective action and producing an annual assurance statement for the audit department.

- The information and cyber security management function must also provide technical and policy-based guidance, policy documents and must advise staff and others representing certain public interests, on best practice. They may also provide information security training for Staff and improve Staff understanding of current risks which will continually change and grow.

- This policy and its related standards should be interpreted consistently with guidelines laid out in ISO 27002:2013 and the relevant parts of the Government's *Security Policy Framework*[4].

[3] See the BCC Incident Response Standard and associated questionnaire.

[4] See July 2014 https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

6. Detailed rules and published guidance that underpin this overall policy document.

This document is a statement of policy and deals in broad principles. Important detail is set out separately in other documents, available on the Intranet or from IT & Digital Services, the most important of which are:

Issued by	Name of document	Main areas covered
BCC	Access Control Standard	User identification, access privilege management, password use
BCC	Compromised User Procedure	Procedure to manage the misuse of user identities and passwords
BCC	Data Protection Policy	Rules for the fair processing of personal information
BCC	Disposal of Information Processing Equipment Standard	Rules for BCC or its contractor to recycle or dispose of the Council's surplus or redundant equipment securely.
BCC	Email and messaging policy and code of practice	Rules of conduct for the use of the council's messaging services
BCC	Freedom of Information Code of Practice	Rules to make documents held by the council available to the public
BCC	Information Assurance Framework	Responsibilities of the SIRO, IAO and others
BCC	Information Classification and Data Storage Standard	Key principles for the classification and protection of information
BCC	Information Incident Response Standard	Rules, reporting responsibilities and standard questionnaires for handling information security incidents
BCC	Internet Use Policy and Code of Practice	Rules of conduct for internet users.
BCC	Monitoring Standard	BCC's policy for monitoring at work
BCC	Investigation Access Procedure[5]	Rules for the conduct of an investigation into wrongdoing, the impact assessment and treatment of evidence.
BCC	Software Control Standard	Rules for legal and security compliance in the software lifecycle and for the prevention of malicious software
SB	13.01 Application Development – a technical policy	A technical list of software development and testing rules
SB	13.09 Network Security Management Checklist	A technical checklist for best practice in network security to protect infrastructure and information on the network.
SB	13.22 Physical Access Control Security Policy	Rules for access to Service Birmingham premises & sets out rules for operating CCTV at these sites.
SB	13.33 ICT Software Patch Management Policy	Rules for all SB managed digital processing to deploy optimal virus protection software; current virus definitions, malware signatures and other identification libraries; the most recent operating systems and security patches; software upgrades and fixes.
SB	ICT DR Policy	Policy for Disaster Recovery plans and procedures

[5] This does not include operations conducted under the Regulation of Investigatory Powers Act which are not part of the Information Security operations but fall under legal and audit areas.

7. The context of this standard and corporate strategy

The policy carries through corporate strategy[6]:

> *"to protect …the organisation from security threats and provide a robust platform of solutions".*

The corporate strategy points out major changes affecting information and cyber security:

- a spending review;
- changes in benefits systems;
- digital integration with health service systems;
- changes in education and in the governance arrangements for schools
- "Channel shifts"[7] in the use of technology.

Against this background, the following areas are important to the Information and Cyber Security Policy:

1. **Risk, governance, responsibility.** The IT/IS strategy recognises –
    a. that while it is challenging to identify risks when information technology services are changing , the council's overall Risk Management Strategy[8] mandates a risk-based-approach in all aspects of the organisation governance.
    b. the use of risk owners ("SIRO"), information asset owners ("IAO") and others to identify who is responsible for allowing access to information and for reporting information security incidents[9];
2. **Collaboration with third parties.** The IT/IS strategy emphasises–
    a. interconnectivity through the Government's PSN is a "major driver" for information security;
    b. security requirements in an environment where information data is increasingly shared among organisations; and much of that sharing takes place across the internet (for example, by encrypted, secure email);
3. **Regulation and legislative change.** The IT/IS strategy emphasises–
    a. the challenge of "meeting the increasingly onerous requirements of external compliance with information security standards";
4. **Technological change, particularly with regard to agility.** The IT/IS strategy emphasises–
    a. significant changes in the way in which the ICT industry now develops and deploys systems and services;
    b. improved methods available for agile, remote and mobile work practices.

[6] CORPORATE INFORMATION SYSTEMS/INFORMATION TECHNOLOGY AND INFORMATION STRATEGY v.8.0
[7] Channel shifts are self-service options on the web and other applications for council tax business, management reporting, election results publication, other transactions.
[8] See the Risk Management Strategy 2015 available from IT & Digital Services.
[9] See the BCC Information Assurance Framework available on the Intranet.

8. Public groups who use IT services provided by the council

Certain groups, outside the control of BCC management, may be permitted to use BCC's information technology services. For example, certain libraries provide the public with internet access and certain areas are covered by BCC supplied wireless connectivity. The conditions of use and security measures in place for the public will fall under the remit of the information and cyber security management, with advice from BCC's legal department.

9. Non-conformity and breaches of this standard

There are no exceptions to this standard. Any employee who disobeys this standard may be investigated under the council's disciplinary procedure and, where appropriate, legal action will be taken. Anyone, whether they are an employee or not, who disobeys this standard, may have their access to information or equipment withdrawn.

End