Business Services Organisation

BSO ICT SECURITY POLICY

(version 1.0)

Approved at BSO Board on 25th February 2010

CONTENT

1. Scope

1.1. The BSO Board has agreed to the adoption of this ICT Security Policy.

1.2. The policy is based on the HSC ICT Security Policy and applies to all staff, including regular full-time, regular part-time, contractors, consultants, agency and temporary employees.

1.3. Where not explicitly mentioned within this policy or the supporting documents listed below, reference should be made to the HSC ICT Security Policy for direction as it mandates the minimum ICT security standards to be applied to HSC organisations.

2. Purpose

2.1. The purpose of this policy is to ensure a consistent and high standard of ICT security across the HSC community from all threats whether internal, external, deliberate or accidental.

2.2. The data stored and processed within the many HSC information systems represents one of HSC's most valuable assets so there is a need to develop an environment within which information systems and networks are secure and efficient.

2.3. Within the HSC information system, staff handle information which may be potentially sensitive and, on many occasions highly confidential. All HSC staff who develop, operate, maintain or use ICT have an explicit and legal obligation to preserve the security of those systems.

2.4. This policy and associated guidelines aim to provide direction in relation to safeguarding the integrity and confidentiality of information held on the HSC's information systems. As the requirement to share information electronically with external bodies increases, it is essential that its integrity and confidentiality is ensured.

2.5. The BSO Records Management policy should be referenced for further information on information management.

3. Organisational Structure

3.1. The Chief Executive is ultimately responsible for the secure operation of that organisation's information systems.

3.2. The HSC ICT Security Manager based in the BSO has the day to day responsibility for ICT security.

3.3. For each information system, an individual is identified as the System Manager. Part of the duties involves looking after security for that

system and reporting on security matters to the HSC ICT Security Manager.

3.4. All ICT users have responsibility to comply with this policy, attend recommended awareness training sessions and notify the HSC ICT Security Manager where breaches have come to their attention.

3.5. Template role summaries are listed in the HSC ICT Security Policy.

4. Data Classification

4.1. All staff must be careful when handling any HSC information and especially when dealing with sensitive or personal data.

4.2. Guidance on the use of identifiable patient/client information is given in *The Code of Practice on Protecting the Confidentiality of Service User Information* document issued by DHSSPS in January 2009.

4.3. The document can be found on the DHSSPS web site http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf

4.4. Examples of sensitive and personal information include but are not limited to:-

- copies or extracts of data from clinical systems;
- commercially sensitive information;
- contracts under consideration;
- budgets;
- staff reports;
- appointments – actual or potential not yet announced;
- disciplinary or criminal investigations.

4.6. Personal data is further defined by the Data Protection Act (1998).

4.7. Under **no circumstances must person identifiable, business confidential or sensitive information** be stored on unencrypted laptops, PDA's or any type of removable media[1].

5. Third Party Access

5.1. Where IT support on an information system is provided by a third party contractor i.e. not BSO-ITS, then this access must be approved by the HSC ICT Security Manager.

5.2. Details of the approved connection methods are found on the ICT Security Section of the HSCWeb website.
link - http://hpssweb.n-i.nhs.uk/security/website/index.html.

[1] Removable media includes but is not limited to USD data pens, optical discs (Blu-ray, DVD, CD), memory cards, floppy/zip disks, magnetic tape and external hard disk drives.

6. Data Transfers

6.1. Staff must follow the HSC Data Access Agreement procedure, detailed in the HSC Data Access Agreement document, before any critical or sensitive data (including software escrow agreements) is exchanged (whether electronic or manual) between HSC organisations and/or outside organisations.

6.2. Either Section B (wishing to access) or Section C (holding the data) must be approved by the BSO Data Protection Manager.

6.3. Section E – Access Authorisation must be approved by the Assistant Director (IT Services) or the HSC ICT Security Manager.

7. Encryption key management

7.1. Where encryption is applied, the data file and password should not be sent by the same route. For example if the data file is sent be email, then the password should be sent to the recipient by SMS text or a phone call.

7.2. Further information on the use of encryption can be found in the Use of ICT Equipment document.

8. Conflicts of Interest

8.1. Employees must declare any conflicts of interests. For instance, an individual working in ICT procurement should make it known if he/she or any close relative has direct interest in a potential supplier.

9. Disposal of Equipment and Media

9.1. Secure disposal of ICT equipment and removable media must be arranged or approved by BSO-ITS to ensure all the security, legal and audit requirements are meet.

10. Loss or Theft of Equipment or Data

10.1. All staff are required to report immediately the loss or theft of any of the following to the HSC ICT Security Manager;

- Desktop computer, laptop, server, printer, removable media, palmtop computer, PDA, Blackberry device, mobile phone, or other such mobile IT device.

- Papers or electronic data files containing person identifiable data about any individual.

11. Supporting Policies

11.1. The HSC ICT Security Policy provides the lead on all ICT security requirements.

11.2. The following policies have been developed and all staff are required to follow them:

- Use of ICT Equipment
- Use of the Internet
- Use of Email
- Clear Desk and Screen Policy
- HSC Data Access Agreement

11.3. They can be found on the BSO intranet.

12. Equality Screening

12.1. This policy and those listed in Section 11 above have been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and for compliance with human rights and disability legislation. Documentation to evidence the screening has been produced and is publicly available.