Business Services Organisation

Information Security Policy

Produced by the Human Resources and Corporate Services Directorate
Business Services Organisation
2 Franklin Street, Belfast, BT2 8DQ

Reference No:

Title:	Information Security Policy		
Author(s):	Alan McCracken		
Ownership:	Director of Human Resources and Corporate Services		
Approval By:	BSO Board	Approval Date:	24/05/2018
Operational Date:	24/05/2018	Next Review:	24/05/2020
Version No.	3.0	Supersedes:	2.0
Key Words:	Information Governance, Data Protection, Information Security, Freedom of Information		
Director Responsible:	Director of Human Resources and Corporate Services		
Lead Author:	Alan McCracken		
Lead Author Position:	Data Protection Officer		
Additional Author(S):			
Department:	Corporate Services		
Contact Details:	dpa.bso@hscni.net		
Links to other Policies:	Information Security Policy		
	Data Protection & Confidentiality Policy		
	Freedom of Information Policy		
	Records Management Policy		
	Incident Reporting Policy		

Table of Contents

1 Introduction

1.1 Due to the sensitive and confidential patient and personal data captured, along with commercially sensitive information, and the reliance on information systems to process and transmit data to stakeholders, Information Security (IS) is fundamental to the operation and success of all HSCNI bodies and of paramount importance to meet the organisations' primary objectives.

1.2 All organisations are obliged to abide by all relevant UK and EU legislation, and best practice guidelines. This includes

- General Data Protection Regulation (GDPR) 2016
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Re-Use of Public Sector Information Regulation 2005
- Access to Health Records (Northern Ireland) Order 1993
- Human Rights Act 1998
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Health and Social Care (Reform) Act 2009
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioners Office (ICO)
- The Department of Health (DoH) Good Management, Good Records (GMGR)

1.2 This policy:

- applies to all business functions and covers all information systems, networks, physical environment and relevant people who support those business functions
- sets out the policy for the protection of the confidentiality, integrity and availability of their information assets
- establishes the security responsibilities for information security
- outlines the approach to information security management
- describes the responsibilities necessary to safeguard the security of information

2 Purpose

2.1 The objectives of this policy are to:

- ensure the security of information assets
- ensure that information assets are available as and when required, in order to meet business objectives
- protect information assets from unauthorised or accidental modification or destruction or unauthorised disclosure, in order to ensure the accuracy and completeness of the information assets
- minimise risk to information.

2.2 The aim of this policy is to establish and maintain the security and confidentiality of Information assets by:

- ensuring that all members of staff are aware of, understand and fully comply with the relevant legislation as described in this and other policies
- describing the principals of information security and explaining how they will be implemented
- introducing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities
- creating and maintaining a level of awareness of the need for IS as an integral part of the day to day business
- protecting information assets
- informing the Chief Executive to assist with the statement of internal control
- protecting the signatory bodies from liability or damage through the misuse of its information.

3 Scope

3.1 This policy relates to the use of all organisation-owned information assets (both physical and system based), network applications, to all privately owned systems when connected directly or indirectly to the network and to all organisation-owned and/or licensed or sanctioned software/data and equipment. This includes, but is not necessarily limited to:

- stored on computers
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten on paper, whiteboards (etc.)
- sent by facsimile (fax), telex or other communications method
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- paper and electronic structured records systems
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

3.3 This policy covers all forms of information held, including (but not limited to):

- information about members of the public
- staff and personal information
- organisational, business and operational information.

3.4 This policy covers all information systems purchased, developed and managed by/or on behalf of the signatory bodies.

3.5 This policy applies to all directorates, services and departments, all permanent and temporary staff, all agency workers, and as appropriate to contractors and third party service providers acting on behalf of the signatory bodies.

4 Responsibilities

4.1 The Chief Executive Officer (CEO) is the **Accountable Officer** and has overall responsibility for ensuring that information security is applied.

4.2 The **Personal Data Guardian (PDG)** is responsible for acting as a central point of contact on IS

4.3 The **PDG** is responsible for:

- ensuring that the IS policy is produced and kept up to date
- producing operational standards, procedures and guidance on IS matters for approval by the Information Governance Management Group (IGMG)
- co-ordinating IS activities, particularly those related to shared information systems or ICT infrastructures
- reporting to the IGMG on matters relating to IS

4.4 The **Senior Information Risk Owner (SIRO)** will be responsible for managing and implementing information security policies and procedures

4.5 The responsibilities of the **Information Asset Owners (IAOs)** include:

- leading and fostering a culture that values, protects and uses information appropriately
- knowing what information is held, and what and how information is transferred
- knowing who has access to each information asset, and ensuring that access / use of each information asset is monitored and controlled
- understanding and addressing risks to IS and providing assurance to the SIRO
- ensuring any data breach incidents are appropriately reported and managed

4.6 The responsibilities for the **Data Protection Officer (DPO)** include the provision of support to all staff in conducting their delegated responsibilities, and liaising with the ICO as required.

4.7 **Managers** are responsible for:

- overseeing the implementation of IS within their area of responsibility
- agreeing, alongside ITS, the most appropriate system security policies for each information system
- the security of the assets is consistent with legal and management requirements ensuring that systems are tested and agreeing subsequent rollout plans
- advising SMT on the accreditation of systems, applications and networks
- providing a business area point of contact on IS issues
- contacting the relevant director / assistant director when
    - incidents or alerts have been reported that may affect systems, networks or applications
    - proposals have been made to connect to systems, networks or applications that are operated by external parties
- ensuring that staff are aware of their security responsibilities and have had suitable training.

4.9 The **ICT Security Manager** has day to day responsibility for ICT Security. This includes the maintenance and review of the ICT Security Policy and subordinate policies and procedures.

4.10 **All Staff**, whether permanent, temporary or agency workers, or agents acting for or on behalf of The Organisations are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with this policy. This includes:

- the operational security of the information systems they use
- preventing the introduction of malicious software on ICT systems
- reporting on any suspected or actual breaches in security

5 Policy Framework

5.1 **Supporting Policies, Codes of Practice, Procedures and Guidelines** have been developed to strengthen and reinforce this policy. These are available for viewing on the BSO's website.

5.2 Human Resources

5.2.1 **Training**: Information security awareness training will be included in the staff induction process. An on-going awareness programme will be established in order to ensure that staff awareness is refreshed and updated as necessary.

5.2.2 **Contracts**: Security requirements will be addressed at the recruitment stage and all contracts of will contain an appropriately worded confidentiality clause. Information Security Requirements will be included in job descriptions.

5.2.3 **Contracts with external contractors** must be in operation before access is allowed to information systems, and must include clauses about information and ICT security and protection. These agreements will require staff or sub-contractors of the external organisation to comply with all appropriate security policies.

5.3 Asset Security

All ICT equipment and equipment for the handling of information will:

- be recorded on the corporate registers
- be physically protected from security threats and environmental hazard
- have a named custodian who will be responsible for the security of that asset.

5.4 **User Access Controls**: Access to ICT equipment, systems and information will be restricted to authorised users who have a business need to access the information.

5.5 **Computer and Network Procedures**: Management of computers and networks will be controlled by standard procedures.

5.6 **Security Incidents**: All security incidents are to be reported to the ITS Security Manager or the DPO. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

In the event of a suspected or actual security breach the SIRO may, after with the relevant senior staff, authorise action to remove or restrict access to systems, facilities and information or anything else deemed reasonable to secure information.

5.7 **Protection from Malicious Software**: The BSO will use software countermeasures and management procedures to protect itself against the threat of malicious software. Users must not install software on computing assets without approval.

5.8 **Removable Media**: Removable media must be approved for use, and encrypted and fully virus checked before being used on ICT equipment.

5.9 **Accreditation of Information Systems**: All new information systems, applications and networks must be compliant with organisational requirements and include a security policy and plan that is agreed by the PDG or, if unavailable, the relevant Director before they commence operation.

5.10 **System Change Control:** Changes to information systems, applications or networks must be reviewed and agreed with the appointed IAO and the SIRO/Data Guardian.

5.11 **Intellectual Property Rights:** The BSO will ensure that all information products are properly licensed and approved by ITS. Staff must not install software on computing assets.

5.12 **Business Continuity and Disaster Recovery Plans**: The BSO will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

5.13 **Reporting:** The DPO and the ICT Security Manager will keep the SIRO/Data Guardian, SMT and IGMG informed of the information security status by means of annual reports.

6 Performance and Monitoring Compliance

6.1 The effectiveness of this policy will be assessed on a number of factors including the management (including frequency) of information security breaches, including near misses.

6.2 The BSO will audit information security management practices for compliance with this policy. The audit will:

- identify areas of operation that are covered by this policy
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the management of information security, and use a subsidiary developmental plan if there are major changes to be made
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
- highlight non-conformance
- report the audit results to SMT and IGMG.

7 Non-Compliance

7.1 A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

7.2 Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

8 Review

8.1 This policy and all associated documents within the Information Governance Framework will be reviewed no later than two years from approval, to ensure their continued relevance to the effective management of information governance within the BSO.

9 Equality Statement

9.1 In accordance with the BSO's Equal Opportunities Policy, this policy will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.