Business Services Organisation

Information Risk Policy

Produced by the Human Resources and Corporate Services Directorate

Business Services Organisation

2 Franklin Street, Belfast, BT2 8DQ

Reference No:

Title:	BSO Information Risk 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:	Data Protection, Information Security, Information Risk		
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 Governance Policy		
	Information Security Policy		
	Records Management Policy		
	Policy for the reporting of adverse incidents, accidents, near misses and dangerous occurrences		
	Policy for the Safeguarding, Movement and Transportation of Records, Files and Other Media		
	Freedom of Information Policy		

Table of Contents

1 Introduction

1.1 Information is a vital asset, both in terms of the management of health and social care for individual service users and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

1.2 Information Risks are risks that relate to the loss, damage, or misuse of information or which threatens the confidentiality, integrity or availability of an information asset, especially information which is personal or confidential in nature.

1.3 Information risk is inherent in all administrative and business activities and everyone within the HSC continuously manages information risk. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks, and should not be seen as something that is the sole responsibility of Information Governance (IG) staff.

1.4 Information risk management is an essential component of information governance and is an integral part of continuous quality improvement. The aim of information risk management is to provide the means to identify, prioritise and manage the risks involved in all of the organisation's activities, and to embed this in a practical way into business processes and functions.

1.5 It is therefore of paramount importance to ensure that information risk is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.6 This policy and its associated sub policies and procedures define how information risk will be managed.

2 Purpose

2.1 The purpose of this document is to provide a risk management framework in which information risks are clearly recognised and the appropriate controls implemented in order to:

- protect the Business Services Organisation (BSO) ,its staff and clients from information risks where the likelihood of occurrence and the consequences are significant
- provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- encourage pro-active rather than re-active risk management
- provide assistance to and improve the quality of decision making
- meet legal or statutory requirements
- assist in safeguarding information assets
- seek to minimise the risk of information governance (IG) incidents from occurring through the misuse of personal and/or sensitive data
- manage and mitigate breaches of personal data

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 BSO 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

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

- Information about members of the public
- Non- employees on organisational premises
- Staff and Personal information
- Organisational, business and operational information

3.3 This policy covers all information systems purchased, developed and managed by/or on behalf of the BSO.

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

4 Responsibilities

4.1 The **Chief Executive is the Accountable Officer** and has overall responsibility for ensuring that information governance is applied throughout the organisation. He/she is responsible for ensuring that information risks are assessed and **managed to ensure information risk is reduced.**

4.3 The **Personal Data Guardian (PDG)** is responsible for:

- ensuring that the Information Risk policy is produced and kept up to date
- producing operational standards, procedures and guidance on Information Risk matters for approval by the Information Governance Management Group (IGMG)

- co-ordinating Information Risk activities, particularly those related to shared information systems or ICT infrastructures
- take a lead on confidentiality issues, acting as a champion for data at Board level ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for all staff

4.5 The **Senior Information Risk Owner (SIRO)** will be responsible for

- coordinating the development and maintenance of information risk management strategies, policies, procedures and standards
- ensuring that the approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- providing a focal point for the resolution and/or discussion of information risk issues
- on-going development and day-to-day management of the Information Risk Management Programme for information privacy and security
- taking ownership of risk assessment processes for information risk, including the review of an annual information risk assessment to support and inform the statement of internal control
- ensuring that risks to IS are reduced to an acceptable level by applying counter measures identified following an assessment of the risk for each asset
- advising the Accountable Officer and the BSO Board on information risk management strategies and provide periodic reports and briefings on programme progress
- ensuring that the Information Risk Management Policy supports the general risk management process

4.7 **Directors** are responsible for ensuring the local implementation of information governance and that they implement this and appropriate IG policies within their sphere of responsibility. This includes taking suitable management action should non-compliance arise.

4.8 **Directors** will ensure that **all Managers** are held accountable for making sure that their staff are aware of their roles and responsibilities in relation to managing information risk. They in conjunction with their Information Governance Lead will identify the level of training required for each member of staff and ensure that have time to carry out the appropriate level of training and have access to appropriate supervision and support.

4.9 **Information Asset Owners (IAOs)** are senior individuals who will:

- ensure that information risk assessments are performed quarterly on all information assets where they have been assigned ‘ownership’, following guidance from the SIRO on assessment method, format, content and frequency
- submit the information risk assessment results and associated risk management action plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks

- ensure information risk management is embedded into the key controls and approval processes of all major business processes and functions

4.10 **Information Asset Administrators (IAAs)** works in conjunction with and on behalf of the IAOs to:

- ensure policies and procedures are followed
- recognise actual and potential security incidents
- consult with their IAO on incident management
- ensure that information asset registers are up to date

4.11 **The Information Governance Manager (IGM)** has responsibility for:

- operational management of IG and for the implementation and co-ordination of the IG work programme, although responsibility for specific requirements is devolved to specialist leads and service managers
- providing advice and guidance on creating and maintaining the information risk management framework
- ensuring the information risk register is regularly reviewed by the IGMG

4.12 **The Data Protection Officer (DPO)** has responsibility for:

- informing the ICO of all serious adverse incidents relating to information governance, and reporting to the Information Governance Management Group (IGMG)
- liaising with external organisations on information risk matters
- reporting to the IGMG on matters relating to information risk

4.13 It is the responsibility of all **employees, agency workers, volunteers, contractors and subcontractors** to:

- ensure compliance with this and other information governance policies and procedures and must undertake annual training
- carry out their roles in accordance with this policy
- abide by the conditions detailed within this policy

5 Assessment of Information Risks

5.1 Information risk management is the process of identifying vulnerabilities and threats to information resources in achieving business objectives, and deciding what countermeasures, if any, to take based on the value of the information resource.

5.2 Identification and threat assessment of risks to information assets will be carried out in line with Risk Management Policy and the Risk Register.

5.3 BSO will take all reasonable steps to protect data whose release or loss could cause:

- harm or distress to clients, patients or staff
- damage to reputation or financial loss
- major breakdown in information systems, information security or information integrity
- potential for an IG incident requiring investigation

5.4 BSO will maintain an Information Asset Register (IAR) for each department which will be managed by each IAO for their area(s) of responsibility, in conjunction with the IAAs.

5.5 Each department will undertake an annual review of Information Flow Mapping and determine potential information risks regarding its data flows. The process will be managed by the IGM.

5.6 Risk Assessments will be conducted for all information systems and critical information assets. Information Risk Assessments should occur:

- within six months of issue of this policy, and on a six monthly basis thereafter
- at the inception of new systems, applications, facilities (etc.) that may impact the assurance of information or information systems*
- before enhancements, upgrades and conversions*
- when HSCNI / Department of Health (DoH) policy or legislation requires risk determination
- when required by the BSO Board.

** Those containing or which involve personal information require a Data Protection Impact Assessment as a part of the development process.*

5.7 Risk must be assessed in terms of the general level of harm that could be reasonably caused if data were to become compromised or unavailable. The risk assessment should cover:

- the balance between level of risk, tolerance of risk and the effort being used to manage the risk
- identification of gaps between the current and target risk positions
- progress being made against agreed information risk priorities
- the effectiveness of the risk management controls including successes and failures.

5.8 Information risk mitigation must be:

- commensurate with the level of risk
- kept simple so that it is manageable and can be communicated to staff
- supplemented with customised controls for specific high risk circumstances.

5.9 All significant findings should be recorded and action plans prepared. These should be available for audit.

5.10 Risk assessment tools and data protection compliance checklists will be made available by the IGM and the DPO.

5.11 Action plans should be recorded at service level meetings where information governance is a standing item on the agenda.

6 Information Incident Management

6.1 Security breaches, information loss or unauthorised disclosure, and other risks associated with information management will be managed in line with the BSO's overall adverse incident reporting processes and template. All such incidents must be documented on an Adverse Incident Form, and could involve:

- loss of patient information
- loss of staff information
- loss of business information
- loss of hardware
- virus or malware attacks
- unauthorised access to information assets
- misuse of access privileges.

7 Performance and Monitoring Compliance

7.1 Indicators that the policy is being enacted are:

- statutory reporting requirements are met
- assessments are completed
- no involvement of the ICO as a result of good practice.

7.2 Indicators for audit are:

- an identified IAO for each information asset
- an information asset register
- inclusion of information risks on risk registers
- number of information risks effectively mitigated and score reduced to lowest achievable.

8 Non-Compliance

8.1 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.

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

9 Review

9.1 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.

10 Equality Statement

10.1 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.