PBNI Probation Board for Northern Ireland

Information Assurance

Policy

Policy Owner	
Owner:	Head of Information Technology
Author:	Information Technology Security Officer
Screening and Proofing	
Section 75 screened:	*18 November 2015*
Human Rights proofed:	*17 November 2015*
Consultation	
	Union consultation – September-November 2015
Approval	
SMT:	*3 November 2015*
Board:	*11 December 2015*
Version	
Version:	1.0
Publication date:	
Implementation date:	*11 December 2015*
Review date:	*No later than December 2019*

Document uncontrolled when printed

Document Control

Version No.	Date	Description
0.1	September 2015	Union consultation
0.1	1 September 2015	Draft reviewed by SMT
0.2	November 2015	Union consultation
0.2	3 November 2015	Draft for approval by SMT
0.2	11 December 2015	Draft for approval by Board
1.0	11 December 2015	Approved by Board

Alternative Formats

This documentation can be made available in alternative formats such as large print, Braille, disk, audio tape or in an ethnic-minority language upon request. Requests for alternative formats can be made to the Probation Board using the following contact information:

Communications Department
Probation Board for Northern Ireland
80-90 North Street
Belfast
BT1 1LD

Telephone number: 028 90262400
Textphone: 028 90262490
Fax: 0300 1233290
E-mail: info@pbni.gsi.gov.uk

Contents

1. Rationale

This policy outlines PBNI's approach to providing the necessary assurance that PBNI's information systems will protect the information they handle under the control of authorised users to enable it to carry out its statutory function, in accordance with its statutory obligations.

PBNI recognises the duties and responsibilities it has, as a public sector organisation, to manage information appropriately.

These duties arise from the following legislation and the common law duty of confidentiality:

- Data Protection Act 1998.
- Human Rights Act 1998.
- Freedom of Information Act 2000 (incorporating Section 46 Lord Chancellor's Code of Practice on the Management of Records).
- Protection of Freedoms Act 2012
- Public Records Act (NI) 1923
- Cabinet Office Government Security Classifications (April 2014)
- The Disposal of Documents Order (S.R&O.1925 No.167)
- Electronic Communications Act (2000)
- Limitation Act (1980)
- Official Secrets Acts (1911 & 1989)
- Computer Misuse Act 1990
- Public Interest Disclosure Act 1998
- Interception of Communication Regulations 2000
- Copyright, Designs and Patents Act 1988
- All other relevant legislative authority

The Information Assurance (IA) policy focusses on the assessment and management of risk related to the use, processing, storage and transmission of information and the systems and processes used for those purposes. Information assurance includes the protection of the integrity, availability, authenticity and confidentiality of the user data with particular focus on the security of information systems, in digital and physical form. The Head of Information Technology Department is the Information Asset Owner (IAO).

This policy is linked directly to PBNI's Management of Information Policy which outlines PBNI's commitment to manage information effectively in accordance with the Data Protection Act 1998, Freedom of Information Act 2000, Common law duty of confidentiality, Human Rights Act 1998 and other relevant laws and regulations.

PBNI's Information Technology Department and Communications Department are key in contributing to information assurance and management within PBNI.

2. Aim

The aim of this policy is to ensure that PBNI's information systems will protect the information they handle and will function, as they need to, when they need to, under the control of authorised users. The policy applies to all information held by PBNI, whether manual or electronic, current or archived and all recorded information, in any form, created, received or maintained by PBNI.

All information held by PBNI should be managed effectively and held securely in accordance with statute, common law and regulatory requirements and in keeping with this policy and any subordinate policies, guidance and procedure, thereby contributing to public confidence in the work of the Probation Board.

PBNI should take all reasonable steps to ensure compliance with current and future legislation covering the following areas: Information Assurance, Information Security, Data Protection, Freedom of Information and Records Management. In order to do so, it is necessary for all PBNI's records to be secure, authentic, reliable and accessible. Additionally, they must support business functions and activities and be retained only as long as they are required by law.

3. Objectives

- To ensure that all information held by PBNI, including the personal information of employees and service users and service providers, should be fairly and lawfully processed to enable PBNI to comply with its legislative responsibilities in this area.

- To ensure that all information held by PBNI should be adequate and accurate for the purpose for which it is required and should be managed in an effective and transparent manner within a framework that gives due regard to:

  Confidentiality: must be preserved and information assets should be protected against unauthorised disclosure.

  Integrity: must be preserved and information assets must be protected from unauthorised or accidental modification.

  Availability: assets should be available as and when required in order to achieve PBNI's business objectives. Information should be easily retrievable to facilitate and enable PBNI to respond to information requests within the appropriate timescales. Information should be accessible to those who require it and should be held in a medium that will continue to be accessible over time.

  Security: information should be secure in both the physical and electronic environment from unauthorised or inadvertent alteration, loss or erasure. Information should have the correct Protective Markings applied, if applicable.

  Accreditation: the accreditation process must be compliant with the current HMG Infosec Standard and will require a detailed Risk Management and Accreditation Document set (RMADS) to be completed.

Business Continuity: all information systems will have a business continuity management process to counteract interruptions to business activities and protect critical business processes from the effects of major failures or disasters.

Incident reporting and response: a procedure for reporting, managing, and recovering from information risk incidents, including losses of protectively marked information.

Responsibility: although PBNI 'owns' the information held in its name, individual members of staff should be made aware of their obligations in relation to records management. All staff have a personal responsibility for how information created or received is managed and stored.

Storage/Transport: the storage/transport of information should be maintained and managed as effectively and efficiently as possible and related information should be held together to aid retrieval.

Training: all staff should be aware of their obligations relating to the management of information as a result of a combination of induction training and ongoing training at local level.

- To ensure PBNI maintains manual and/or electronic systems which facilitate appropriate management practices in the creation, retrieval, storage, preservation, retention and destruction of its records.

4. Procedures

The PBNI Procedures supporting this policy are as follows:

Information Security Procedures
Monitoring at Work Procedures
Data Loss Incident Response Plan

5. Responsibilities

This section provides an overview of organisational roles and responsibilities, with further detailed information provided in relevant procedures, guidance and other documents.

5.1 **The Director** has a duty to ensure that PBNI complies with the requirements of legislation.

5.2 **Senior Information Asset Owner** (SIAO) at Deputy Director level, and has overall responsibility for information assurance and risk management within PBNI. The SIAO has delegated the overall responsibility and control for security, policy and implementation to the Head of IT.

5.3 **The Head of IT** is responsible for the following areas and associated policies, procedures and guidance:

Information Assurance
Risk Management
Information Security
Internet and E-mail Usage
Monitoring at Work
Data Loss Incident Response Plan
Protective Marking Guidance
Accreditation Guidance
Information Awareness

5.4 **The Head of Communications** is responsible for the following policies, procedures and guidance:

Management of Information
Records Management
Freedom of Information
Data Protection
Retention and Disposal
Publication Scheme Access to Information
Data Sharing Access to Information
Information Awareness

5.5 **The Information Technology Security Officer** (ITSO) is responsible for creating, maintaining, giving guidance on and overseeing the implementation of Information Security including incident management. This post holder is the central point of contact on information security in PBNI, for both staff and external organisations, and is responsible, for example, for implementing an effective framework for the management of security. Day-to-day responsibility for implementing policy within the context of information systems development and use in PBNI is delegated to the ITSO.

5.6 **The Communications Department (Compliance Section**) has a responsibility for providing guidance and support on issues relating to Freedom of Information, Data Protection and Records Management to ensure that PBNI complies with its legislative responsibilities in these areas.

5.7 **The Records Officer** is responsible for the development and oversight of a records management policy and will work with Deputy Directors, Assistant Directors, Heads of Departments, Office Managers and other managers to ensure that there is consistency in the management of records. The Records Officer will also ensure that advice and guidance on good records management practice is given and provides the Director with assurances on compliance with records management policy.

5.8 **Data Protection and Freedom of Information Executive Officer –** this role sits within the Compliance Section of the Communications Department and the person is responsible for ensuring that staff are aware of PBNI's obligations under Data Protection Act and Freedom Of Information Act.

5.9 **Information Asset Owners (IAOs) –** these are senior individuals within PBNI with responsibility for relevant business departments (eg Heads of Departments, Deputy Directors/Assistant Directors). This is a mandated role and they are responsible for ensuring that they understand what information is held, what is added, what is removed, how information is moved, and who has access and why.

5.10 **All Managers** are responsible for ensuring that information systems in their areas conform to this policy and to the requirements of legislation.

5.11 **All Members of Staff and Board Members** are responsible for applying the correct principles when dealing with the information that they process and hold.

6. Resources

Costs associated with the effective application of this policy include:

Staff time and resources across several departments and responsibilities for monitoring adherence and compliance i.e.

- Information Technology (Information Security Officer, Helpdesk Analyst, Technical Support Analysts)
- Hardware/Software related to Information Assurance
- Information incident investigation and management
- Accreditation
- Communication Department
- Staff training

7. Communication and Training

7.1 The Head of Information Technology and Head of Communications will ensure that staff understand their responsibilities in managing information and that IA is a regular agenda item at team meetings.

7.2 All relevant area and office/department managers will be clear about their specific role in relation to ensuring their staff are aware of their obligations and who to contact for further guidance.

7.3 All staff will be adequately trained through:

a) hands on support by staff in IT (Security Officer) and Compliance (Communications Department) - information security, technical and advisory assistance
b) use of E-Learning resources; and
c) circulation of relevant guidance, desk aids, posters, leaflets.

8. Monitoring and Evaluation

8.1 This policy and any subordinate policies, guidance, procedures, and documents will be monitored by the Head of Information Technology and the Head of Communications (see 5.3 and 5.4), and staff within those departments who have specific responsibility for Information Assurance, IT Security, DPA/FOI, and Records Management.

8.2 This policy and any subordinate policies, guidance, procedures and documents may be evaluated on behalf of the Heads of Communications and IT. PBNI may also be subject to review and/or audit by the Information Commissioner's Office in respect of compliance with Data Protection and the Department of Justice in respect of security of information systems and practice.

9. Review

This policy will be reviewed within four years from date of approval.

Supporting guidance, procedures and documents will be subject to ongoing monitoring and may be amended in light of changes in legislation, updated guidance from the Cabinet Office, Information Commissioner's Office, Department of Justice, feedback, challenge or identified best practice.

10. Non Compliance

Failure to manage information in accordance with relevant PBNI policies (procedures or guidance) and appropriate legislation may result in disciplinary and/or criminal action.

11. References

The Data Protection Act 1998
The Freedom of Information Act 2000
The Information Commissioner's Office
HM Government – Cabinet Office guidance
The National Archives
The Public Records Office Northern Ireland (PRONI)