

serving
the community
through the
administration
of justice

The Northern Ireland Court Service

Information Assurance: Statement of Intent

June 2009



INVESTOR IN PEOPLE

www.courtsni.gov.uk

Objective

1. Reliable and accurate information is critical to proper decision making in the Northern Ireland Court Service (NICtS). This makes information a critical business asset that we need to protect. Information Assurance (IA) provides this protection by managing risks to the confidentiality, integrity and availability of information so that our business always functions effectively.
2. IA is important to NICtS because it will:
 - enhance our reputation by instilling the public with greater confidence and trust in how we collect, store, transfer and dispose of their information and all other official information;
 - improve controls that increase assurances we have in our partners' ability to handle information; and
 - demonstrate real quality and achievement to our stakeholders in relation to how we discharge our responsibility for information across Government.

Scope

3. This Statement of Intent covers all NICtS information. Information means any data, text, images, sounds, codes, computer programs, software, databases or the like concerning any matter relating to the policies, activities and decisions falling within our remit and which we communicate using paper, information and communications technology (ICT), the spoken word or another medium.
4. This Statement of Intent applies to all NICtS staff. This includes people employed temporarily or through contract with a third party, delivery partners and any other users of our information.

Influences

5. This Statement of Intent acknowledges the documents noted at Annex A and NICtS responsibility for implementing the directives and suggestions they contain in a consistent, timely and cost effective way.

Key Principles

6. The Director of NICtS delegates responsibility for IA to the NICtS Senior Information Risk Owner (SIRO) who is a member of the NICtS

Management Board. The SIRO owns this Statement of Intent, serves as an advocate for information risk management on the Management Board and provides written advice on information risk to the accounting officer as an input to NICtS annual Statement of Internal Control.

7. NICtS business areas have designated Information Asset Owners (IAOs), who provide a clear focal point for IA and will have responsibilities aligned with those of the SIRO but for a defined business area. Each IAO will engage the relevant sponsor teams to ensure the chairs and chief executives of non-departmental public bodies (NDPBs) and “arms-length” bodies take appropriate IA-related action.

8. NICtS have established an Information Assurance Programme Board, chaired by the SIRO, which will provide a cross-NICtS focus on IA from a business perspective. That Board will oversee IA-relevant actions undertaken within each business area. These actions will include:
 - producing information asset registers that identify all information assets and assign an appropriate information asset owner for each;
 - assessing risks to the confidentiality, integrity and availability of information assets at least quarterly;
 - reducing information risks to an acceptable level and reporting the status of protective controls and residual risks to information;
 - ensuring protective controls conform to the standards and codes of practice embodied in the BS ISO/IEC 27000 series, which provides an internationally recognised code of practice for information security management, and HMG’s Security Policy Framework; and
 - routine monitoring and review to ensure IA arrangements remain effective.

9. NICtS will protect information in a manner appropriate to the information’s sensitivity, value and criticality. NICtS will ensure protection is cost effective, commensurate with the risks and consistent with the departmental strategic aim of promoting confidence in the justice system.

10. NICtS will comply with relevant UK and European Commission (EC) legislation, such as the Data Protection Act 1998 and the Freedom of Information Act 2000; HMG’s Security Policy Framework, including all related documentation; and the BS ISO/IEC 27000 series, the international standard for information security.

11. NICtS will provide all staff with the awareness they need to discharge their IA responsibilities effectively whatever their role. This includes making staff aware of the principles and processes underpinning the Data Protection Act and Freedom of Information Act so they understand how to apply these principles and processes whenever they receive requests for information. NICtS will achieve staff awareness by publishing written guidance and through education and training initiatives delivered as part of the NICtS commitment to an IA training programme.

12. Staff across NICtS will apply IA-relevant principles, policies, procedures and work instructions in a way that demonstrates an understanding of and responsibility for the value and risk attached to information they handle during the course of their duties.

Policy Statements

13. NICtS will ensure that each business area:
 - creates and maintains an information asset register that identifies an appropriate information asset owner for every information asset therein;
 - instructs all staff to use HMG's protective marking system to label and handle information assets in keeping with the value assigned to those assets;
 - assesses and maintains its requirements for storing information, taking prevailing legal and regulatory requirements into account, and documents a retention schedule based on Public Records Office of Northern Ireland (PRONI) guidelines;
 - trains all members of staff on their specific responsibilities for IA;
 - gives access to information assets in a way that limits this access to that which a person needs to discharge their legitimate responsibilities in a timely and effective manner;
 - maintains current and historical records of access controls applied to information assets in order to detail who has had access to what and when;
 - reviews the access granted to information assets regularly to confirm that authorisation processes continue to operate satisfactorily and that the access given remains consistent with business needs and business risks;
 - identifies IA requirements and incorporates appropriate IA provision as part of any new project or significant change initiative;
 - disposes of all information assets securely, in keeping with any approved disposal procedures;

- encourages third-party service providers and other service delivery partners to conform to the requirements of the BS ISO/IEC 27000 series where appropriate;
- are aware of the NICtS knowledge and information liaison officer (KILO), or equivalent, who provides an identifiable and accessible point of contact for matters pertaining to the Data Protection Act and Freedom of Information Act;
- appoint a Local Records Officer (LRO) within that business area, who has responsibility for the confidentiality, integrity and availability of all records belonging to that business area; and
- appoint an accreditor who risk assesses ICT-based information systems used to meet business requirements and accredits these systems impartially on behalf of the relevant management board.

14. All NICtS staff will fulfil their responsibility for maintaining IA by:

- keeping abreast of what they must do to protect information assets and apply principles in this Statement of Intent;
- familiarising themselves with the demands of IA-relevant procedures and work instructions published on the NICtS intranet or disseminated in some other way;
- reporting any actual or suspected software malfunctions, hardware malfunctions, virus infections, faults, weaknesses or other security incidents affecting ICT-based information systems or services to the appropriate officer in a clear and timely manner;
- reporting any actual or suspected breaches of physical, personnel or procedural security to an appropriate security authority in a clear and timely manner; and
- maintaining effective “IA culture” by participating fully in education, training and awareness sessions designed to improve their appreciation of IA.

Implementation

15. Business areas will ensure all staff recognise their responsibility for IA and comply with this Statement of Intent. Non-compliance may result in disciplinary action.

Ownership and approval

16. The NICtS SIRO owns this Statement of Intent on behalf of the NICtS Management Board. Each Information Asset Owner (IAO) approves this Statement of Intent.

Annex A

Reference	Document summary
1	<p>A National Information Assurance Strategy (NIAS): the Central Sponsor for Information Assurance (CSIA), part of the Cabinet Office, published this document in 2007. It is available at:</p> <p>www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx</p> <p>The document sets out how the UK should approach information risk management by encouraging: the right level of professionalism, education and training; availability of IA products and services; as well as compliance and adoption of standards. It aims to: make Government better able to deliver public services through appropriate use of ICT; strengthen the UK's national security by protecting information and ICT at risk of compromise; and enhance the UK's economic and social well-being as government, businesses and citizens realise the full benefits of ICT.</p>
2	<p>The Security Policy Framework (SPF): the Cabinet Office Security Policy Division issues this document on the authority of the Official Committee on Security (SO). It is available through departmental security officers who have access to it on both CD-ROM or via the Government Secure Intranet (GSI).</p> <p>The document provides guidance that helps Government departments and agencies and other organisations discharge their security responsibilities by protecting the confidentiality, integrity and availability of assets used during the conduct of Government business.</p>
3	<p>Code of Connection for the Government Secure Intranet (GSI CoCo): OGCbuying.solutions issues this document. It is available at:</p> <p>www.cesg.gsi.gov.uk/bookstore/title.html</p> <p>The document aims to develop the trust required both within and between Government Secure Intranet (GSI) communities by setting down a minimum set of security standards that organisations must adhere to when joining the GSI.</p>
4	<p>Code of Connection for the Criminal Justice Extranet (CJX CoCo): the National Policing Improvement Agency (NPIA) issues this template document. It is available from the National Accreditor for the Police Service.</p> <p>The document aims to develop the trust required between CJX-connected organisations by setting down a minimum set of security standards that organisations must adhere to when joining the CJX.</p>