Commission for Victims and Survivors

GUIDANCE NOTE FOR INFORMATION ASSET OWNERS

Explanatory Note: This note seeks only to offer 'see at a glance' guidance and is not intended as a substitute for consulting comprehensive Commission policies and procedures concerning a wide range of Information Assurance matters. See the Commission Information Security Policy for more detailed guidance. There is also guidance available on the procedure to be followed in the event of a significant loss or theft of Information or IT equipment.

Information Asset Owners (IAOs): role and responsibilities

You are a senior officer responsible for the operational management of information. In running your business area you need to;

- understand what information – paper and electronic – is held and how it is maintained; know and approve who has access to it and why
- seek to use information fully within the law by means of publication and disclosure; ensure all systems processing protectively marked data are accredited
- identify and address risks to the information – review your risk register regularly – approve access to barred internet sites and sign off the disposal/transfer of IT equipment
- sign off quarterly Stewardship Statements and provide input to the Statement on Internal Control and other statements or returns concerning the management of information assets
- Encourage a culture that values, protects and uses information for the public good (e.g. through Team Brief discussion) - lead by example
- Act as the Senior Information Risk Owner's 'eyes and ears'

Ask yourself the following questions, so that you can gauge the extent to which you are satisfying your obligations – note that almost all of these relate to responsibilities that you discharge already:

'Line of Business' systems – Have you a register of systems? Are there any bespoke systems used within your area of responsibility that store and/or process sensitive information (even spreadsheets)? If so, have they been accredited to ensure that any risks have been mitigated to a level that you are content with? Do you know who has access to each system?

Flow of information – Are you aware of all information flows into and out of your area of responsibility? Is the information transmitted in an appropriate manner in line with relevant policies? Does any regular electronic transmission need to be encrypted?

Internet Access – Are you aware of any special permissions for your staff to access Internet sites that are blocked normally, e.g. social networking sites?

Security Clearance – Are your staff security cleared to an appropriate level considering the information to which they have access? Do any clearances need renewed? Are your contractors and consultants appropriately cleared and briefed? If not cleared, they must be escorted at all times.

Protective Markings – Does the information you hold carry an appropriate protective marking and is it stored accordingly?

Disposal of information – Are you holding information longer than is necessary?

Physical Security – Are all the assets within your area of responsibility secured physically during and outside of office hours? Do you have an up-to-date inventory of all IT equipment? Are all premises secure? Has approval been recorded for all non-encrypted laptops used outside Commission premises?

Business Continuity Planning – Do you have a Business Continuity Plan(s) covering all areas of your business? When was it tested last?

Staff awareness – Are your staff aware of their statutory responsibilities under the Public Records Act (NI), 1923; the Computer Misuse Act 1990; the Data Protection Act 1998 and the Freedom of Information Act 2000? Are all staff aware of the latest Information Assurance guidance, e.g. the procedure for the secure disposal of IT equipment/assets?

Advice and Guidance – For further help, see table below:

Role	Main Area of Responsibility	Name	Tel	Email
Accounting Officer and Senior Information Risk Owner	Commission level risk All aspects of protective security. Commission level information risk. Commission physical security advice; breach investigations.	John Beggs	(t) 02890 311 000 (m) 07530 610 687	john.beggs@cvsni.org
Departmental Accreditor	Accreditation of ICT systems – advice on information risk management, information security and accreditation process. Forensic investigations.	Joe Beattie	(t) 02890 522 670 (m) 07747616378	joe.beattie@ofmdfmni.gov.uk
Information Asset Owners	Information Management (electronic & paper records), FOI and Data Protection ALSO Staff security and clearances; premises and physical security	Adrian McNamee Craig Gartley	(t) 02890 311 000 (m) 07540 200 665 (t) 02890 311 000 (m) 07595 244 696	adrian.mcnamee@cvsni.org craig.gartley@cvsni.org
IT Security Officer	IT Security – Internet access permissions – help for IAOs regarding the preparation of accreditation documentation (RMADS)	Donal Shiels	X 617 (m) 07738 836 652	DShiels@equalityni.org