

**ROYSTON HOUSE REVIEW
RECOMMENDATION ACTION PLAN & STATUS**

For Glossary of Terms used please see final page

- 1. Clearly allocate the responsibility and accountability for the security of all NICS office space, and ensure that the responsible person is resourced, trained, competent, and supported by senior staff.**

Action(s):

Responsible Owners: SAU / PD

A Special Review of the Physical Security of NICS premises, being carried out by SAU and Departments, is nearing completion.

Status: Report due end December 2009

- 2. Build on this good practice by formalising the policy for the last person leaving the office so that it applies to all NICS office space. Based on an assessment of risk to information and other assets, consider implementing a standard sign out and security checking process for the last person out of the office. Review the process for ensuring compliance with such policy to ensure this is fit for purpose.**

Action(s):

Responsible Owners: SAU / DSO

Recommendation accepted. Reference will be made in the next revision of the Premises Officer Guide to the Last Person Out policy.

Status: Action ongoing – will be included in next revision

- 3. In future, procurement of lockable storage should draw upon the expertise of the Security Advisory Unit in Northern Ireland in order to ensure sufficient physical security. The Security Advisory Unit also have a valuable role to play in providing guidance in selecting and planning for new NICS office space.**

Action(s):

Responsible Owners: SAU/PD

Recommendation accepted. SAU and PD will clarify and review current procedures for the specification of lockable storage furniture, make recommendations for future procedures and specification and if appropriate on any changes to existing lockable storage furniture. When considering new office space or changes to existing office space Departments must consult with DSOs who should consult with SAU as appropriate.

Status: Ongoing

4. **In line with the measures set out in the Data Handling Review¹, ensure that information risk is properly represented in departmental risk registers, produce physical and information asset registers and make clear the protection or other action that should be in place for assets of different value.**

Action(s):

Responsible Owner(s): Departmental DSOs

Recommendation accepted. Risk responsibility was agreed by PSG in December 2008 following recommendations outlined by second NI Data Protection Review.

Status: Action completed

The annual Statement of Internal Control (SIC) prepared by Departments and the HOCS Statement of Compliance also addresses this issue.

Status: Action to be undertaken annually – next statement due March 2010

5. **Develop and implement a regular and effective testing regime for both the alarm system and response mechanism.**

Action(s):

Responsible Owner(s): SAU/DSO

Recommendation accepted. The recently published Premises Officer Guide contains appropriate guidance on testing of alarms and reporting to appropriate DSO.

Status: Action completed November 2009

6. **Review the access control system for staff entering buildings to ensure it is fit for purpose. This should include a review of the role of the 'guard' position at the main entrance and the arrangements for staff entering offices used by NICS.**

Action(s):

Responsible Owners: SAU/DSO

Recommendation accepted. DSO/SAU will review Guard arrangements for Royston House.

Status: Review substantially complete - December 2009

Guard arrangements in general will also be covered by the Special Review of the Physical Security (see Recommendation 1).

7. **Consideration should be given to implementing local building inductions for all staff, including security issues.**

Action(s):

Responsible Owners: DSO

Recommendation accepted - DFP will continually review the security material contained within its Staff Induction to ensure it is up to date.

Status: Ongoing

¹ The data handling review can be found at:

http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf and <http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/dhr080625.pdf>

Responsible Owner: SAU

SAU will issue correspondence to all DSOs in December requesting that they ensure security issues are considered in their Departmental Induction.

Status: Completed - correspondence issued December 2009

8. **Planning should be put in place for the management of any future incidents. This should include a means for clearly identifying who leads management of incident/ key personnel / key Action(s): Existing Whitehall best practice may be helpful in this respect².**

Action(s):

Responsible Owner: DID

Recommendation accepted – an incident management guide has been developed by Whitehall, known as the First Responders Guide, and is available to the NICS. IAO's have also received baseline training in dealing with incident response.

Status: Action completed – guide available and baseline training provided.

Responsible Owner: DID

DID will continue to liaise with Whitehall to monitor the release of any best practice advice or guidance. and where appropriate adopt it for NI. The updates will be issued via the NICS DSOs.

Status: Action – monitoring is ongoing

Responsible Owner: DID

Baseline training for Departmental Information Asset Owner (IAO) arranged to include outline roles and responsibilities for IAO post-holders.

Status: Action completed: a series of baseline training sessions held for IAO post-holders in November 2009

9. **A systematic assessment of the potential impact of this loss should be made and appropriate mitigation put in place. Action to address the risks to those not yet contacted about the loss should also be taken.**

Action(s):

Responsible Owners: DSO/CHR

An impact assessment of the loss was undertaken by relevant business area and a full report made to the Information Commissioner. The relevant business area will continue to review actions in respect of risks based upon current PSNI advice

Status: Action ongoing

10. **The process and accountability for identifying removable media that require encryption should be made clear. This should include measures to ensure compliance with this policy.**

² The Cabinet Office guidance on Incident management will be made available to DFP and NICS more broadly

Action(s):

Responsible Owner: DID

Recommendation accepted. All staff were issued with the 10 key rules for laptops and media. Further detailed policies on the use of laptops and of removable media have been prepared and issued for comment. These policies will provide further clarity on identifying the requirement for encrypted laptops and compliance audits will be put in place. In addition DID will work with IT Assist to initiate the programme to lock down access to removal media for storage across the NICS PC Estate.

Status: Revised policies to issue January 2010

11. **In the interests of greater protection for all personal data, and greater clarity in identifying the information assets that this policy should apply to, consideration should be given to implementing a programme for the encryption of *all* removable media containing personal data.**

Action(s):

Responsible Owner: DID

Recommendation to consider programme accepted. All staff issued with the 10 key rules. Two policies have been drafted and are under review for issue in December 2009. This will mandate the lock down of laptops and the use of encrypted storage devices (USB Iron Keys) only. A secure product has been developed (Securedox) to facilitate the necessary transmission of data in encrypted form.

Status: Facility for secure transmission in place, use of Ironkeys USB devices and new policies for laptops and media in place for December 2009

12. **In line with the measures set out in the Data Handling Report and Data Protection legislation, processes for issuing and returning laptops should be reviewed to ensure they are fit for purpose and made clear to all staff with access to laptops. Guidance to staff on the secure use and protection of laptops should be reviewed and made clearer. This should include the effective use of Kensington locks in physically securing laptops.**

Action(s):

Responsible Owner: DID

A series of '10 Key Rules' issued (June 2009) to staff which outlined arrangements on the approved use and protection of laptops including the use of Kensington locks.

Status: Action completed - guidelines issued June 2009

Responsible Owner: IT Assist

IT Assist has worked with the department to ensure that essential users are being prioritised in the project to roll out encrypted laptops.

Status: All high priority users within DFP have now received encrypted laptops

Responsible Owner: IT Assist

Contractual arrangements are in place to ensure that laptops are cleansed to CESG standards if they are redeployed or are for disposal.

Status: Action ongoing

Responsible Owner: PD

The revised Premises Officer Guide now provides additional guidance on the proper use of laptop locks.

Status: Action completed November 2009

13. In line with measures set out in the Data Handling Report, the accountability for the security and proper handling of personal data should be made clear. This should encompass both existing senior roles such as the Senior Information Risk Owner and also those accountable for and knowledgeable about specific data sets to ensure compliance with policy and to provide the SIRO and accounting officer with assurance about the personal information held and managed. Clear policy should be developed for the means of transferring personal information. The measures set out in the Data Handling Review may be helpful in this respect³.

Action(s):

Responsible Owner: DID

Recommendation accepted. Guidelines on the roles and responsibilities for Accounting Officer, SIRO and IAO post-holders are in place.

Status: Completed - Guidelines available

Responsible Owner: DID

Information assurance baseline training provided for Departmental Information Asset Owners.

Status: Action completed November 2009.

Responsible Owner: DID

The need for additional data handling measures remains under regular review.

Status: Action ongoing

Responsible Owner: DID

While there is much information and guidance available DID have been developing an Information Governance Framework (IGF) to bring this information together and to better signpost linkages, roles and responsibilities. The introduction of the new framework will include NI specific information management guidelines. The draft framework will be issued to SIROs for sign-off in January 2010.

Status: Action under development. Draft framework will be issued to SIROs for consideration in January 2010

³ The Data Handling Report (paragraphs 13-15 pages 3-4) provides information on different options for transferring information
http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

Responsible Owner: DID

A product to encrypt and transfer sensitive data (SecureDox) has been developed and is now in widespread use

Status: Action completed – product now available for use

14. **Personal data held and transferred should be reduced to only those necessary to meet business need. Such data should only be held for as long as necessary to meet business need. Data no longer required should be disposed of securely.**

Action(s):

Responsible Owner: DIM

Recommendation accepted. A revised DFP Data Protection Action Plan was agreed at Departmental Board in November 2009. A Departmental Data Protection policy which was cleared by ICO and a data protection handbook for staff are also now in place.

Status: Action completed – Departmental action plan agreed and policy in place

15. **Existing information security policy and guidance should be reviewed with a view to producing a clear and succinct statement of mandatory policy, and to provide a single authoritative source of guidance.**

Action(s):

Responsible Owners: SIRO/SAU

Recommendation accepted. The NICS Information Assurance Policy as outlined in the Cabinet Office Security Policy Framework and the NICS Guide to Document and IT Security is now subject to annual review as part of the reporting process to HOCS.

Status: Action completed and subject to annual policy review

Responsible owner: DID

While there is much information and guidance available DID have been developing an Information Governance Framework (IGF) to bring this information together and to better signpost linkages, roles and responsibilities. The introduction of the new framework will include NI specific information management guidelines. The draft framework will be issued to SIROs for sign-off in January 2010.

Status: Action under development. Draft framework will be issued to SIROs for consideration in January 2010

Responsible Owner: DID

DID will liaise with Whitehall to monitor the release of any new or updated policies or guidance. The updates will be issued via the NICS DSOs.

Status: Action – monitoring is ongoing

16. **Action should be taken to address the organisational culture with regard to the handling of information. This might include raising awareness, training⁴ for all staff handling data, and a clear statement of the HR and disciplinary position for data losses. Furthermore consideration should be given to using the new CPNI security awareness culture tool to help establish the desired security culture and identify any gaps.**

Action(s):

Responsible Owner: DID

Recommendation accepted. An e-learning training package to raise staff awareness of data protection issues is being rolled out across NICS Departments and Agencies. The National School of Government Protecting Information e-learning training package is being used where appropriate as additional data handling awareness training and the CPNI tool may also be used to further embed training as required.

Status: Action underway – e-learning package rollout commenced April 2009

Responsible Owner: DID

Additional and updated guidance on the use of laptops ('10 Key Rules' Notification) issued to staff.

Status: Action complete - guidance issued June 2009

Responsible Owner: DID

The Northern Ireland Data Protection Review Report recommended an NICS-wide Data Protection Awareness Campaign. The cost to run such a campaign is estimated at £200k with roll-out subject to successful in-year bidding.

Status: Roll-out remains subject to successful in-year bidding

Responsible Owner: DID

The Information Governance Framework (IGF) identifies a need to develop a comprehensive training programme - this is under development and should be finalised by end March 2010

Status: Action ongoing – requirements to be finalised Mar 2010.

Glossary of Terms:

CAL	Centre for Applied Learning (DFP)
CHR	Corporate HR
DID	Delivery & Innovation Division (DFP)
DIM	Departmental Information Manager
DSO	Departmental Security Officer
GSI	Government Secure Intranet
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IGF	Information Governance Framework
PD	Premises Division
SAU	Security Advisory Unit (OFMDFM)
SIRO	Senior Information Risk Owner

⁴ For example the Cabinet Office's protecting information e-learning, which will be made available to DFP and NICS more broadly