

# POLICY FOR SENDING INFORMATION TO THIRD PARTIES

## Review History

Version	Author / Reviewer	Review Date	Approved by
1.0	Danny Smyth	4 Sep 2009	Charles Hamilton / Information Security Forum
2.0	Danny Smyth	2 February 2010	Charles Hamilton
3.0	Danny Smyth	10 October 2011	Charles Hamilton

---

## 1. INTRODUCTION

- 1.1 Please read this policy carefully as you will, in the future, be deemed to be aware of its contents in the event that there is any breach of Invest NI's policy.
- 1.2 This policy must be followed when sending any **personal or business sensitive** information to a third party outside Invest NI. Third parties include External Delivery Organisations, Contractors, Stakeholders, Client Companies etc.
- 1.3 Personal or business sensitive information must never be sent via email, except as permitted in 1.4 below.
- 1.4 Any information being sent to a NICS Department can be sent securely from your Invest NI email account. This includes all emails sent to DETI. This extends only to the NICS from an Invest NI account. If the information you are planning to send to a NICS Department cannot be sent via email then the procedure in this policy must be followed.
- 1.5 Any third party not contracted through Central Procurement Directorate (CPD) who is being given access to Invest NI personal or business sensitive information that does not relate to them must sign the associated Third Party Data Processing Contract.

## 2. PURPOSE

- 2.1 The purpose of this policy is to set guidelines to ensure security and confidentiality of information whilst it is being sent to appropriate third parties. It aims to ensure that third parties present or create no unnecessary business risk to the organisation.

### 3. CONFIDENTIALITY OF INVEST NI PERSONAL AND BUSINESS SENSITIVE INFORMATION

- 3.1 All personal information processed by Invest NI must comply with the Data Protection Act 1998. Please see Invest NI [Data Protection Policy](#) for further details.
- 3.2 Prior to making arrangements to provide a third party with personal or business sensitive information held by Invest NI that does not relate to them, a contract must exist to state the purpose for which access to this information is being granted. For most Contractors this will be the Contract made through CPD. For all other third parties a '[Third Party Data Processing Contract](#)' must be signed.
- 3.3 The '[Third Party Data Processing Contract](#)' must be signed on behalf of Invest NI at Director level in line with all other legal agreements. This contract must state a 'permitted purpose' for which Invest NI is providing the information to the third party and this must be in line with the purpose for which Invest NI collected this information from the Data Subject. If the purpose does not correspond to the reason Invest NI collected the information then Invest NI must seek consent from the relevant Data Subject(s) affected prior to release of their information.

### 4. SECURITY AND CONTROL

- 4.1 As Data Controller Invest NI must ensure the security of information being provided to third parties. This includes ensuring the secure sending (transfer) of the information.
- 4.2 At present there are two methods of sending personal and business sensitive data approved by Invest NI:
  - (i) Secure **USB Ironkey** device;
  - (ii) Secure file uploading service '**sendthisfile**'
- 4.3 Staff should decide on the most appropriate method of transfer to suit their business need e.g. the USB Ironkey may be most appropriate for delivering presentations that contain business sensitive information, whereas 'sendthisfile' may be most efficient for the transfer of large files within a tight timescale.
- 4.4 Requests for a secure USB Ironkey device should be made by logging an ICT Service Desk call (ext 140 or [servicedesk@investni.com](mailto:servicedesk@investni.com)).
- 4.5 The 'sendthisfile' website can be accessed at the following link: <https://www.sendthisfile.com/investni>
- 4.6 **Use of secure USB Ironkey device**  
The steps that must be taken to ensure the safe transfer of electronic personal and business sensitive information is as follows:

- 4.6.1 Data is transferred from Invest NI's system onto a secure Ironkey USB device. Other mobile devices should **NOT** be used to transfer information;
- 4.6.2 Arrangement is made with the third party for collection of the Ironkey;
- 4.6.3 The third party contacts Invest NI to advise receipt of the Ironkey;
- 4.6.4 Password for access to the Ironkey's contents is given to third party over the telephone when they are ready to transfer information onto their systems;
- 4.6.5 The third party confirms transfer of data onto their systems;
- 4.6.6 Arrangements are made for return of the Ironkey to Invest NI;
- 4.6.7 Third party confirms by email that data has been securely destroyed after its use;
- 4.6.8 If the third party does not confirm destruction of information within appropriate timescale, the Invest NI team who provided the information must seek this confirmation in writing.

#### 4.7 **Use of 'sendthisfile' uploading service**

Technical guidance on how to use the uploading service will be provided directly by ICT.

- 4.7.1 Passwords to allow access to sent documents should not be provided to the recipient until after they confirm the notification email has been received;
- 4.7.2 The Third Party should confirm by email that data has been securely destroyed after its use;
- 4.7.3 If the third party does not confirm destruction of information within appropriate timescale, the Invest NI team who provided the information must seek this confirmation in writing

#### 4.8 **Transfer of Physical Files**

- 4.8.1 Whenever possible physical information should be converted to electronic information, in line with the Invest NI [Scanning Policy](#), to share with third parties per the procedure above. When this is not practical e.g. the audit office /forensic investigations require numerous historic files, the process set out in paragraph 4.4 below should be followed. Please refer to the [Records Management Policy](#) regarding the

lifecycle of records to ensure that files are not kept for longer than is necessary.

- 4.8.2 When arranging collection and return of physical (paper-based) files it is the responsibility of the staff member co-ordinating the transfer, to liaise directly with the third party, and to be present during the collection and return of files.
- 4.9 The steps that must be taken to ensure the secure transfer of physical personal and business sensitive information are as follows:
- 4.9.1 Information (files) is listed to ensure that Invest NI has a full record of files being provided to the third party;
  - 4.9.2 Either (i) third party comes to Invest NI to collect files or (ii) Invest NI brings files to the third party. Use of a courier is not recommended unless they can confirm secure delivery;
  - 4.9.3 Third party signs for the files listed acknowledging their receipt of information as listed in paragraph 4.4.1 above;
  - 4.9.4 Third party returns files. Invest NI checks the returned files against the list of files provided to the third party. If all files are present, confirmation of receipt of files is provided to Third Party (if requested) and a copy is kept for Invest NI records;
  - 4.9.5 If all files are not present Invest NI should only acknowledge receipt of files that are returned. The third party should be notified of the missing file(s) in writing as soon as possible and a search for any missing file(s) should be instigated. If files are not found then a breach should be reported as per the [Information Security Breach Management Procedure](#).

## 5. OWNERSHIP

- 5.1 It is the responsibility of each member of staff to ensure that any information they wish to share with a third party is done so in line with the [Data Protection Policy](#) and that the transfer itself is in line with this policy.
- 5.2 This policy forms part of the Information Security Handbook and should be read in conjunction with the relevant policies contained therein, including the [Data Protection Policy](#). Any further clarification required concerning this policy can be sought from the Information Governance Manager at [privacy.officer@investni.com](mailto:privacy.officer@investni.com) .