

Title: **INVEST NI ICT SYSTEMS ACCEPTABLE USAGE POLICY**
 Author: Neil McGarry
 Issue Number: 2.0
 Approver: Liam Hagan
 Status: Approved
 Effective Date: 1st February 2010
 Expiration Date: 30th June 2012

Review History

Issue No.	Current Author	Review Date	Reviewer	Amendment History
1.0	Martin Graham	June 2002	NIPSA & Liam Hagan	
1.1	Susan Cairns	14 August 2003	Neil McGarry	
1.2	Neil McGarry	21 November 2003	Susan Cairns	
1.3	Neil McGarry	7 th March 2005	Ian Boylan	
1.4	Neil McGarry	9 th November 2005	Ian Boylan	
1.5	Neil McGarry	5 th April 2006	Ian Boylan	
1.6	Neil McGarry	11 th April 2007	Liam Hagan	
1.6.1	Neil McGarry	19 May 2009	Ian Boylan	www.nibspdatabase.co.uk changed to www.edpmis.co.uk
1.7	Neil McGarry	31 st October 2010	Charles Hamilton	Policy title changed

1 INTRODUCTION

- 1.1 This document is an acceptable usage policy providing user guidance on how to ensure the availability, confidentiality and integrity of Invest NI's ICT systems.
- 1.2 IT Security requirements are based on an analysis of the risks facing Invest NI so that they may be properly countered. There are various aspects of computer misuse to be considered, namely its prevention, detection, investigation and related disciplinary procedures. This document provides measures to cover these aspects.

2 PURPOSE

- 2.1 The objective of this policy is to ensure that:
- Information on any of Invest NI's ICT systems is protected from unauthorised sources
 - Confidentiality required through regulatory and legislative requirements is ensured
 - Integrity of information is maintained
 - Information is available to authorised personnel as and when required.
 - Invest NI staff are aware of their responsibilities towards the security of all information systems

3 SCOPE

- 3.1 All electronic information held by Invest NI is regarded as falling within the scope of this policy. This policy relates to all elements of Invest NI where information within ICT systems is used or operated, including those supplied or operated on its behalf by external contractors. The policy applies further to joint working arrangements with other agencies and applies to any user accessing information using Invest NI ICT equipment.

Expires 30th June 2012

4 ROLES AND RESPONSIBILITIES

- 4.1 All Invest NI staff and Third Parties:
 - 4.1.1 All staff using any Invest NI ICT system will have a personal responsibility in the use of that system for its security and integrity.
 - 4.1.2 All staff will ensure that they themselves uphold the principles of this policy, the **Information Security Policy** and the [Invest NI Policy on Internet & Email Usage](#).
 - 4.1.3 Use of Invest NI's systems must not bring the organisation into disrepute.
- 4.2 Line Managers:
 - 4.2.1 Line managers will inform HR about staff changes, including Third Parties, affecting systems access so that permissions and accounts can be changed or withdrawn.
 - 4.2.2 Line managers will determine individual needs to systems under their aegis and ensure that access is based on need rather than status.
 - 4.2.3 Line managers will ensure that no unauthorised staff are allowed access to systems under their aegis.
- 4.3 System Managers:
 - 4.3.1 Each ICT system in Invest NI will have a nominated System manager who will have daily responsibility for the ICT security on that system (see Appendix B).

4 AUTHORISED USE OF SYSTEMS

- 4.1 Only authorised users have the right to access and update Invest NI's information systems. Access is restricted to information required for the authorised user's job function and is on a need-to-know basis.
- 4.2 Users must not attempt to illicitly connect to any ICT facility without the express permission of the ICT Team and Senior Management. **This is known as hacking and is a criminal offence.**
- 4.3 Where multiple users share access to an ICT system, each user must possess a verifiable and unique identity.
- 4.4 Updates and changes to data must be made by authorised personnel with the intention to maintain data accuracy and integrity. Other user's data can only be changed with their express permission.
- 4.5 Information stored in any of Invest NI's information systems must not be transferred out of the organisation via an unsecure method of transport and without permission e.g. documents stored in Google Desktop, using web-based email accounts such as Hotmail for business use or utilising non-Invest NI memory sticks.

Expires 30th June 2012

5 PREVENTION OF ICT SYSTEM MISUSE

- 5.1 All staff MUST be committed to Information Security within Invest NI and have signed the Appendix A of the Information Security Policy. When a member of staff is appointed, changes role or leaves Invest NI, the staff member's access rights will be reviewed or cancelled by the ICT Team. The ICT Team will be informed of changes by Human Resources.
- 5.2 **All hardware and software must be purchased and installed by the ICT Team.** Requests must be sent via the ICT Service Desk. Users must not download software from any source. If a user finds software on the internet that may be useful as part of their job role, they must in the first instance contact the ICT Service Desk.
- 5.3 **The illegal copying of software or data is theft and will be treated as a disciplinary offence.**
- 5.4 No staff member must purchase a hardware device with the express intention of connecting it (or any associated software) to the Invest NI network.
- 5.5 All staff are responsible for informing HR and the ICT Team if a Third Party requires access to any of Invest NI's ICT systems. If granted it is the users responsibility to ensure that the [Invest NI Policy on Third Party Access](#) is signed before the Third Party gains system access.
- 5.6 All staff must take all reasonable precautions not to introduce any malware to Invest NI systems. If a user detects a virus or spyware on their machine this should be reported immediately to the ICT Service Desk or IT Security Officer who will deal with the problem and record it appropriately.
- 5.8 No ICT hardware shall be removed from Invest NI without the full approval of the ICT Team, except for assigned laptops or mobile media that are the responsibility of each individual user.
- 5.9 All staff will take adequate care when eating or drinking near ICT equipment.
- 5.10 All staff will store confidential hardcopy documents and media in safes, locked cabinets or locked desk drawers and adhere to the Clear Desk Policy. Staff will not attempt to access comms rooms within any Invest NI premises where they have not been granted physical access.
- 5.11 Workstations must be locked immediately using the 'Lock Computer' option when being left unattended by an Invest NI user. All staff must switch off all hardware when not in use for extended periods, such as overnight or during weekends.
- 5.12 All staff must accept the security responsibility for any ICT assets given to them by the ICT Team, whether software or hardware. Special care must be taken with laptops and mobile devices. These must not be left unattended for extended periods and must be made secure (locked away or tethered by cables) overnight or when not in use.
- 5.13 Hardware should be positioned so that it cannot be viewed by outsiders e.g. display screens should not be visible from windows outside the building.
- 5.14 Passwords must never be written down or given out to other users. In the event where a password becomes known it is the responsibility of the user to ensure that it is changed as soon as possible.

Expires 30th June 2012

- 5.15 All network users must be positively identified before the user is allowed access to the programs or applications. Users will be asked for the identity authorised for a particular system. A warning message stating the need for authorisation or in breach of the Computer Misuse Act will be put in place for all Invest NI systems.
- 5.16 Sensitive printouts, for example those identifying named individuals or financial details, must be placed in confidential waste bins provided in each building.
- 5.17 All users must report any equipment losses **as soon as is feasibly possible** to the IT Security Officer and line management.

6 INTELLECTUAL PROPERTY POLICY

- 6.1 Intellectual property (IP) is the term used to describe intangible assets resulting from creative work carried out by an individual or an organisation. For example, IP can arise from contracts or letters of agreement with the providers of activities for Invest NI. IP can be traded in the same way as physical assets.
- 6.2 Invest NI owns the intellectual property created by its employees under the conditions stated below:
 - 6.2.1 IP created by an employee within the scope of employment.
 - 6.2.2 IP created on Invest NI's time with the use of corporate facilities or Invest NI financial support.
 - 6.2.3 IP commissioned by Invest NI pursuant to a signed contract.
 - 6.2.4 IP resulting from research funded by Invest NI.
- 6.3 Invest NI claims ownership of all IP which is devised, made or created:
 - 6.3.1 by persons employed by Invest NI in the course of their employment;
 - 6.3.2 by other persons engaged in research for Invest NI. A condition of their being granted access to corporate premises or facilities is that they agree in writing that this claim shall apply to them;
 - 6.3.3 by persons engaged by Invest NI under contracts for services during the course of or incidentally to that engagement.

8 BREACHES OF THE ICT SYSTEMS ACCEPTABLE USAGE POLICY

- 8.1 Breaches of the ICT Systems Acceptable Usage Policy shall be logged by the ICT Team. Any Breach discovered by an Invest NI user should be forwarded to the IT Security Officer for further investigation.
- 8.2 The ICT Team will assess the level of risk associated with any violation and take appropriate action to minimise the risk and prevent re-occurrence of the violation.
- 8.3 The IT Security Officer will notify the appropriate line manager/ group head depending on the seriousness of any breach as well as the consequences related to the breach and remedial action taken.
- 8.4 Serious breaches will be reported to Human Resources especially where the Equal Opportunities Policy or Harassment Policy may have been breached. In any case of possible theft/fraud the HR and Finance Directors will be notified as stated in the [Invest NI Fraud Response Plan](#).

Expires 30th June 2012

Appendix A – LAW

Invest NI is required by law to comply with the following Acts. Please note that this list is not exhaustive.

Computer Misuse Act (1990) - <http://www.legislation.gov.uk/ukpga/1990/18/contents>
 Copyright, Designs & Patents Act (1988) - <http://www.legislation.gov.uk/ukpga/1988/48/contents>
 Data Protection Act (1998) - <http://www.legislation.gov.uk/ukpga/1998/29/contents>
 Employment Act (2002) - <http://www.legislation.gov.uk/ukpga/2002/22/contents>
 Environmental Information Regulations (2004) - <http://www.legislation.gov.uk/uksi/2004/3391/contents>
 Freedom of Information Act (2000) - <http://www.legislation.gov.uk/ukpga/2000/36/contents>
 Obscene Publication Act (1964) - <http://www.legislation.gov.uk/ukpga/1964/74?view=extent>
 Protection of Children Act (1978) - <http://www.legislation.gov.uk/ukpga/1978/37>
 Regulation of Investigatory Powers Act (2000) - <http://www.legislation.gov.uk/ukpga/2000/23/contents>

Appendix B – INFORMATION ASSET OWNERS

The following table contains the contact names of the people responsible for managing major Invest NI application systems:

System Type	ICT Analyst/Support	Information Asset Owner
Client Database	John McBride	Damian McAuley
Client Contact Management System	Lorraine McAllister	Damian McAuley
Document & Record Management System	Joan Boone	Damian McAuley
Reporting system	Lorraine McAllister	Damian McAuley
Human Resources Management System	Ciaran McGirr	Liam Hagan
Finance system	<i>Northgate IS</i>	Brian Dolaghan
Overseas CRM system	Ciaran McGirr	Bill Montgomery
Payroll system	Ciaran McGirr	Brian Dolaghan
Web Content Management System	Oliver McErlane	Peter Harbinson
Network	Jonathan Caughey	Liam Hagan
www.nibusinessinfo.co.uk	Oliver McErlane	Olive Hill
www.investni.com	Oliver McErlane	Peter Harbinson
www.buynifood.co.uk	<i>Pierce Communications</i>	Maynard Mawhinney
www.edpminis.co.uk	Jonathan Caughey	Alistair Higgins
Telephony system	Claire Greenwood	Liam Hagan

Expires 30th June 2012

Appendix C – Summary of INVEST ICT SYSTEMS ACCEPTABLE USAGE POLICY

The ICT Systems Acceptable Usage Policy can be summarised as follows:

- This policy applies to all Invest NI staff including contractors, secondees and temporary staff.
- Invest NI end users have the right to update data where they are the data “owners” or within agreed limits.
- All staff using ICT systems will have a personal responsibility for the security & integrity of that system. Each ICT system in Invest NI will have a nominated Information Asset Owner who will have full responsibility for IT security on that System.
- Invest NI operates a Software Asset Management (SAM) Policy
 - **All software must be purchased and installed by the ICT Team.**
 - **The illegal copying of software or data is theft.**
 - **The deliberate introduction of malicious or unlicensed software to a system is a criminal offence under the Computer Misuse Act (1990).**
- When a member of staff is appointed, changes role or leaves Invest NI then the staff member’s access rights will be reviewed or cancelled on departure from Invest NI by the ICT Team.
- **If an Invest NI user detects a virus on their machine this should be reported immediately.**
- No ICT software or hardware shall be removed from Invest NI without the express permission of the ICT Team except for laptops or mobile devices that are the responsibility of each individual user.
- All hardware **must** be switched off when not in use for extended periods, such as overnight or during weekends.
- Sensitive printouts, for example those identifying named individuals or financial details, must be placed in confidential waste bins provided.
- Any hardware not procured by Invest NI’s ICT Team must not be introduced to the Invest NI network.
- Invest NI maintains an Intellectual Property (IP) Policy. Invest NI owns the IP created by employees and will claim ownership if IP is created under certain working conditions.
- Breaches of the Invest NI ICT Systems Acceptable Usage Policy shall be logged by the ICT Team. Any Breach discovered by an Invest NI user should be forwarded to the IT Security Officer for further investigation. In any case of possible theft/fraud the HR and Finance Directors will be notified as stated in the **Invest NI Fraud Response Plan**.

Expires 30th June 2012