	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 1 of 8
---	---	-------------------------------------	--	------------------------

1. Purchase of Information Technology, Systems and Equipment

- 1.1. This guidance is in accordance with the NITHC / TRANSLINK Financial Memorandum Final Version dated 28/07/07.
- 1.2. Those in the Purchasing Department who are involved in the Procurement of IT must ensure they have awareness of the following Special requirements which are placed on the IT Department and also make sure that the WEEE Regulations (see TPP111) are also considered when considering the Disposal of IT Equipment.

1.3. IT Projects


IT projects present risks which differ from those arising from capital expenditure generally. DAO 33/03 deals with IT enabled projects and states that “departmental accounting officers should ensure that equally rigorous standards are applied to ICT enabled projects and associated expenditure in their Agencies, NDPBs and other sponsored bodies for which they are responsible”

Business cases in respect of IT projects should be consistent with the requirements of DAO 33/03.

The CPD guidance note 06/04 “The OGC Gateway Review Process” must also be considered when dealing with IT projects as it supplements the instructions issued in the DAO (DFP) 33/03. It is the responsibility of the Project Manager to ensure a Gateway Review is conducted if it is required.

2. Delegated Arrangements for Information Technology, Systems and Equipment

- 2.1. Due to the specific risks involved in the acquisition of IT equipment and systems, all procurements must be carried out in accordance with the guidance contained in DAO (DFP) 33/03 – Information Communication Technology (ICT) – Enabled Business Change, Guidance on Management, Justification, Evaluation and Responsibilities.
- 2.2. IT projects should be the subject of competitive tendering unless, exceptionally, there are convincing reasons to the contrary. The form of competition should be appropriate to the value and complexity of the project and in line with the Procurement Control Limits (which can be found in TPP101a Procurement Planning and Requests for Contract Action).

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 2 of 8
---	---	-------------------------------------	--	------------------------

2.3. Business cases should be constructed for all IT projects in accordance with the guidance and templates contained in DAO 33/03. Requirements for approval of IT business cases are set out below.

Delegated Limits for Approval of IT Projects, Systems and Equipment


	Internal Approval [to be completed by NITHC]	DRD Approval	DFP Supply Approval
Up to £1,000	Blank on MSFM therefore as per Agresso		
£1,000 to £25,000	Blank on MSFM therefore as per Agresso		
£25,000 to £75,000	Blank on MSFM therefore as per Agresso		
£75,000 to £500,000	Chief executive	Required	
Over £500,000		Required	Required

NITHC /Translink Financial Memorandum – Final Version 28/07/2006


3. Contracting for ICT and Information related requirements.

3.1. OGC ICT Model contract should be used as the basis and guide for public sector ICT procurement. This document should be considered for all Translink requirements which have an element of ICT within them. The terms and conditions relating to ICT in this model contract are the baseline precedent clauses for consideration when contracting for outputs or outcomes in ICT. The Model contract can be found at <http://www.partnershipsuk.org.uk/ictguidance/>. This means that when drafting contracts for ICT or information related requirements both the Translink standard and the ICT model terms and conditions must be considered.


3.2. OGC Information Note 13/08 – 26th November 2008 stresses the importance of certain key Terms and Conditions being included in ICT or information related contracts and the Cabinet Office made these enhancements mandatory for all new contracts from the 1st July 2008 (in Central Civil Government), therefore Translink view it as best practice to include these in contracts for this area. The headings of these recommended conditions are illustrated below;

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 3 of 8
---	---	---	---	------------------------

the full clauses should always be taken from the master OGC ICT Model contract template to ensure Translink are using the latest version. The Conditions should also be used after consultation with the Translink IT Department and the Translink Records Management Section as there is reference to security policies, staff vetting policy and disaster recovery plans which need to be in place for the conditions to be effective.

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 4 of 8
---	---	-------------------------------------	--	------------------------

Recommended clause	Translink Position		
<ul style="list-style-type: none"> Contractor Personnel – Staffing Security <table border="1" data-bbox="151 539 651 1182"> <tr> <td data-bbox="151 539 363 1182"> "Staff Vetting Procedures" (OGC ICT Model Contract Definition) </td> <td data-bbox="363 539 651 1182"> the Authority's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989; </td> </tr> </table>	"Staff Vetting Procedures" (OGC ICT Model Contract Definition)	the Authority's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;	<p>Insert into ICT/ information related contracts as required.</p> <p>Translink Vetting Procure for employees of Translink whose role will involve the handling of information of a sensitive or confidential nature or the handling of information is to take up employee references prior to offering the post (current at August 08 HR Division). Therefore Translink Contractors whose role will involve the handling of information of a sensitive or confidential nature or the handling of information shall also be required to comply with the Translink policy on 'taking up references'.</p> <p>The Staffing Security clause 28.11 will need to be amended by Translink by adding after the last line "Translink Vetting and Recruitment Procedure for those whose role will involve the handling of information of a sensitive or confidential nature or the handling of information can be obtained by contacting the Translink HR Division".</p> <p>If a requirement with highly sensitive information is considered then enhancements to this vetting policy and the detail of which is held within the contract may be required. The Translink Records & Information Manager should be consulted.</p> <p>For further information about Staff Vetting please contact the Translink Records & Information Manager in the first instance and the Human Resources Division in the second.</p>
"Staff Vetting Procedures" (OGC ICT Model Contract Definition)	the Authority's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;		
<ul style="list-style-type: none"> Authority Data 	Insert into ICT/ information related contracts as required		
<ul style="list-style-type: none"> Protection of Personal Data 	Evaluate, review and omit if required Translink standard Condition on Data Protection Act 1998 and apply the enhanced OGC Protection of Personal Data Clause if personal data is involved.		
<ul style="list-style-type: none"> Freedom of Information 	This is the same as the Translink standard FOI clause and no changes are required.		

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 5 of 8
---	---	-------------------------------------	--	------------------------

<ul style="list-style-type: none"> Confidentiality 	This is the same as the Translink standard Confidentiality clause and no changes are required.
<ul style="list-style-type: none"> Security Requirements 	Insert into ICT/ information related contracts as required
<ul style="list-style-type: none"> Warranties 	Insert into ICT/ information related contracts as required
<ul style="list-style-type: none"> Security Requirements Plan (schedule) 	Insert into ICT/ information related contracts as required

To find the OGC guidance note please follow the link:

http://www.ogc.gov.uk/documents/PPN13_08_Data_Handling.pdf

In addition please find the NITHC/Translink Data Protection Policy which should be regarded when considering information related requirements at the following link:


<http://sharepoint/C5/Records%20and%20Information%20Manage/default.aspx>

3.3. It should be noted that ICT or information related contracts that use information systems do not only sit within the IT Department. Therefore any contract in which information and communication systems are utilised will require enhanced measures to protect the Translink information they handle. The definitions listed below are used by the Translink to define Sensitive Data and therefore can be used as a reference when considering OGC ICT Terms in cases which are outside of pure ICT. The OGC Information Assurance in Procurement document can be viewed below in Annex 1.

Sensitive Data Definition

NITHC / Translink categorises 'sensitive data' into three distinct groupings, being:

- (1) Sensitive personal data as defined by the Data Protection Act 1998, which covers information concerning a person's:
 - Racial or ethnic origin;
 - Political opinions;
 - Religious beliefs or other beliefs of a similar nature;
 - Membership of a trade union;
 - Physical or mental health condition;
 - Sexual life;
 - Commission or alleged commission of any offence; and
 - Involvement in proceedings for any offence committed or alleged to have been committed.

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 6 of 8
---	---	-------------------------------------	--	------------------------

(2) Personal data (i.e. names, address, contact details, journey details etc.) relating to customers within vulnerable groups i.e. young people, the elderly and any other group of persons which may be deemed as vulnerable.

(3) Commercially sensitive information relating to the organisation or the activities of the organisation – this includes all information which, if accessed by the wider public, could prejudice the commercial interests of NITHC / Translink – for example information relating to route profitability.

For further information on the Definition's above please contact the Records Management Section of Translink.

4. Further Reading

- 4.1. CPD guidance note 06/04 The OGC Gateway Review Process.
- 4.2. OGC Information note 08/08 Data Handling Review – Mandatory application for security provisions in contracts.
- 4.3. OGC Model ICT Services Agreement – Baseline Precedent Clauses for Consideration when Contracting for Outputs or Outcomes
- 4.4. TPP115 Control of Documents
- 4.5. NITHC /Translink Financial Memorandum – Final Version 28/07/2006


Annex 1

Information Assurance in Procurement

Every Government Department should be taking suitable precautions to safeguard its information. Therefore every Information Communications Technology (ICT), or information related, service contract must contain Information Assurance (IA) requirements. Indeed IA extends beyond ICT contracts, since for example even in construction projects there is likely to be an ICT system used in designing, managing or communicating about the project, and this will have IA requirements.

What is Information Assurance?

Information Assurance (IA) is the confidence that information and communication systems will, through their life cycle, protect the information they handle (i.e. ensure the information's Confidentiality and Integrity), and will

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 7 of 8
---	--	--	---	-------------------------------

function as and when they need to (i.e. information is Available as required), under the control of legitimate users. This confidence is vital, as UK government and business all depend on such information systems.

1.1. Why is IA needed?

Information is fundamental to the business of government. Effective IA is core to ensuring that this asset is safeguarded appropriately.

The continued growth throughout government in the use of ICT systems, all linked together, carries with it increased vulnerability. In addition these ICT systems are under threat of attack from foreign intelligence services, criminal gangs, and even individuals inside the organisation.

Protection against such threats and vulnerabilities is essential.

Assurance is the confidence that may be held in the security provided by an ICT system or products supporting a service. CESG (the UK National Technical Authority for IA) has developed an Assurance Framework which is intended to stimulate 'good practice' thinking about the assurance of an ICT solution throughout its lifecycle, from inception to decommissioning. The framework is not a prescriptive process, a 'badge' or a 'check list' – it is a tool for organisations to use within their risk management process.

IA is therefore something that should not be considered as a separate entity in the procurement process, but must be integral and is key to meeting the business objectives, preserving reputation, and legal compliance etc.

1.2. Government Security Policy

The Manual of Protective Security (MPS) (via www.security-matters.gsi.gov.uk) sets out HMG policy on all aspects of protective security (including physical, personnel, communications and information security matters). The MPS in turn references other IA standards, including IS1 and IS2 covering risk management. The MPS applies to all government departments, and to any other organisation involved in handling government assets.


International Standards ISO/IEC27002 and ISO/IEC27001 are referenced in Schedule 2.5 of the ICT model contract.

The MPS is currently under review, and will be replaced by the Security Policy Framework (SPF) in October 2008.

How does the ICT Model Contract for Services deal with Information Assurance (IA)?

The Information Assurance requirements must be explicitly stated in the contract specification. The terms and conditions of the contract must ensure that failure to deliver any aspect of the IA requirement will be at the supplier's risk. However failure by the supplier will invariably have a knock on effect on the department's business function and reputation. Tender evaluation must explicitly assess the suitability of the proposed Information Assurance solutions.

Demonstrating legal compliance is one key aspect of any contract. The ICT model contract has provisions dealing with a range of information protection aspects: Clause 40 (Authority Data); Clause 41 (Protection of Personal Data); Clause 42 (Freedom of Information) and Clause 43 (Confidentiality).

	TITLE: Purchase of Information Technology, Systems and Equipment TPP125	OWNER: Purchasing Manager	LAST MODIFIED: 6th January 2009	PAGE: 8 of 8
---	--	--	---	-------------------------------

How ever given the variety of ICT applications and their relationships to the wider business it is prudent to seek advice to ensure that a) the security requirements cover the IA issues adequately; and b) the resulting Security Plan (produced in accordance with Schedule 2.5 of the ICT model contract) also meets Government IA standards. Authorities should also include security requirements from: 2.1 (Service Description); 4.2 (Commercially Sensitive Information); and 8.4 (Record Provisions).

The provision of adequate IA is not straight forward, and relies for example on effective and continuous Information Risk Management. In order to gain appropriate assurance in a service (or ICT system or product) a full risk assessment should be carried out. The MPS is a good starting point, but consultation should be sought within an organisation from those responsible for risk management.

If in doubt appropriate advice should be sought:

- at a HMG policy level, from CSIA, www.cabinetoffice.gov.uk/csia/ia_governance.aspx ;
- at departmental level, from CESG for technical IA advice, www.cesg.gov.uk
- at an organisational level, from the Department's Chief Information Officer (CIO) and Chief Technology Officer (CTO), Departmental Security Officer (DSO) and IT Security Officer (ITSO), and from private sector IA Consultants who are part of the CESG Listed Adviser Scheme (CLAS) www.cesg.gov.uk/site/clas/index.cfm.

1.3. Developing an IA Catalogue

OGC, Cabinet Office, MOD and CESG are working together to provide an easy route to market for the public sector to purchase government approved IA products and services (<http://www.dcsacat.mod.uk>).

Source:

<http://www.partnershipsuk.org.uk/ictguidance/newsattachments/documents/IA%20guidance%20for%20standard%20contract.doc>