

Procurement Policy Note: Data Handling Review



Further information about the processes and contractual provisions that are necessary for robust and appropriate data handling processes.

Information note 13/08 – 26 November 2008

Issue

1. This information note provides further guidance on the mandatory application of security provisions in contracts in order to safeguard data.

Timing

2. The requirements in this PPN build on PPN 08/08 and apply to all new contracts entered into since 1 July 2008. For ease of reference this PPN adopts material from PPN 08/08 and replaces it.

Dissemination

3. To be circulated within your organisation, agencies, non-departmental public bodies (NDPBs) and any other bodies for which you are responsible.

Contact

4. Enquiries about this paper should be addressed to the OGC Service Desk 0845 000 4999 or servicedesk@ogc.gsi.gov.uk.

Background

5. PPN 08/08 highlighted the fact that information is a key asset and its proper use is fundamental to the delivery of public services. This PPN builds on the guidance set out in PPN08/08. Procuring Authorities need to identify the different types of information they handle and the action that must be taken to protect this information. This assessment should be undertaken in the context of clear minimum standards and with the aim of protecting personal and any other confidential information and also applies where information may be managed and processed by third parties
6. The report on Data Handling Procedures in Government Report (“the Data Handling Review”) outlines a number of mandatory standards for data handling, in order to provide a minimum baseline level for the protection and handling of personal data. Paragraph 3.9 of the Data Handling Review states that “From July 2008, standard contract clauses on information assurance will be incorporated into contracts”. The aim of this measure is to provide assurance that any contract will have appropriate clauses and associated processes in place, which comply with the new standards.
7. Procuring Authorities are encouraged to read the explanatory note in Annex 2: This note considers how Information Assurance relates to the Security Schedule in the OGC ICT model

agreement (and consequently all relevant departmental security policies and procedures).

8. Procuring Authorities are reminded that information assurance risks may arise in a wide range of contracts. This means that the identification and appropriate management of such risks should be part of all organisations' internal risk management strategies and processes. Relevant contractual provisions which are underpinned by appropriate processes should ensure greater information assurance.

The basic mandatory requirement for contracts (including framework agreements) let from 1 July 2008

9. The basic mandatory requirement is for there to be contractual clauses which deal with the following specified issues: contractor personnel – staffing security, authority data, protection of personal data, freedom of information, confidentiality, security requirements, warranties, in all contracts where personal or other confidential information will be used, disseminated or otherwise handled by a Procuring Authority and any other third party associated with the contract. (i.e. not just applicable to ICT contracts). There should also be a Security Requirements and Plan. The clauses and specific security plan schedule from the OGC Model ICT Services Agreement (“**the OGC Model clauses**”) which address these matters are the recommended text. These clauses can be found at Annex 3:

Application of the Mandatory Requirement

10. There are some contracts for which it may be clear that the use, dissemination or other handling of personal and/or other confidential information is a clearly identifiable part of delivering the contractual requirement e.g. for the provision of ICT services to implement a project/programme where the handling, transference and other use of information is a key part of the requirement. In these types of contracts there must be clauses which address: contractor personnel – staffing security, authority data, protection of personal data, freedom of information, confidentiality, security requirements, warranties, and a security requirements and plan. It is recognised that ICT contracts are wide ranging and may or may not involve the handling of personal or other confidential information. Procuring Authorities are best placed to assess which contracts involve information handling.
11. Once a Procuring Authority has identified a contract where the use, dissemination or other handling of personal and/or confidential information is likely, a decision must be taken as to whether the contract should contain clauses which are appropriate to address any information assurance risks. The OGC Model clauses should be adopted unless their inclusion is disproportionate and/or unnecessary in the context of the particular contract.
12. In some circumstances the contracts which a Procuring Authority proposes to use for its requirements may contain clauses which provide a greater or lesser degree of protection for information security or which addresses risks that are not set out in the OGC Model clauses. Procuring Authorities are responsible for assessing whether all of the OGC Model clauses are necessary for each contract, this assessment necessarily involves consideration of whether information assurance risks can be addressed by more or fewer clauses than are set out in the OGC Model clauses. Given that public bodies are subject to the Data Protection Act 1998 and Freedom of Information Act 2000 it is expected that there will always be clauses regarding obligations under those Acts in contracts. In any event it would be highly unusual for a contract to have none of the mandatory clauses.

Application of the requirements to contracts (including framework agreements) let before 1st July 2008

13. Information Assurance is a fundamental issue for all organisations and Procuring Authorities are advised to assess whether any changes may be necessary to existing contracts by considering matters such as:

- (a) whether any of their existing contracts depend on the sharing of information (internally or with third parties)
 - (b) where information is being shared, whether any risks arise from the use/handling of such information
 - (c) whether the Procuring Authority has identified and implemented appropriate ways of addressing any risks by e.g. the use of certain contractual provisions, contract management and information assurance processes.
14. The points set out at 13(a) – (c) above are *indicative* only and the extent to which changes to existing contract terms and processes may be necessary is a matter that Procuring Authorities are best placed to assess.

General

15. The requirements set out in the preceding paragraphs apply to all departments in Central Civil Government and any bodies over which they have direct control. Where Departments cannot require the use of new measures throughout their area of responsibility they are required to influence their delivery chain partners.
16. Appendix 1 provides further guidance on a number of questions that Procuring Authorities might have and aims to assist procurers in adhering to these new requirements.

1. **Question:**
If the requirements apply to all contracts does that include call-off contracts under existing Framework Agreements?

Answer:

Yes with effect from 1 July 2008.

2. **Question:**
What does the “handling” of information mean?

Answer:

2.1 Where a Procuring Authority has information in its custody or control handling refers to any action taken by the Procuring Authority which determines constraints on the use of the information in relation to the following:

- (a) the processes necessary to ensure that the information is secure, accessible to the extent required;
- (b) the time(s) at which access to the information may be required;
- (c) the specific location(s) in which the information may be stored, used or to which it may be transferred;
- (d) the purposes for which the information can be used;
- (e) the persons who are authorised to have access to and/or use the information.

The matters referred to in (a) – (e) above are *indicative* only as Procuring Authorities may specify more or fewer requirements in relation to information handling depending on the particular contract in issue.

2.2 A supplier handles information where:

- (a) it uses information obtained and/or created in order to perform its contractual obligations to the Procuring Authority; **and**
- (b) complies with the Procuring Authority’s instructions in respect of matters *such as* the manner in which the information is stored, the purposes for which the information may be used, the individuals who may be granted access to the information, the processes necessary to ensure the integrity and security of the information, whether or not the information may be shared with any other person/organisation and any constraints on sharing.

The matters referred to in (a) – (b) above are *indicative* only.

3. **Question:**
The PPN mentions personal information and confidential information; what does this mean?

Answer:

In the context of the PPN a reference to personal information means any information about a person (including sensitive information). Confidential information means any information that can be described in this manner for the following reasons:

- (a) the nature of the information,

- (b) the circumstances in which it was created, generated, disseminated, held or used in any way or
- (c) the fact that the information falls within a legally defined or legally recognised category of protected information

4. Question:
How can I apply the requirements in practice?

Answer:

The approach adopted by a Procuring Authority will vary depending on the particular form of contractual documentation (e.g. Framework Agreement, Call-Off contract, individual Public Contract) that may require change. It would be useful to consider the following points:

- (a) Is it necessary to change any of the terms of the relevant agreement?
- (b) If yes, is there an enabling provision which allows this?
- (c) In all circumstances consider whether any change to contractual provisions alters the relationship between the parties and/or the pricing
- (d) In all circumstances Procuring Authorities should seek legal advice

The points set out at (a) – (d) above are *indicative* only and it is recognised that there may be other matters which a Procuring Authority should consider.

5. Question:
What does “adoption”/ “inclusion” of the OGC Model clauses mean?

Answer:

Adoption/inclusion of clauses from the OGC Model clauses means:

- (a) using the text of the clauses in an un-amended form in a Procuring Authority’s contract where such use is appropriate and consistent with the language and meaning of existing contract terms;
- (b) using the text of the OGC Model clauses with the amendments that are necessary to ensure linguistic clarity/consistency with existing contract terms;
- (c) using the text of the OGC Model clauses, subject to any changes that may be necessary for linguistic clarity or in order to address additional issues which relate to the specific contract.

6. Question:
How should a Procuring Authority respond to suppliers’ comments that any changes required for enhanced information security are impermissible, change the nature of the contractual requirement and/or increases costs?

Answer:

The requirement that all contracts contain provisions which ensure greater information assurance is mandatory for all government departments and their executive agencies. Security and other information assurance provisions would normally be permissible under an enabling provision (e.g. a clause about compliance with the Authority’s general or specific instructions) in a Framework Agreement, Call-Off Contract or individual Public Contract. Any changes required for enhanced information security are essentially about the way in which the services are to be provided and not necessarily about the scope of service provision.

If the changes that a Procuring Authority requires are likely to or will result in a material change to the scope of a Framework Agreement, Call-Off Contract or individual Public Contract this must be demonstrable in fact. It is not inevitable that any or every potential change a Procuring Authority requires for the purposes of information assurance will change the nature of the contract (whether in the economic or operational balance between the parties). *If* it appears likely that a change in the nature of the contract may

occur Procuring Authorities should seek legal advice.

If amendments to a Framework Agreement, Call-Off Contract or individual Public Contract *in order to* ensure information assurance mean in fact that the cost of service provision will increase then Procuring Authorities will need to consider how to address this situation and take appropriate action.

7.

Question:

Which factors should a Procuring Authority consider when assessing whether or not its information assurance clauses are adequate?

Answer:

Procuring Authorities should consider a range of issues including,

- (a) whether the contract involves the collection, storage, dissemination, destruction of information that is personal/confidential (whether commercially or for other reasons);
- (b) the types of information that are being used/handled under the contract/framework, by whom, and where will the handling take place;
- (c) the risks that arise in respect of each type of information and each type of process/transaction that such information is likely to be part of – i.e. internal departmental dissemination only, departmental and supplier dissemination, inter-departmental dissemination etc;
- (d) the steps that must be taken to mitigate any risks identified, including any amendments to contractual clauses and the organisational processes which underpin such clauses.

The points set out at (a) – (d) are *indicative* only. Procuring Authorities must take such steps as are appropriate in the context of any particular contract that is under consideration. A risk assessment (whether general or focussed on information assurance in particular) should form part of this process together with advice from the organisational Senior Information Risk Owner (SIRO), legal advisers and any other relevant advisers if necessary.

Where it is decided that OGC clauses are not appropriate or applied in full, the SIRO must be fully aware and have agreed to the changes. The SIRO must also ensure that equivalent measures are in place to compensate for any potential lack of control.

Annex 2

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 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.

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.

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 December 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).

However 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.

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>).

Annex 3

OGC ICT Services Model Agreement Security Provisions

This document contains the security provisions that should be included in any UK government IT contract which involves the storage or handling of personal or sensitive data. The document includes only those security provisions that are contained in the Terms and Conditions. For a complete set of security provisions the reader should also see Schedule 2.5 (Security Requirements and Plan, available at the Partnerships UK website, <http://www.partnershipsuk.org.uk/ictguidance/>)

See also Schedule 1 of the Model ICT Agreement (appended to the Terms and Conditions, also on the PUK website) for definitions of defined terms (those which have an initial capital letter in the text below).

Clause 28.11 and 28.12: Contractor Personnel – Staffing Security

The Contractor shall comply with the Staff Vetting Procedures in respect of all Contractor Personnel employed or engaged in the provision of the Services. The Contractor confirms that all Contractor Personnel employed or engaged by the Contractor at the Effective Date were vetted and recruited on a basis that is equivalent to and no less strict than the Staff Vetting Procedures.

The Contractor shall provide training on a continuing basis for all Contractor Personnel employed or engaged in the provision of the Services in compliance with the Security Policy and Security Plan.

Clause 40: Authority Data

The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Agreement or as otherwise expressly authorised in writing by the Authority.

To the extent that Authority Data is held and/or processed by the Contractor, the Contractor shall supply that Authority Data to the Authority as requested by the Authority in the format specified in schedule 2.1 (Services Description) [and/or in schedule 8.5 (Exit Management)].

The Contractor shall take responsibility for preserving the integrity of Authority Data and preventing the corruption or loss of Authority Data

The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Business Continuity and Disaster Recovery Plan. The Contractor shall ensure that such back-ups are available to the Authority at all times upon request and are delivered to the Authority at no less than **[insert period]** monthly intervals.

The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy.

If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:

- require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data to the extent and in accordance with the requirements specified in schedule 8.6 (Business Continuity and Disaster Recovery Provisions) and the Contractor shall do so as soon as practicable but not later than **[insert period]**; and/or
- itself restore or procure the restoration of Authority Data, and shall be repaid by the Contractor any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in schedule 8.6 (Business Continuity and Disaster Recovery Provisions).

If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

Clause 41 Protection of Personal Data

With respect to the parties' rights and obligations under this Agreement, the parties agree that the Authority is the Data Controller and that the Contractor is the Data Processor.

The Contractor shall:

- Process the Personal Data only in accordance with instructions from the Authority (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by the Authority to the Contractor during the Term);
- Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of

the Services or as is required by Law or any Regulatory Body;

- implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;
- take reasonable steps to ensure the reliability of any Contractor Personnel who have access to the Personal Data;
- obtain prior written consent from the Authority in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services;
- ensure that all Contractor Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this clause [reference];
- ensure that none of Contractor Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority;
- notify the Authority (within [five] Working Days) if it receives:
 - a request from a Data Subject to have access to that person's Personal Data; or
 - a complaint or request relating to the Authority's obligations under the Data Protection Legislation;
- provide the Authority with full cooperation and assistance in relation to any complaint or request made, including by:
 - providing the Authority with full details of the complaint or request;
 - complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Authority's instructions;
 - providing the Authority with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Authority); and
 - providing the Authority with any information requested by the Authority;

permit the Authority or the Authority Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit, in accordance with clause [reference] (Audits), the Contractor's data Processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Authority to enable the Authority to verify and/or procure that the Contractor is in full compliance with its obligations under this Agreement;

provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data (within the timescales required by the Authority); and

not Process Personal Data outside the European Economic Area without the prior written consent of the Authority and, where the Authority consents to a transfer, to comply with:

- the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is transferred; and
- any reasonable instructions notified to it by the Authority.

The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Agreement in such a way as to cause the Authority to breach any of its applicable obligations under the Data Protection Legislation.

Clause 42: Freedom of Information

The Contractor acknowledges that the Authority is subject to the requirements of the Code of Practice on Government Information, FOIA and the Environmental Information Regulations and shall assist and cooperate with the Authority to enable the Authority to comply with its Information disclosure obligations.

The Contractor shall and shall procure that its Sub-contractors shall:

- transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within [two] Working Days of receiving a Request for Information;
- provide the Authority with a copy of all Information in its possession, or power in the form that the Authority requires within [five] Working Days (or such other period as the Authority may specify) of the

Authority's request; and

- provide all necessary assistance as reasonably requested by the Authority to enable the Authority to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

The Authority shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, FOIA or the Environmental Information Regulations.

In no event shall the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Authority.

The Contractor acknowledges that (notwithstanding the provisions of Clause 42[reference]) the Authority may, be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Services:

- in certain circumstances without consulting the Contractor; or
- following consultation with the Contractor and having taken their views into account;

provided always that where [reference] applies the Authority shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

The Contractor shall ensure that all Information is retained for disclosure [in accordance with schedule 8.4 (Records Provisions)] and shall permit the Authority to inspect such records as requested from time to time.

The Contractor acknowledges that the Commercially Sensitive Information listed in schedule 4.2 is of indicative value only and that the Authority may be obliged to disclose it in accordance with clause [reference].

Clause 43: Confidentiality

Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this Agreement, each party shall:

- treat the other party's Confidential Information as confidential [and safeguard it accordingly]; and
- not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

Clause [reference] shall not apply to the extent that:

- such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA, Code of Practice on Access to Government Information or the Environmental Information Regulations pursuant to clause [reference] (Freedom of Information);
- such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;
- such information was obtained from a third party without obligation of confidentiality;
- such information was already in the public domain at the time of disclosure otherwise than by a breach of this Agreement; or
- it is independently developed without access to the other party's Confidential Information.

The Contractor may only disclose the Authority's Confidential Information to the Contractor Personnel who are directly involved in the provision of the Services and who need to know the information, and shall ensure that such Contractor Personnel are aware of and shall comply with these obligations as to confidentiality.

The Contractor shall not, and shall procure that the Contractor Personnel do not, use any of the Authority's Confidential Information received otherwise than for the purposes of this Agreement.

[At the written request of the Authority, the Contractor shall procure that those members of the Contractor Personnel identified in the Authority's notice signs a confidentiality undertaking prior to commencing any work in accordance with this Agreement.]

Nothing in this Agreement shall prevent the Authority from disclosing the Contractor's Confidential Information:

- to any Crown Body or any other Contracting Authority. All Crown Bodies or Contracting Authorities receiving such Confidential Information shall be entitled to further disclose the Confidential Information

to other Crown Bodies or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Authority;

- to any consultant, contractor or other person engaged by the Authority or any person conducting an Office of Government Commerce gateway review;
- for the purpose of the examination and certification of the Authority's accounts; or
- for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources.

The Authority shall use all reasonable endeavours to ensure that any government department, Contracting Authority, employee, third party or Sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to clause [reference] is made aware of the Authority's obligations of confidentiality.

Nothing in this clause [reference] shall prevent either party from using any techniques, ideas or know-how gained during the performance of the Agreement in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of IPR.

Clause 48: Security Requirements

The Contractor shall comply, and shall procure the compliance of the Contractor Personnel, with the Security Policy and the Security Plan and the Contractor shall ensure that the Security Plan produced by the Contractor fully complies with the Security Policy.

The Authority shall notify the Contractor of any changes or proposed changes to the Security Policy.

If the Contractor believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the Services it may submit a Change Request. In doing so, the Contractor must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Change Control Procedure.

Until and/or unless a change to the Charges is agreed by the Authority pursuant to clause [reference] the Contractor shall continue to perform the Services in accordance with its existing obligations.

Malicious Software

The Contractor shall, as an enduring obligation throughout the Term, use the latest versions of anti-virus definitions available [from an industry accepted anti-virus software vendor] to check for and delete Malicious Software from the ICT Environment.

Notwithstanding clause [reference], if Malicious Software is found, the parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

Any cost arising out of the actions of the parties taken in compliance with the provisions of clause [reference] shall be borne by the parties as follows:

- by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software or the Authority Data (whilst the Authority Data was under the control of the Contractor); and
- by the Authority if the Malicious Software originates from the Authority Software or the Authority Data (whilst the Authority Data was under the control of the Authority).

Clause 45.2: Warranties

The Contractor warrants, represents and undertakes for the duration of the Term that:

- all personnel used to provide the Services will be vetted in accordance with Good Industry Practice, the Security Policy and the Standards;

OGC 1 Horse Guards Road,
London SW1A 2HQ

Service Desk: 0845 000 4999
ServiceDesk@ogc.gsi.gov.uk
www.ogc.gov.uk

About OGC

The Office of Government
Commerce is an independent
Office of HM Treasury.

The OGC logo is a registered
trademark of the Office of
Government Commerce
in the United Kingdom.

OGC Service Desk

OGC customers can contact
the central OGC Service Desk
about all aspects of
OGC business.

The Service Desk will also
channel queries to the
appropriate second-line
support. We look forward
to hearing from you.

You can contact the Service
Desk 8am – 6pm Monday
to Friday:

T: 0845 000 4999
E: ServiceDesk@ogc.gsi.gov.uk
www.ogc.gov.uk

Press enquiries

T: 020 7271 1318
F: 020 7271 1345

© Crown copyright 2008