

# Procurement Policy Note

Information Note 08/08 – 1 July 2008

## Data Handling Review

### Mandatory application of security provisions in contracts

#### Issue

1. This information note provides guidance on the new Cabinet Office **mandatory** requirements for the adoption of OGC model contract clauses and provisions relating to security and information assurance in contracts. This follows the publication of the Data Handling Procedures in Government, June 2008.

#### Timing

2. The mandatory use of the clauses and provisions applies to all new contracts signed from 1 July 2008.

#### 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 [servicedesk@ogc.gsi.gov.uk](mailto:servicedesk@ogc.gsi.gov.uk).

#### Background

5. Information is a key asset, and its proper use is fundamental to the delivery of public services. Whilst procuring authorities are best placed to understand their information and protect it, they need to do so with a context of clear minimum standards, ensuring protection of personal information. This applies equally where information may be managed or processed by third parties.
6. The Data Handling Procedures in Government report outlines a number of new mandatory standards for data handling, in order to provide a minimum baseline level for protection and handling of personal data.

7. Within these measures, paragraph 3.9 states that “From July, **standard contract clauses** on information assurance will be incorporated into contracts”. The aim is to provide assurance that any contract will have processes in place which comply with the new standards.
8. This requires procuring authorities to use the information assurance/security elements of *OGC’s model terms and conditions for ICT services contracts*, which are the approved Government standards for ICT services contracts, and which embody current policy and best practice. The full suite of terms and conditions (which includes all the security/information assurance clauses and provisions) can be accessed on Partnerships UK’s website at <http://www.partnershipsuk.org.uk/ictguidance/index.asp>.
9. These requirements 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 immediately, they are required to influence their delivery chain partners.
10. The Data Handling Procedures in Government Report makes it clear that Departments will be accountable for the actions taken to ensure that the mandatory standards are applied. This accountability will be exercised through an annual assessment process to support the Accounting Officer’s judgement for the Statement on Internal Control.
11. Appendix 1 provides further guidance and help on a number of issues and questions, which aims to assist procurers in adhering to these new requirements.

**Policy and Standards Division**  
**Office of Government Commerce**

## **Appendix 1**

### **Key questions answered**

1. Before you start - how information assurance relates to the security elements of OGC's guidance

OGC would encourage you to read an explanatory note <http://www.partnershipsuk.org.uk:/ictguidance/newsattachments/documents/A%20guidance%20for%20standard%20contract.doc> around how Information Assurance relates to the Security schedule (2.5) in the OGC ICT model agreement (and by consequence all relevant departmental security policies and procedures) before embarking on the drafting of any security related provisions.

2. Which clauses and schedules must a procuring Authority include unamended from the OGC Model ICT Services Agreement?

In order to comply with the minimum requirements, all procuring Authorities should ensure that the following clauses from the OGC Model ICT Services Agreement<sup>1</sup> are included in any ICT or information related contract. Third party contracts shall also comply with minimum requirements.

<http://www.partnershipsuk.org.uk:/ictguidance/>

### **Clause 28.11 and 28.12 Contractor Personnel – Staffing Security**

These sub-clauses of the Agreement ensure that Contractor Personnel are suitably vetted and trained in compliance with the provisions of the Security Policy and Security Plan detailed in schedule 2.5 (Security Requirements and Plan).

### **Clause 40 Authority Data**

This clause contains obligations on the Contractor as to how it should deal with Authority Data, which is essentially defined under the Agreement as data supplied to the Contractor by the Authority or Personal Data under the Data Protection Act 1998 where the Authority is the Data Controller.

### **Clause 41 Protection of Personal Data**

---

<sup>1</sup> Please note that all references to clauses and schedules are unless otherwise provided references to the OGC Model ICT Services Agreement V2.2 (“Agreement”) and all defined terms used in this note are detailed in Schedule 1 (Definitions) of this Agreement.

This clause sets out provisions from data protection legislation that any procuring Authority (or its contractors) is required to meet in relation to the management of Personal Data e.g. regarding the processing, data integrity management, security, consent and data subject access requests. Any changes therefore should be treated with caution and not made without taking advice from specialist data protection advisers or lawyers.

It will be important to double check whether or not when procuring a service that a Contractor can meet the level of security required under this clause. The details of the security requirements should be transparent and form part of the detail in schedule 2.1 (Service Description) (or equivalent). The Authority must assure itself that the bidders are capable of providing the level of security that is appropriate to the nature and use of the data in any given situation.

Additional provisions may need to be added to clause 41 where Authority Data / Personal Data will be transferred to any country or territory outside the European Economic Area (“EEA”) as part of the Contractor Solution. Where this is likely to happen further guidance should be sourced from your departmental SIRO on any relevant HMG or departmental data transfer/off-shoring policies.

## **Clause 42 Freedom of Information**

This clause is necessary to ensure the Authority's compliance with the Freedom of Information Act 2000 (“FOIA”). There are several points to note:

This clause is intended to cover all information related to the Agreement emanating from the Contractor and information provided to the Contractor from the Authority.

Depending on the precise nature of the services and the information being exchanged and generated during the term of the Agreement, it may be necessary to ensure that the clause remains in force after the expiry of the Contract. This is usually achieved by a survivorship clause.

Additional auditing and document management provisions may be required to ensure compliance - see clause 24 Audits for further guidance on this subject.

For these reasons a procuring Authority should obtain specific advice regarding the application of the FOIA, and the Environmental Information Regulations, to the Agreement and the specific project.

The primary responsibility for responding to FOIA requests, and the costs of discharging those responsibilities, rests with the Authority. However, it may on occasion be necessary for the Authority to seek support from the Contractor in complying with these obligations (e.g. where the Contractor holds the relevant data). These costs to the Contractor will, in the considerable majority of projects, not be substantial and should be subsumed within the ongoing

service management overhead. However, in exceptional circumstances, under certain conditions, the services being procured could become the subject of public interest and hence generate a disproportionately high number of FOIA requests. If the Authority believes such a situation could occur, an additional clause should be inserted to establish a mechanism requiring the Contractor to monitor effort expended in servicing FOIA requests, which should be reviewed by the Parties on a regular basis as part of routine contract management procedures. This mechanism should provide visibility to the Authority to assist fulfilment of its responsibility for responding to FOIA requests, and also allow for the Contractor to be paid reasonable additional costs where the volume of FOIA requests exceeds an agreed threshold over a period (e.g. one year). It would be expected that any such threshold would be at least an order of magnitude greater than the expected “normal” level of FOIA requests.

When reviewing the drafting of clause 42 procuring Authorities should also consider the interplay with schedule 4.2 (Commercially Sensitive Information) and the relevant defined terms. Careful consideration of these issues will assist an Authority in respect of compliance with FOIA

### **Clause 43 Confidentiality**

This clause contains standard confidentiality provisions restricting the use that can be made by the Contractor of the Authority’s Confidential Information and vice versa. Critically, in relation to the practical application of this clause an Authority will need to consider the scope of the relevant defined terms referenced in this clause (see schedule 1 (Definitions)) such as Confidential Information, Authority’s Confidential Information and Contractor Confidential Information.

An Authority should note that the requirement for direct confidentiality undertakings from specified Contractor Personnel at sub-clause 43.5 may not always be appropriate and should be used only where this is strictly necessary. Employees of the Contractor should be under an obligation of confidence to the Contractor and Sub-contractors, advisors, etc, should be retained under contracts imposing a like obligation. Please also note that the Supply Chain Rights in clause 23 requires the Contractor to impose conditions into its Sub-contracts and where appropriate an Authority might consider imposing similar obligations of confidentiality.

### **Clause 48 Security Requirements**

This clause prescribes that the Contractor and the Contractor Personnel comply with the provisions of the Security Policy and Security Plan. Schedule 2.5 (Security Requirements and Plan) of the Agreement provides for the creation of the Security Plan. This should be based on the project’s security requirements and any relevant Departmental security policies. A procuring Authority should ensure that it does not draft the Security Policy and Security Plan to be annexed to Schedule 2.5 (Security Requirements and Plan) in a way which constrains the output specification of the services to be procured.

Clause 48 also includes obligations on the Contractor to mitigate the impact of an attack from malicious software may have on the ICT Environment and any loss or corruption this may cause to Authority Data.

### **Clause 45.2 Warranties**

This clause provides for the Contractor to warrant that during the term of the Agreement all personnel used to provide the services will be vetted in accordance with Good Industry Practice, the Security Policy and the Standards as defined by the Agreement. Where security is of paramount concern it may be necessary for the procuring Authority to stipulate detailed requirements regarding staffing vetting which can be included within the Security Policy annexed to schedule 2.5.

### **Schedule 2.5 – Security Requirements and Plan**

The purpose of this schedule is to specify the principles of security to be applied in providing the Services by the Contractor and to set out the key elements of the procedure for further developing security plans for the Services.

A procuring authority needs to ensure that this schedule sets out the security principles and its security requirements in respect of the Services it would like the Contractor to deliver and that it clearly delineates between the obligations on the Authority and the specific responsibilities of the Contractor. The schedule should be drafted to conform with departmental security policies and to appropriate technical input.

An Authority should specify within this schedule its requirements for physically protecting servers, data backups, access rights and staff security clearances. The Authority should also describe its requirements for securing data, password controls, user permissions, network protection, virus, software patches and firewalls. Compliance with the Manual of Protective Security and relevant ISO security standards currently ISO/IEC 27002 and ISO/IEC27001 and any other additional security measures, not catered for by these standards should also be covered in this schedule.

The Authority should detail in this schedule a clear process for agreeing the security plan and its implementation as well as the testing and auditing of the security requirements. More importantly, this schedule should set out the measures the parties should take in the event of a security breach.

### **Related Clauses and Schedules to Consider**

In addition to the above mandated clauses and schedules OGC would recommend that all procuring authorities review and consider the security aspects of the following provisions.

Clause 12 Standards

Clause 13 Quality Assurance and Performance Monitoring

Clause 24 Audits

Clause 49 Business Continuity and Disaster Recovery

Schedule 1 Definitions

Schedule 2.3 Standards

Schedule 4.2 Commercially Sensitive Information

Schedule 8.5 Exit Management

Schedule 8.6 Business Continuity and Disaster Recovery Provisions

### **3. Frequently Asked Questions**

#### **Question:**

**What if my contract is not an ICT services one? Will the above requirements still apply?**

#### **Answer:**

Yes, if data handling or security is an issue, you should be using the model clauses and provisions as appropriate, as described in this note. You should consult your own SIRO, and, or legal advisers if in doubt, (or alternatively the Partnerships UK helpdesk/OGC).

#### **Question:**

**What if I think a clause or provision is not relevant to my contract?**

#### **Answer:**

You should ask your department's SIRO for advice.

#### **Question:**

**What should I do about existing contracts?**

#### **Answer:**

Whilst these mandatory provisions do not apply to procurements/contracts which

- i) were signed prior to 1 July 2008, or;

- ii) where the ITT/ITP for the relevant procurement was issued prior to 1 July 2008

you are strongly encouraged to review such procurement/contracts, taking advice from the SIRO. Procuring authorities need to assure themselves that where data handling/security is relevant or an issue, adequate and sufficient security requirements and provisions have been incorporated in to those agreements so that personal information is protected, and that the procuring authority's security policy is complied with. It may be necessary to consider variations to contractual agreements, where this is practically possible, taking on board the OGC model clauses. Any decisions related to incorporation of contractual variations should be made in the context of the aim of any such changes and securing best value for money for the taxpayer.

It is recommended that as a minimum, you alert contractors to the new standards, so that they are clearly sighted on what Government's expectations will be in this area when existing contracts are recompleted.