SCHEDULE 23

STANDARDS AND POLICIES

(Clause 9)

This page is left intentionally blank

SCHEDULE 23

STANDARDS AND POLICIES

1. GENERAL

1.1 In addition to any standards stated elsewhere in this Agreement the CONTRACTOR shall as a minimum meet the current AUTHORITY service and information technology standards detailed in this Schedule including any changes thereto which occur during the life time of this Agreement and be subject to the Change Control Procedures as modified by Clause 8.5.7.

1.2 The standards shall include but not be limited to:

1.2.1 The Civil Service Code; and

1.2.2 Department for Work and Pensions (DWP) Welsh Language Scheme.

2. INFORMATION TECHNOLOGY

2.1 The CONTRACTOR shall at all times comply (and shall ensure each of the CONTRACTOR's personnel shall comply) with all of the mandatory statements and policies detailed below:

2.1.1 DWP IT Accessibility Standards;

2.1.2 DWP Sustainable Development Policy;

2.1.3 ISO9000 (or as an alternative, the CONTRACTOR must operate to equivalent standards/requirements);

2.1.4 IT Continuity Policy;

2.1.5 ISSS (in accordance with the provisions of Schedule B9 (Security Requirements));

2.1.6 Prince 2 (or an alternative, the CONTRACTOR must adopt equivalent procedures/processes);

2.1.7 ITIL set (to the extent that any such document is applicable having regard to the Services to be provided by the CONTRACTOR);

2.1.8 BS15000 (or as an alternative the CONTRACTOR must operate to equivalent standards/requirements);

2.1.9 Strategic Supply Charter; and

2.1.10 OGC Sponsored Intellect Code of Best Practice.

2.1.11 DWP Incident Management Response Times

2.2 In addition, the CONTRACTOR should be aware of the following policies, standards and working practices. Compliance with these is not mandatory but a working knowledge of them is necessary to enable a thorough understanding of the environment in which the CONTRACTOR will be required to operate:

2.2.1 DTSS Service Charter;

2.2.2 DWP Enterprise Architecture – levels 0 and 1;

2.2.3 DWP Multi-collaborative Model (MSM);

2.2.4 Renaissance Round Table Terms of Reference;

2.2.5 Renaissance Steering Group Terms of Reference;

2.2.6 Renaissance Operating Model; and

2.2.7 Renaissance Key Messages.

2.3 The CONTRACTOR shall comply with the terms and conditions of all licences for the AUTHORITY Software and AUTHORITY Third Party Software which they choose to licence from the AUTHORITY.

2.4 Any CONTRACTOR IT system which connects to and uses core AUTHORITY Data, including current DWP operational strategy systems shall interface with those DWP systems using the required interfaces, protocols, DWP data/file formatting standards, approved data access controls, any specific software, hardware or infrastructure components mandated by the AUTHORITY for the particular DWP system and must comply with all corresponding security and audit facilities.

2.5 Where the IT system of the CONTRACTOR used in the performance of the Services has, or will have, some interface or interchange of information with an existing IS/IT system of the AUTHORITY or one of its suppliers, the CONTRACTOR shall ensure conformance, within the CONTRACTOR IS/IT systems, to all applicable interface standards, without cost or inconvenience to the owners or operators of the targeted IS/IT system(s).

2.6 If services similar to the Services are provided to the AUTHORITY by more than one supplier, the CONTRACTOR shall co-operate with the other suppliers of the AUTHORITY to enable its supporting IS/IT system to interchange any data or information held therein such that the receiving IT system can incorporate the information in a useable fashion.

2.7 Any CONTRACTOR system which uses electronic information shared or exchanged with other AUTHORITY business units shall comply with shared data definitions agreed with the AUTHORITY.

2.8 The CONTRACTOR must ensure that any systems which transmit data to any databases containing AUTHORITY Data do so in accordance with rules governing data verification, which will be specified by the AUTHORITY following any CONTRACTOR proposal to connect to such a database. Data updates shall be applied by the CONTRACTOR using authentication and access controls, with event logging and an audit trail service, in accordance with the Security Policy detailed in Schedule 20.

2.9 Hardware and software employed by the CONTRACTOR in the provision of the Services shall have sufficient performance and capacity to provide for any foreseeable increase in business volumes.

2.10 Software used by the CONTRACTOR in the provision of the Services shall, wherever it is suitable and available, be commercial off-the shelf software adhering to de facto industry standards and having some or all of the attributes listed in the appropriate AUTHORITY guidance such as DITIS.

2.11 The CONTRACTOR, and any Subcontractors or other representative engaged by the

CONTRACTOR, shall keep computerised records and data about all access attempts, successful or otherwise, relating to Claimants and IT based processes (including processes which introduce and authenticate users of the IT) performed in connection with the Services. Electronic data security functions shall be auditable for their correct operation in terms of AUTHORITY Data creation, change, access, storage, transmission and print.

2.12 Any IT systems management tools employed by the CONTRACTOR shall be capable of an upgrade which will provide remote access management functions for an operator, acting on behalf of the AUTHORITY to perform tasks in connection with MIS, security and audit for CONTRACTOR systems.

2.13 Any IT-based payment authorisation or issue process operated by the CONTRACTOR on behalf of the AUTHORITY shall be subject to a suitable audit service, as defined by the AUTHORITY.

2.14 The CONTRACTOR shall comply with all AUTORITY IS/IT policy and strategic requirements when using IS/IT systems to perform AUTHORITY business and to handle AUTHORITY Data, including those arising from:

2.14.1 legal obligations such as the Data Protection Act and EU Data Protection Directive (due 24/10/98); Police and Criminal Evidence Act (PACE); the Civil Evidence Act; and Health and Safety at Work legislation;

2.14.2 AUTHORITY operational management functions, eg the provision of required security and audit procedures;

2.14.3 constraints from existing AUTHORITY contracts which dictate the use of certain IT-related services for some aspects of AUTHORITY business;

2.14.4 AUTHORITY change programme constraints which dictate the use of certain IT for some aspects of AUTHORITY business; and

2.14.5 EC rules which dictate that government projects should be re-completed obliging the AUTHORITY to ensure that a disparate or uncontrolled IT provision does not make the business unattractive to an incoming front line provider where the equipment and software are handed over.

2.15 The CONTRACTOR shall confirm that evidence based protocols that underpin the production of electronic reports are updated on a regular basis as agreed with the AUTHORITY. The protocols shall be reviewed and updated as necessary at least once every three (3) years.

2.16 The CONTRACTOR shall confirm that where required they will develop and deliver new protocols.

2.17 Any new IT introduced by the CONTRACTOR shall be the CONTRACTOR's responsibility in terms of specification, design, procurement, installation, support and maintenance. IT products, services and builds shall nevertheless conform to the IS/IT standards required by the AUTHORITY, including standards in respect of:

2.17.1 business data;

2.17.2 security and access control;

2.17.3 audit-ability;

2.17.4 inter-operability with AUTHORITY or other CONTRACTOR systems; and

2.17.5 strategic direction within the AUTHORITY.

2.18 Any IS/IT-based solutions proposed by the CONTRACTOR following the award of business shall be subject to review and agreement by the AUTHORITY before their adoption, to ensure conformance to relevant standards, and interfaces within the AUTHORITY's corporate and Agency IS/IT strategies.

2.19 Any AUTHORITY's Data created and kept by CONTRACTOR IT systems on behalf of the AUTHORITY shall be handled in conformance with the relevant provisions of the Data Protection Act. In addition, and subject to Clause 9.5.2 the CONTRACTOR must conform to any requirements of the AUTHORITY's Data Protection Unit in respect of DWP business data and to any relevant requirements of the coming EC Directive on Electronic Data Handling.

2.20 Any electronic documents created by CONTRACTOR IT system which contain AUTHORITY's Data or information which may be used in legal proceedings of any kind shall be treated in accordance with the British Standards Institute (BSI) Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP 0008).

2.21 Medical services information provided by the CONTRACTOR in electronic format for the public domain shall conform to the relevant AUTHORITY house-style for the media used. Information about medical services which is published on the Internet or any other public network shall be cross referenced to other relevant AUTHORITY information sites, by arrangement with the AUTHORITY acting on behalf of DWP Information Branch.

2.22 Software applications used by the CONTRACTOR to create data structures, including databases, documents and other formatted electronic files, shall ensure that these applications meet certain de jure or de facto standard formats which shall be specified by the AUTHORITY.

2.23 The CONTRACTOR shall be responsible for ensuring compliance with the standards, regulations and legislative requirements set out in this Schedule 23 (including, but not limited to, those set out in Paragraphs 2.24 to 2.37 below) or the equivalent standards of other EC member states together with any other standards, regulations and legislative requirements from time to time in force.

2.24 Safety of information technology equipment including electrical business equipment:

2.24.1 BS EN 60950;

2.24.2 IEC 60950; and

2.24.3 BS 7002.

2.25 UK Provision and Use of Work Equipment Regulations, 1998 (Health and Safety Executive).

2.26 Safety of DP equipment:

2.26.1 IEC 60435.

2.27 Safety of electrical energised office machines:

2.27.1 IEC 60380.

2.28 Safety of domestic mains powered electrical equipment:

2.28.1 BS 415; and

2.28.2 BS EN 60065.

2.29 Safety of apparatus for connection to BT Networks:

2.29.1 EN 41003.

2.30 Radiation and safety of laser products and systems:

2.30.1 BS EN 60825; and

2.30.2 PD IEC 60825.

2.31 UK Workplace (Health, Safety and Welfare) Regulations 1992.

2.32 Measurement of Airborne Noise:

2.32.1 BS EN ISO 7779.

2.33 Measurement of High Frequency Noise:

2.33.1 BS 7135-2;

2.33.2 EN 29295; and

2.33.3 ISO 9295.

2.34 Electrical Interference:

2.34.1 BS EN 55014;

2.34.2 CISPR 14;

2.34.3 BS EN 55022; and

2.34.4 CISPR 22.

2.35 Electromagnetic Compatibility:

2.35.1 BS EN 60801-2;

2.35.2 BS EN 61000-4-1;

2.35.3 BS EN 61000-4-3;

2.35.4 BS EN 61000-6-1;

2.35.5 BS EN 61000-6-3;

2.35.6 EC Directive 89/336/EEC; and

2.35.7 EC Directive 92/31/EEC.

2.36 Ergonomics:

2.36.1 BS EN 29241; and

2.36.2 EC Directive 90/270/EEC.

2.37 All applicable EC and UK Legislation on the use of VDUs and display screens including:

2.37.1 The UK Health and Safety (Display Screen Equipment) Regulations 1992; and

2.37.2 BS EN 29241 - European Standard on ergonomic requirements for office with

visual Display Terminals.