Crown Hosting Framework Agreement

Schedule 3.5

Standards

1. Introduction

1.1 This Schedule sets out the Standards that the Supplier shall comply and/or be Certified with in the provision of the Services and the process which shall determine the date from which the Supplier shall comply with and/or be certified as compliant with the requirements of each of the Standards.

1.2 The Industry Standards are set out in Annex 1 (Industry Standards) to this Schedule.

1.3 The Public Sector Standards which are applicable to this Framework Agreement and each Call-Off Agreement are set out in Annex 2 (Public Sector Standards) to this Schedule.

1.4 The Public Sector Standards which are specific to a Call-Off Agreement shall be set out in the Call-Off Order Form for the relevant Call-Off Agreement.

1.5 The Supplier shall ensure that its Key Sub-contractors comply and/or are Certified with those Standards which are applicable to the scope of the sub-contracted services.

2. Standards Compliance Exercise

2.1 As at the Framework Effective Date the Supplier shall ensure that it, its Key Sub-contractors and/or the Services (as appropriate) meet the requirements of each of the following Standards:

(a) ISO 9001:2008 (or later); and

(b) ISO 27001: 2013.

2.2 The Supplier shall, within sixty (60) Working Days of the Framework Effective Date, deliver a written report to the Framework Authority which states:

(a) whether or not the Supplier, its Key Sub-contractors and/or the Services meet the requirements of each of the Standards as applicable (**"Compliant"**);

(b) where the Supplier, its Key Sub-contractors and/or the Services are Compliant with a Standard, whether or not a third party certification body (which is independent of the Supplier and which is recognised by the UK Accreditation Service or an international equivalent also recognised by the UK Accreditation Service) has provided certification that the Supplier, its Key Sub-contractors and/or the Services are Compliant with the requirements of that Standard ("**Certification**" or "**Certified**"); and

(i) where the Supplier, its Key Sub-contractors and/or the Services are not Compliant with a Standard: the reasons why the Supplier, its Key Sub-contractors and/or the Services are not Compliant;

(ii) the remedial measures needed to be implemented to enable the Supplier, its Key Sub-contractors and/or the Services to become Compliant; and

(c) the date by which the Supplier, its Key Sub-contractors and/or the Services shall be Compliant which shall be no later than the date on which the Supplier first commences provision of the Data Centre Co-Location Services to a Customer,

(the **"Standards Compliance Report"**), and the Supplier shall provide the Framework Authority with such additional information as it may reasonably request to enable it to decide, acting reasonably, whether or not to accept the Standards Compliance Report.

2.3 Within fifteen (15) days of receipt of the Standards Compliance Report and all additional information required by paragraph 2.1, the Framework Authority shall notify the Supplier whether or not it agrees with the Standards Compliance Report.

2.4 The Parties agree that the Supplier shall not be in breach of its obligation to be compliant with a particular Standard until the relevant date set out in the agreed Standards Compliance Report.

3. Certification Requirements

3.1 Where the Supplier identifies in the Standards Compliance Report that the Supplier, the Services and/or a Key Sub-contractor (as applicable) are Certified, the Supplier shall maintain and shall use reasonable endeavours to ensure that any relevant Key Sub-contractor maintains such Certification for the duration of the Framework Agreement.

3.2 In respect of each Standard where Certification is possible, if the Standards Compliance Report agreed with the Framework Authority pursuant to paragraph 2.2 above identifies that the Supplier, the Services and/or Key Sub-contractor (as applicable) are not Certified as Compliant with such Standard or Standards, the Supplier shall, and shall procure that any relevant Key Sub-Contractor shall, obtain Certification for each such Standard by the date on which the Supplier first commences provision of the Data Centre Co-Location Services unless otherwise agreed in writing between the Parties.

3.3 The Parties agree that the Supplier shall not be in breach of its obligation to obtain Certification for compliance with a particular Standard until the relevant date set out in the agreed Standards Compliance Report.

4. Audit

4.1 Where this Framework Agreement requires:

(a) Compliance with a Standard, the Supplier shall, within each Report produced pursuant to Clause 11 (Financial Reports, Records, Audit and Open Book Data), demonstrate that the Supplier, the Services and/or Key Sub-Contractor (as applicable) is Compliant with that Standard; and

(b) Certification of Compliance with a Standard, the Supplier shall, within each Report produced pursuant to Clause 11 (Financial Reports, Records, Audit and Open Book Data), demonstrate that the Supplier, Services and/or the Key Sub-Contractor is Certified as meeting the requirements of that Standard.

Annex 1

Industry Standards

Standard	
General Standards	
• ISO 9001:2008 (or later) Quality Management Standard • Tier III Uptime Institute compliant system and architecture (or equivalent) such Standard to apply to all elements of the Services	
Security Standards (ICT and Data Security)	
• The facilities housing and services supporting the data centre must be fully within the Information Security Management System (ISMS) regime of a conformant ISO 27001 and audited annually to confirm compliance. • To ensure that the security controls and procedures implemented are proportionate to the risk, the Supplier will undertake an Operational Requirements Review (ORR) at both levels 1 and 2 in accordance with Centre for the Protection of National Infrastructure (CPNI) guidance. • ISO/IEC 27002:2013 Information Security Management • Security screening of individuals employed in a security environment. Code of practice - BS7858:2012	
Environmental Standards	
• ISO 14001 Environmental Standard and the Carbon Trust Standard • European Union Code of Conduct for Data Centres • Waste Electrical and Electronic Equipment (WEEE) Directive 2012/19/EU • Thermal guidelines for data processing environments 2012 ASHRAE • ISO 14664 Cleanrooms and associated controlled environments	
ICT Standards	
Uninterrupted Power Supply (UPS)	EN/IEC 62040 (Parts 1,2 and 3)
Perimeter Physical Security	• Fences (or walls built in lieu of a fence) must conform to BS 1722
Secure Access & Entry Systems	• Entry doors and fire exit doors to data halls must be certified to LPS 1175 SR3 and exit devices must be certified to BS EN 179 or BS EN 1125.
Intruder Detection & Alarm Systems	• Sites must be protected by IDS which is compliant with BS EN 50131-1, Grade 3, and must be compliant with the ACPO Policy for Security Systems. Only alarm systems meeting these requirements will qualify for the issue of a Unique Reference Number (URN) and police response. Systems installed after June 2012 must conform to PD 6662:2010 and BS 8243.

	• Static guards, mobile patrols and key-holding services must comply with BS 7499.
Fire Suppression Systems (Smoke & Heat Detection & Alert)	• Dry sprinkler fire detection system to meet BS 5306, 3115 • Fully addressable two stage fire detection system • Detectors to meet BS5839, 6266, 5445 and 5588 • Data halls must have appropriate detection systems for fire, smoke, water leaks/flooding and, where necessary, for asphyxiating or explosive gases. Fire detection and suppression systems must be compliant with the following Standards and Codes of Conduct: EN 15004; EN 54-20; BS 6226; BS 7273; BS 5839 and BS5306.
External Perimeter Access Control	• Anti-ram protections must conform to the appropriate mass/speed/penetration rating of BSI PAS 68. Guidance on the operation and deployment is in BSI PAS 69.
Facilities Service Continuity Planning	• ISO 27001 • ISO 9001
Disaster Recovery Planning & Service Provision	• ISO/IEC 24762 • ISO22301 • ISO/IEC 27002:2013 and 27031
Employee & Contractor Security Clearance	All security officers must be screened to BS 7858.
General	• BS EN 50174-3:2003 Installation technology cabling installation – Part 3 Installation planning and practices outside buildings • BS EN 50174-2:2009 Information Technology Cabling Installation – Part 2 Installation planning and practices inside buildings • BS EN 5017-1:2009 Information technology. Cabling installation. Installation specification and quality assurance • BS EN 50600-2-2:2014 Information technology. Data centre facilities and infrastructures. Part 2 Power distribution • IEE Wiring Regulations 17th Edition BS 7671:2008

Annex 2

Public Sector Standards

Standard
Security Standards (ICT and Data Security)
HMG Security Policy Framework 2014
HMG IS1 and IS2 – Supplement – Technical Risk Assessment and Risk Treatment
HMG IS1 and IS2 - Information Risk Assessment
HMG Security Classifications Issue 1, 2014
CESG Supplier IA Assessment Framework Issue 1.0 January 2011
HMG Baseline Personnel Security Standard – v3.1- April 2013
ICT Standards
Information stored on any form of equipment or device must be systematically erased to comply with HMG Infosec Standard 5
Published Government Technology Strategies, Standards and Policies Technology Code of Practice
The Government Digital Service Manual
PSN Code of Connection (including CSP Compliance) HMG IA/IS7- Authentication
HMG Baseline Personnel Security Standard