DEFENCE AS A PLATFORM
SIP FINAL SCHEDULE 5
AUTHORITY STANDARDS

Table of Contents

SCHEDULE 5
AUTHORITY STANDARDS

Capitalised terms used but not defined in this Schedule are defined in Clause 1.1 (*Definitions and Interpretation*).

1. AUTHORITY STANDARDS

1.1 The Authority Standards comprise of:

1.1.1 the policy standards referred to in Paragraph 3 below;

1.1.2 the process standards referred to in Paragraph 4 below;

1.1.3 the information assurance and cyber security standards referred to in Paragraph 5 below;

1.1.4 the environmental standards referred to in Paragraph 6 below; and

1.1.5 the accessibility standards referred to in Paragraph 7 below.

1.2 The Parties acknowledge and agree that the Contractor's performance of its obligations under this Agreement in no way depend on the Authority's performance or omission of any act contemplated by the Authority Standards.

2. CHANGES TO STANDARDS

2.1 The Authority Standards may be amended or updated from time to time and the Contractor shall comply with such amendment.

3. POLICY STANDARDS

3.1 When performing its project management obligations (including in relation to implementation), the Contractor shall make use of APMP/PRINCE2 methodology (or such equivalent methodology as required by the Authority), supplemented where appropriate by the tools and method of the Contractor's own project management methodologies.

3.2 The Contractor shall comply with the following documented policy Authority Standards:

Standard
Government Classification Scheme (GCS) Version 1.0, date April 2014
Security Policy Framework (SPF), dated April 2014 and supporting documentation
DEFCON 659a Security Measures, Version February 2017

4. PROCESS STANDARDS

4.1 The Contractor shall comply with the following ISS TSCM Model Processes (including all of the obligations, interfaces, activity and inputs shown in the ISS TSCM Processes as being carried out by the entity referred to as the "**MSP**"):

Process
ISS Ways of Working Process Set - Service/Function Definition and Operating Model, Change Management Process, Version 9.0, flowchart 9.0
ISS Ways of Working Process Set - Service/Function Definition and Operating Model, Evaluation Process, Version 9.0

ISS Ways of Working Process Set - Service/Function Definition and Operating Model, Service Validation and Testing Process, Version 9.0
ISS Ways of Working Process Set - Service/Function Definition and Operating Model, Transition Planning & Support Process, Version 9.0, flowchart 9.0
ISS Service Management Framework, Version 3.2

5. INFORMATION ASSURANCE AND CYBER SECURITY STANDARDS

5.1 The Contractor shall comply with the following information assurance and cyber security Authority Standards:

Standard
ISO/IEC 27002:2013 - Information security management, Version 1.0, date October 2013
ISO/IEC 27001:2013 Information Technology - Security Techniques - Information security management systems - Requirements, date October 2013
Defence Cyber Protection Partnership (DCPP) Cyber Security Model (CSM), date March 2017
DEFENCE STANDARD 05-138 - Cyber Security for Defence Suppliers, Version 2.0, date 28 September 2017
NCSC 14 – Cloud Security Principles, Implementing the Cloud Security Principles, date September 2016
Information Security Note (ISN) MOD ICT Security Accreditation and The Defence Assurance Risk Tool (DART), date January 2017
Information Security Note (ISN)– Requirement to report security incidents affecting the Authority material to the Authority, date February 2014

6. ENVIRONMENTAL STANDARDS

6.1 The Contractor shall comply with the following environmental Authority Standards:

Standard
ISO 14001 – Environmental management, date 2015
EU Code of Conduct on Data Centres' Energy Efficiency
Greening Government - IT Strategy contained in the document "Greening Government: ICT Strategy", date March 2011
Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU
Sustainable MOD Strategy- Waste Management (2015-2025), date 19 February 2016
Sustainable Procurement - the GBS for office ICT equipment, Statutory Guidance, date 2 January 2012
Where the Sustainable Procurement guidance described above does not apply, the Contractor shall instead ensure that any Equipment used in the provision of the Services complies with the following (in order of priority): 1. applicable EU Green Public Procurement Criteria developed by the European

Standard
Commission 2. ECMA or equivalent Energy Star accreditation or EPEAT equivalent accreditation
DEFSTAN 00-51 – Environmental Management Requirements for Defence Systems

6.2 The Contractor shall be required to comply with ISO 140001 up to but not including the date on which DEFSTAN 00-51 comes into effect, in which case the Contractor shall no longer be required to comply with ISO 140001 and shall instead be required to comply with DEFSTAN 00-51.

7. ACCESSIBILITY STANDARDS

7.1 The Contractor shall comply with the following accessibility Authority Standards:

Standard
ISO/IEC 13066-1 - Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability, date 2011
In respect of End User-facing Services, the UK Government Accessibility standards set out in the Gov.uk Service Manual (https://www.gov.uk/service-manual/helping-people-to-use-your-service/making-your-service-accessible-an-introduction)