This document has been redacted to remove any commercially sensitive information and is now classified as DCC Public.

Should you have any queries, please contact Commercial@SmartDCC.co.uk

SCHEDULE 6

STANDARDS

1. **PURPOSE**

1.1 This Schedule 6 details certain Standards with which the Contractor is required to comply in delivering the Services under this Agreement.

1.2 This Schedule 6 is without prejudice to the Contractor's other obligations under this Agreement, including any requirement to comply with other Standards referred to elsewhere in this Agreement.

1.3 For the avoidance of doubt, references to Standards in this Agreement refer to the latest version of such Standards, as updated from time to time in accordance with Clause 29 *(Change in Mandatory Requirements)*.

2. **STANDARDS**

2.1 Without prejudice to any other provisions of this Agreement, the Contractor (and the Contractor Solution) shall comply with the Standards referred to in this Schedule 6 throughout the Term.

ITIL standards

2.2 Standards contained in the Office of Government Commerce's IT Infrastructure Library ("**ITIL**").

Technical standards

2.3 Technical standards, including:

No.	Standard
1.	Open and accessibility standards, wherever possible, following www.w3.org guidelines for web services
2.	Java Coding Standard

2.4 **Security standards**

Security standards, including:

No.	Standard
ISO/BS Standards	
1.	ISO/IEC 27001:2005 (Information technology — Security techniques — Information security management systems — Requirements)
2.	ISO/IEC 27002:2005 (Security techniques – Code of practice for information security management)

3.	ISO/IEC 27005:2011 (Information technology – Security techniques – Information security risk management)
4.	ISO/IEC 27033 (Information technology – Security techniques – Network security)
5.	ISO/IEC 27035:2011 (Information technology – Security techniques – Information security incident management)
6.	ISO/IEC 22301:2012 (Societal security – Business continuity management systems – Requirements)
7.	ISO/IEC 27031:2011 (Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity)
8.	BSI BS 10008 (Evidential weight and legal admissibility of electronic information)
9.	DISC PD 0008 (Code of practice for legal admissibility and evidential weight of information stored electronically)
10.	BS 7858 – Security Screening
HMG/CESG Standards	
11.	HMG Information Assurance Standard No.4 (Management of Cryptographic Systems)
12.	HMG Information Assurance Standard No. 5 (Secure Sanitisation of Protectively Marked or Sensitive Information)
13.	HMG Information Assurance Standard No. 6 (Protecting Personal Data and Managing Information Risk)
14.	HMG Security Procedures – Telecommunications Systems and Services
15.	HMG Security Policy Framework
16.	HMG Baseline Personnel Security Standard (BPSS)
17.	Compliance with latest National Cyber Security Centre Guidance.
Other Standards	
18.	RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework)
19.	Any requirements or advice of the Centre for Protection of National Infrastructure regarding Critical National Infrastructure (CNI) category as notified to the Contractor from time to time by the DCC

2.5 Quality and service management standards

Quality and service management standards, including:

No.	Standard
1.	"Managing Successful Programmes" (the HMG-approved programme management methodology)
2.	ISO 9001:2000 (Quality management systems – Requirements)
3.	TickITplus
4.	ISO/IEC 20000 (Standard for IT service management)

2.6 Business continuity standards

Business continuity standards, including:

No.	Standard
1.	ISO/IEC 27031:2011 (Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity)
2.	ISO/IEC 22301:2012 (Societal security – Business continuity management systems – Requirements)
3.	BS 25999:2006 (Business Continuity Planning Standard)
4.	Business Continuity Institute (BCI) Good Practice Guidelines

2.7 Environmental standards

Environmental standards, including:

No.	Standard
1.	European Code of Conduct on Data Centres Energy Efficiency
2.	BS EN ISO 14001:2004 (Environmental management systems – Requirements)

2.8 Interface standards

Interface standards, including:

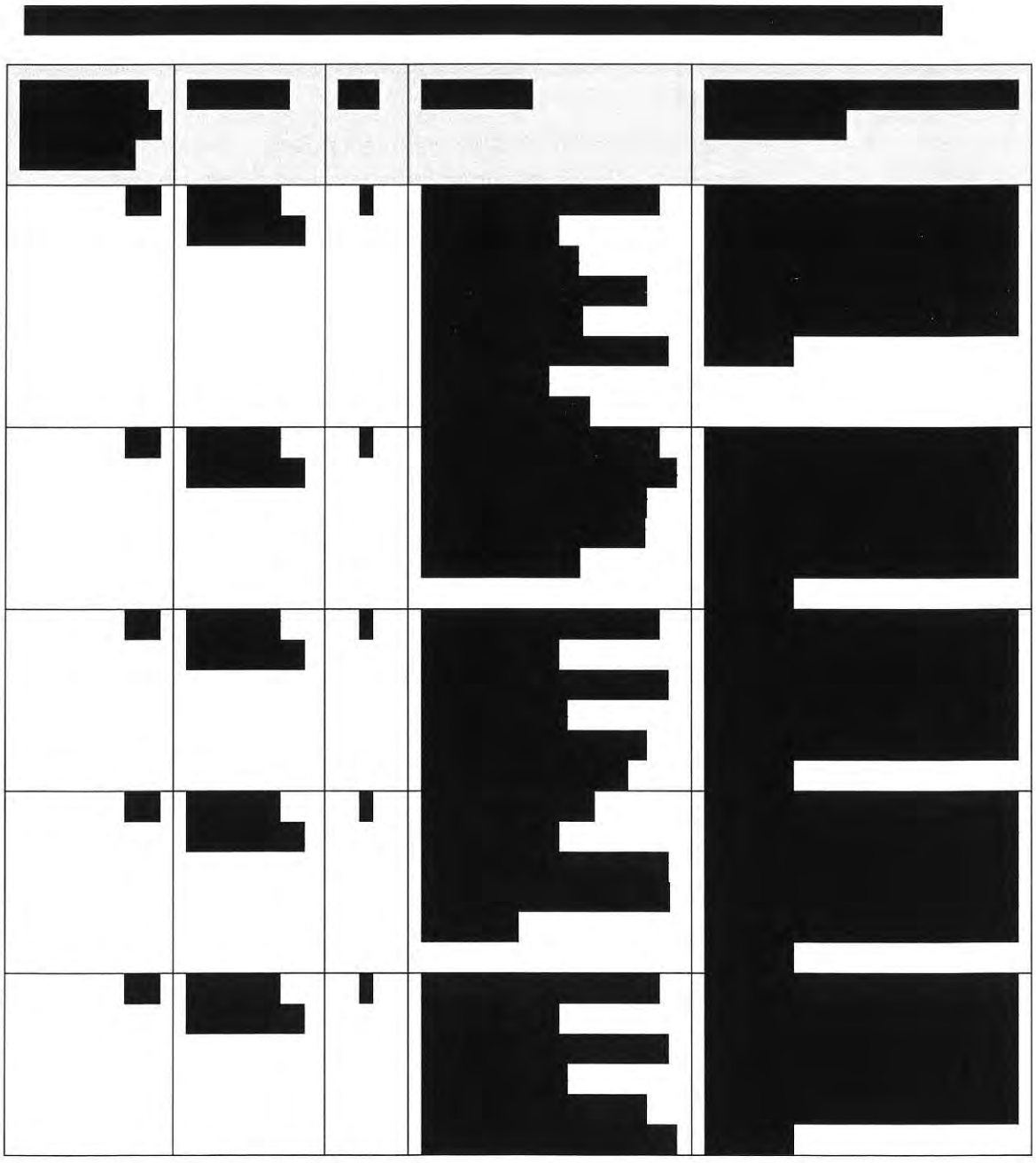
No.	Standard
1.	Web Content Accessibility Guidelines (WCAG) 2.0, W3C Recommendation 11 December 2008 (http://www.w3.org/TR/2008/REC-WCAG20-20081211)

2.9 **NOT USED**

2.10 **Health and safety standards**

Health and safety standards, including:

No.	Standard
1.	BS EN 60950-1:2006 Information Technology Equipment. Safety. General Requirements
2.	BS 7671:2008 IEE Wiring Regulations. Requirements for Electrical Installations



[1] Commercially Sensitive Information – Access by Other DCC Contractors Generally Prohibited

REDACTED
SMSO Development Agreement - Trilliant

[redacted]

[2] Commercially Sensitive Information – Access by Other DCC Contractors Generally Prohibited