# FUTURE SERVICE DELIVERY CONTRACT

## SCHEDULE 2.1 – SERVICE REQUIREMENTS

## PART 15 - TECHNOLOGY

**CONTENTS**


| Clause | Heading | Page |
|---|---|---|
| 1 | DEFINITIONS | 1 |
| 2 | INTRODUCTION | 3 |
| 3 | SERVICE CHANGE & SERVICE DESIGN | 3 |
| 4 | TECHNOLOGY ROADMAP | 5 |
| 5 | SERVICE OPERATION MANAGEMENT & SERVICE DESIGN | 6 |
| 6 | DBS DESIGN STANDARDS AND PRINCIPLES | 12 |
| 7 | INFORMATION TECHNOLOGY BACK-UP AND RESTORE | 12 |

## 1 DEFINITIONS

1.1 In this Part 15 of Schedule 2.1, the following definitions shall apply:

| | |
|---|---|
| **Anti-Virus Software** | any Software designed to prevent, search for, detect and remove software virus and other malicious software (including but not limited malware, adware and trojans); |
| **Application** | Software designed to perform a group of coordinated functions, tasks, or activities; |
| **Application Instance** | single or multiple instances of Software and Hardware to perform a group of coordinated functions, tasks, or activities which support delivery of a specific Service; |
| **Architecture Management Procedures** | those procedures as set out in in Part 13 of Schedule 2.1 (Service Requirements – IT Service Management); |
| **Authority Communications Infrastructure** | the 4 primary communications systems provided by the Authority, being:<br>(a) UK Fixed;<br>(b) Overseas Fixed;<br>(c) Land Deployed; and<br>(d) Maritime Deployed; |
| **Authority to Operate** | an approval granted by the 'Defence ICT Design Authority (DIDA)' Board, in accordance with JSP 604, to all Authority ICT systems that permits them to operate on the Authority's Networks; |
| **Back-Up Plan** | Describes the scope of all required backup activities, including all schedules, processes, procedures and standards that will be followed to ensure the Authority's requirements are satisfied; |
| **Capacity Management Report** | the reports as detailed in M1.20 of Annex M to Schedule 2.1 (Technical & Applications); |
| **Cloud** | has the meaning given to it in Paragraph 5.7 of Part 15 of Schedule 2.1; |
| **Data Centre** | a dedicated space used to house computer systems and associated components; |
| **DBS Mil Pers & Vets Design Standards & Principles** | the DBS Military Personnel & Veterans Design Standards & Principles, being design standards and principles; |
| **Engineering Change Request (ECR)** | change request forms, in the format provided by SCIDA; |
| **Environment** | describes the physical and logical construct, where a collection of application and technology components are instantiated to support the provision of the Service for either Production, Disaster Recovery or Development purposes; |
| **Evergreen** | the requirement that Software is always within one release of the current approved version (unless agreed with the Authority) with a clear upgrade or migration path identified, running on a sufficient and capable platform throughout the life of the Agreement and capable of supporting the provision of the Services in accordance with the requirements set out in the Agreement (albeit such services may be provided by a replacement supplier) for a minimum of 2 years after the expiry or termination of this Agreement; |
| **Hardware** | in the context of ICT, refers to the physical elements that make up a computer or electronic system and everything else involved that is physically tangible; |
| **Information Communications and Technology** | those technologies that provide access to information through telecommunications (including but not limited to the Hardware, the Software, and the Network); |

| | |
|---|---|
| **Mature IT Service Management** | the achievement of level-4 maturity, as detailed in Part 13 of Schedule 2.1 (Service Requirements - IT Service Management); |
| **Microservices** | a software development technique which is a variant of the Service-Oriented Architecture architectural style that structures an application as a collection of loosely coupled services; |
| **MoD Core Network** | a single communications infrastructure that provides the entire Defence community with a managed LAN to LAN service, at OFFICIAL-SENSITIVE level (e.g. network cables, switches, routers, etc.). For the avoidance of doubt, the legacy naming for MCN is Restricted LAN Interconnect (RLI);<br>Assured LAN Interconnect (ALI); and Official LAN Interconnect (OLI); |
| **MODCERTS** | a notification of security vulnerabilities issued by the Ministry of Defence Computer Emergency Response Team; |
| **MODNet** | the latest iteration of the Authority's End User accessed devices and networked systems with common provisioned Software tooling, which replaces DII and may be changed or updated from time to time; |
| **Network** | a digital telecommunications network which allows computer systems to share resources and communicate; |
| **Patch** | an Update to Software generated as required by the Contractor, Sub-Contractor or relevant Third-Party Software provider to rectify identified shortfalls in the delivered Software and may include fixes or workarounds; |
| **Production Environment** | the Technical Infrastructure (including all Hardware and Software) situated either permanently or temporarily at any of the Contractor Premises or at any Authority Premises and which Technical Infrastructure is used by the Contractor to operate the supported Applications in the delivery of the live services; |
| **Recovery Point Objectives** | the maximum targeted period in which data (transactions) might be lost from an IT service due to a major incident; |
| **Recovery Time Objectives** | the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity; |
| **Service Desk** | a form of Help Desk concerned with the primary discipline of IT service management (ITSM) as defined by the Information Technology Infrastructure Library (ITIL). It is intended to provide a single point of contact to meet the communication needs of both End Users and each Party's staff for business and technical matters; |
| **Service Transformation Strategy** | contained Appendix to Schedule 6.1 (Implementation Plan); |
| **Service-Oriented Architecture** | a style of system design where Services are provided to the other components by application components, through a communication protocol over a Network; |
| **Technical Infrastructure** | the physical components of the Technical Infrastructure (being the Hardware listed in the Configuration Management Database and the Software listed in Schedule 5 (Software) up to the SDP on the MoD Core Network which are required to provide connectivity in order to deliver the Services and which, for the avoidance of doubt, includes 'Agencynet'; |
| **Technical Refresh** | the process whereby items of the Technical Infrastructure are replaced whether by new or previously used items, upgraded or (with the Authority's prior written consent) reconditioned such that, following the replacement, upgrade or |

| | |
|---|---|
| | reconditioning, the item of Technical Infrastructure conforms to accepted industry standards of performance and functionality existing at that time; |
| **Technology Roadmap** | a set of documents and design artefacts that support the strategic and long-term planning of the technology solutions used to deliver the Services. It must provide a current state detailed view and assessment of all Technical Infrastructure, with an accurate record of the obsolescence dates, support level, upgrade path and vendor plans for all products and components; |
| **TEMPEST** | a standard for screening IT equipment to guard against electronic emissions divulging classified information; |
| **COBIT** | Control Objectives for Information Technology; |
| **HVAC** | heating, ventilation, and air conditioning; |
| **MCN** | MoD Core Network; |
| **TCO** | total cost of ownership; |
| **WAN** | Wide Area Network; |

## 2 INTRODUCTION

2.1 This Part 15 to Schedule 2.1 sets out the Authority's requirements, in relation to:

(a) Transition Services (including Transformation) for Technical Infrastructure;

(b) Technical Refresh to comply with Evergreen requirements;

(c) hosting, Hardware and Software obligations regarding licensing, technology management and configuration management;

(d) the DBS Mil Pers & Vets Design Standards and Principles; and

(e) technology back-up requirements.

2.2 The related Performance Levels are set out in Part 13 of Schedule 2.1 (Service Requirements – IT Service Management), Schedule 2.2 (Performance Levels), and Annex M (Technology and IT Services).

## 3 SERVICE CHANGE & SERVICE DESIGN

3.1 The Contractor understands that the Technical Infrastructure may be the subject of upgrade, renewal, or replacement during the Term to allow the Contractor to continue to deliver the Services and undertake Transformation. If the Authority requires the Contractor to make any other change to the Technical Infrastructure this shall be dealt with in accordance with the Change Control Procedure. This Paragraph sets out the:

(a) basis on which the Contractor may make changes to the Technical Infrastructure as Operational Changes;

(b) the Authority Requirements for Technical Refresh to maintain Evergreen state; and

(c) Transformation activities to support the Transformation Requirements set out in the Detailed Transformation Plan, contained in Schedule 6.1 (Transition and Transformation Plan).

3.2 The Contractor shall:

(a) only be entitled to make changes to the Technical Infrastructure in accordance with the agreed Architecture Management Procedures and the Change Control Procedure;

(b) when planning or implementing any changes to the Technical Infrastructure, work collaboratively with the Authority in accordance with:

(i) the Architecture Management Procedures and the Joint Architecture Governance framework; and

(ii) if necessary, the Change Control Procedures to ensure that plans relating to changes to the Technical Infrastructure are integrated and coherent with the overall change programme and plans;

(c) maintain the Technical Infrastructure providing the Services with an Evergreen state by doing the following:

(i) refreshing all Hardware components of the Technical Infrastructure at least once during the Initial Term (excluding the Authority Communications Infrastructure and MODNet (or equivalent) connected End User accessed devices (save those devices provided to the Contractor for use by the Contractor);

(ii) ensuring that the Software is within a single release of the current approved version (known as n-1), unless otherwise agreed with the Authority, with a clear upgrade or migration path identified, running on a sufficient and capable platform throughout the life of the Agreement and capable of supporting the provision of the Services in accordance with the requirements set out in the Agreement for a minimum of 2 years after the expiry or termination of this Agreement. Either Party may make a written recommendation to the other that it is not in the interests of the Authority to undertake such an upgrade so as to conform with this requirement;

(iii) ensuring that all ICT used to deliver the Services is fully supportable (with all necessary security, legal or core functional Updates and Patches) by the ICT vendor or a vendor authorised third-party, for a period of 2 years after the Expiry or Termination of this Agreement; and

(iv) specifying the Technical Refresh commitment on a Change Authorisation Note adding any Hardware and Software components to the Technical Infrastructure and notified such commitments, when agreed between the Parties, against the items on the Configuration Management Database;

(d) notwithstanding the above Paragraph 3.2(c) (unless otherwise agreed in writing by the Authority):

(i) identify and, with the Authority's agreement, implement appropriate alternatives in the event that they are aware any Software and Hardware will or may be declared obsolete by the third party vendor (for example, where such Software and Hardware is announced to be at its terminal release or has no viable future upgrade roadmap at the termination of the Agreement);

(e) undertake planning and design determinations for Evergreen adherence, which includes the latest vendor software product release and support characteristics which shall factor in a higher frequency of application update release cycles and/or alternative deployment mechanisms into future Evergreen planning; and

(f) replace peripheral equipment (supplied by the Contractor to deliver the Services) as reasonably required in order to maintain the functionality of equipment at or close to accepted industry standards as agreed by both Parties and in any event at least once during the period from the Effective Date for the remainder of the Initial Term.

3.3 Where any Application (for which the Contractor is not responsible) is already installed then the Contractor shall reinstall the Application as part of any Technical Refresh process, after undertaking the appropriate due diligence analysis to establish the validity of the Application being reinstalled.

3.4 Where the Technical Refresh carried out under Paragraphs 3.2(c) and 3.2(f) contains enhanced functionality as part of the standard product, the enablement of such enhanced functionality will not be the subject of an additional charge by the Contractor.

## 4 TECHNOLOGY ROADMAP

4.1 The Contractor understands that the Authority is engaging with it to ensure that the Hardware and Software underpinning the delivery of the Services (save for the Authority Communications Infrastructure) is upgraded and refreshed during the Term, in order to ensure that:

(a) such Hardware and Software is capable of delivering the Services (throughout the Term) in accordance with the provisions of the Agreement;

(b) the Contractor hands over a 'viable service' upon expiry or termination of this Agreement (i.e. the Hardware and Software is capable of being supported for a period of 2 years post expiry of the Agreement); and

(c) the Authority transformation needs for the services and technology adhere to the Service Transformation Strategy, as regards application transformation and technology and service disaggregation.

4.2 The Contractor shall:

(a) produce, maintain and make available to the Authority a detailed Technology Roadmap of Hardware and Software, for the Term and 2 years thereafter, to show the complete set of Technical Refresh activities of all Hardware and Software components;

(b) provide support to the Authority, as part of the Joint Architecture Governance framework, in creating an Authority owned and maintained rolling 10-year Technology Roadmap; and

(c) carry out the Technical Refresh in accordance with Schedule 4.1 (Contractor Solution), which is the Contractor Solution for delivering the Services Transformation as specified by the Service Transformation Strategy.

## 5 SERVICE OPERATION MANAGEMENT & SERVICE DESIGN

**Capacity Management**

5.1 The Contractor shall:

(a) continually seek to reduce costs associated with the Contractor System by reducing the size and scale of the ICT landscape (including, but not limited to, consolidating, rationalising, simplifying product usage and adoption of alternative solutions through the use of thin provisioning, multi-tenanting, and ICT housekeeping measures);

(b) provide the scalability characteristics (including but not limited to storage, bandwidth, compute and memory) of the ICT landscape of the Contractor Solution, which must be made available as costed and fully defined elements of the Service Catalogue;

(c) provide and maintain storage capacity and capability that provides for the established growth projections of the Services; and

(d) provide evidence of such cost-saving actions performed under this Paragraph 5.1, as identified in the Capacity Management Reports.

**Data Centre Facilities**

5.2 The Contractor shall:

(a) unless agreed by the Authority, ensure that all Data Centre facilities used to deliver the Services are Authority-owned or, if not Authority-owned, compliant with Tier 3 and List X;

(b) ensure power, space, security and HVAC requirements within all Contractor Premises hosting ICT equipment are maintained and optimised to meet current requirements and have consideration to planned change in line with the Technology Roadmap;

(c) fund and resource activities resulting from both planned and unplanned system downtime and outages impacting on the delivery of the Services;

(d) host the Disaster Recovery environment within a separate Site to the Production Environment;

(e) ensure that the Contractor administration of delivered services is not impacted by planned outages of Authority or any third party Networks (where services are not hosted in Authority data centres);

(f) where possible, use Data Centres and Cloud Hosting which are capable of operating unmanned and/or with autonomous processes during both core and non-core hours and, where these processes need to be monitored remotely, the Contractor shall ensure delivery of the Services is not impacted by planned Network outages impacting Authority or any third party Networks; and

(g) provide support to third parties undertaking testing and maintenance tasks in locations where DBS Mil Pers Technical Infrastructure is located but suitable resources are not based on site including, but not limited to:

(i) electrical testing in accordance with the 'Electricity at Work Regulations';

(ii) the servicing or replacement of HVAC requirements within in Data Centres and Network rooms;

(iii) provide escorted access to Data Centre cages;

(iv) the power down and up of Data Centre or Network room Hardware as required; and

(v) works services, upgrades, maintenance and testing.

**Site Co-ordination and Installation Design Authority Standards (SCIDA)**

5.3 The Contractor shall:

(a) ensure that the Contractor System is sited and installed in accordance with SCIDA standards;

(b) propose and implement TEMPEST countermeasures to conform to standards and be approved by the Authority prior to implementation; and

(c) where applicable, complete the Engineering Change Request documentation and submit for approval by DAIS.

**Authority to Operate for Services**

5.4 The Contractor shall:

(a) ensure that the Contractor System meets the policy and accreditation mandates of the Authority to be granted an Authority to Operate;

(b) for all ICT, ensure that the hosting platforms utilised in this Agreement are:

(i) able to access the Services via an accredited route that is compliant with JSP 604 (for example, MCN through SDP or SMI gateway);

(ii) accredited and holding Authority to Operate in compliance with JSP 604 and utilise the risk-appropriate security measures for information at 'OFFICIAL-SENSITIVE' or higher classification in accordance with the 'Government Security Classification' and associated documentation (as amended and updated from time to time);

(iii) maintained and supported by undertaking all necessary data centre activities related to the maintenance of data centre power, space and HVAC requirements; and

(iv) maintained and supported in line with rest of the ICT, in accordance with the corresponding Service Requirements contained in Annex M (Technology and Applications).

**Maintain all Information and Communications Technology**

5.5 The Contractor shall:

(a) maintain all ICT used to deliver the Services with support arrangements which ensure the Service adheres to the stipulations of the Authority to Operate, security accreditation and Evergreen requirements;

(b) support and adhere to the Authority's policy for reducing the overall carbon footprint and use of resources by mandating the procurement and use of energy-efficient ICT contained in DIN 2011 DIN06-008, whereby the Contractor is required to consider the sustainability criteria when purchasing or developing ICT equipment, solutions or services, including:

(i) 'direct effect', being the change in resource consumption between old and new equipment;

(ii) 'indirect effect', being the impact on the overall resource consumption of the business processes supported by ICT;

(iii) 'procurement effect', being the resource consumption involved in the change (such as design, manufacturing and disposal, or relocation and termination of services); and

(iv) 're-use', where the energy consumption and carbon emissions of the older ICT equipment are consistent with the intent of this policy then consideration must be given to the re-use of available ICT equipment in meeting the requirement;

(c) create and maintain a Patch management strategy for the Technical Infrastructure used to deliver and support the Services, to include the following:

(i) all Hardware and Software Patching is to be kept up to date and implemented in accordance with the patching requirements and timescales as detailed in Appendix 3 of Annex M (Patch Requirements and Timescales);

(ii) monitor the deployment status for Patches for all networked and non-networked ICT;

(iii) impact assessment, Testing and implementation of Patches to be in accordance with the Change Control Procedures;

(iv) maintain an audit and history record of Patches, to be made available to the Authority on request;

(v) review all MODCERTS and deploy Patches, or take other appropriate actions, to address the documented vulnerabilities identified; and

(vi) source Patches from DOBUS or where not available, from vendor websites; and

(d) implement Anti-Virus Software updates across all ICT systems used to deliver and support the Mil Pers & Vets services, including:

(i) Anti-Virus Software Patching and Anti-Virus Software database updates are to be kept up to date and implemented in accordance with the patching requirements and timescales as detailed in Annex M (Technology and Applications);

(ii) monitor the deployment status for Anti-Virus Software updates for all networked and non-networked ICT;

(iii) impact assessment, Testing and implementation of Anti-Virus Software Patches and database updates to be in accordance with the Change Control Procedure;

(iv) where it is not technically feasible or advisable to implement, the Authority must be notified immediately; and

(v) Anti-Virus Software updates to be sourced from DOBUS or where not available, from vendor websites.

**Migration to Cloud**

5.6 When producing the Transformation Plan in accordance with Part 2 Schedule 6.1 *(Transition and Transformation Plans)*, the Contractor shall detail how all existing applications and technology used for the Services will be migrated to Cloud (or a hybrid-Cloud) services utilising 'Infrastructure as a Service' as the minimum level (unless otherwise agreed by the Authority).

5.7 For the avoidance of doubt, where the Authority refers to a requirement for Cloud, the Authority is seeking the following characteristics from such a solution:

(a) a well-defined catalogue of Technical Infrastructure, Platform and Software service options;

(b) pricing (seeking an overall cost reduction) on a utility computing basis and 'fine-grained' or modularised with usage-based billing options for all service variants (for example, Technical Infrastructure tiers, platform management options, application options, availability, and security levels);

(c) high levels of scalability (agile, flexible and responsive), with capabilities that can be elastically provisioned (in some cases automatically) to scale rapidly outward and inward commensurate with demand;

(d) high levels of automation and orchestration of tasks and processes (leading to flexible and rapid provisioning with lower costs);

(e) mature ITSM across all areas;

(f) mature security controls (appropriate to the requirement);

(g) abstraction from maintenance, insulating the Authority from the need to additionally consider and fund Evergreening of underlying service components (for example, ICT and datacentre facilities);

(h) high levels of reliability, evidenced through mature service level reporting;

(i) mature business continuity and disaster recovery measures (low recovery times) and options for Recovery Time Objectives and Recovery Point Objectives;

(j) high levels of portability to relocate technology/application components to alternative hosting platforms in the future with relative ease with no cost penalty (Cloud native applications);

(k) application solutions must be Cloud native releases which are transportable and modularised;

(l) platforms which are Cloud native (for example, the Services should have a platform agnostic in relation to the underlying operating system) offering maximum portability between Application Instances, based on a containerisation and build script automation approach); and

(m) adoption of hybrid solutions, due to complexity of customisations of COTS products must be considered, to allow for a staged Transition and Disaggregation of the Services.

**Access to Contractor Hosted Services & Tooling**

5.8 The Contractor shall:

(a) make available to the Authority or embedded Contractor Personnel the Contractor provided tools, services, and resources at the individual's regular place of work and utilising the Authority provisioned End User access device on the Authority's Network, in line with any and all specific requirements detailed with this Agreement;

(b) up to 6 months from the Operational Services Commencement Date, enable access to End Users via Contractor provided devices (with prior agreement of the Authority) and, where Contractor provided devices are provisioned, they must have the following capabilities available for use:

(i) comply with all requirements within Annex M for the delivery of ICT in terms of JSP604 and JSP440 compliance;

(ii) be connected to the MCN;

(iii) have, as a minimum, Microsoft Office Standard (including Microsoft Outlook) and Internet Explorer and any other software to enable the required connectivity;

(iv) host an End User profile;

(v) allow End Users to log on from any device on the Contractor managed Network;

(vi) host a working messaging service for internal and external e-mail;

(vii) provide access to approved internet hosted websites;

(viii) provide access to File storage (Personal and Shared); and

(ix) support provided via the Service Desk; and

(c) within 6 months from the Operational Services Commencement Date:

(i) provide and maintain access by End Users to Contractor hosted services and tooling provided via Authority MODNet devices; and

(ii) perform user identity and access management.

5.9 **Access to Third Party Software vendor support services**

(a) The Authority acknowledges and understands that Third Party Software vendors such as Oracle have a rich source of information available on their support websites, which will be pertinent to the Technical Assurance capability of the Authority which they shall make available to Authority staff.

**Access to be provided**

(b) The Contractor will provide access to the Third Party Software vendor support services, where this is not prohibited by commercial agreements in place between Contractor

and such third party, across all applications and technology stack that are used to deliver the Mil Pers & Vets services. Such access is to include, but not be limited to:

(i) ability to view active and historical service requests or problem records for the Mil Pers & Vets services; and

(ii) ability to view any Third Party Software vendor knowledge or training materials pertinent to the service provision.

**Fall-back alternatives to direct access**

(c) Where the Contractor is unable to provide direct access to the Third Party Software vendor support services, due to commercial agreements in place between Contractor and such third party, the Contractor will provide, on request, a technically unexpurgated report of the detail regarding service requests or problem records related to the Mil Pers & Vets services.

## 6 DBS DESIGN STANDARDS AND PRINCIPLES

6.1 All Contractor produced design materials, testing scope, tools, applications, operational processes and service delivery shall evidence the adherence to and implementation of (unless agreed otherwise with the Authority) the design standards and principles as contained within DBS Mil Pers & Vets Design Standards & Principles.

6.2 The DBS Mil Pers & Vets Design Standards & Principles does not override or make redundant any Standards contained in Schedule 2.3 (Standards).

6.3 The Contractor is required to input to and enhance the DBS Mil Pers & Vets Design Standards & Principles document, to drive benefit for the Parties which shall be triggered by (but not limited to) the following events:

(a) changes to industry best practice;

(b) changes to technology trends;

(c) issue or up-issue of vendor roadmap or direction statements; and/or

(d) Mil Pers & Vets change deployments.

6.4 The Authority shall maintain the DBS Mil Pers & Vets Design Standards & Principles document and any changes to it during the Term shall be subject to approval by the Joint Architecture Board.

## 7 INFORMATION TECHNOLOGY BACK-UP AND RESTORE

7.1 The Contractor shall, no later than 30 Working Days prior to the Operational Service Commencement Date, provide a draft Back-Up Plan for approval by the Authority. The draft Back-Up Plan shall be based on Paragraph 7.5 below and the existing Back-Up Plans (which will be provided to the Contractor on request).

7.2 The Parties shall ensure that the draft Back-Up Plan is agreed no later than 10 Working Days following the Operational Service Commencement Date.

7.3 The Contractor shall:

(a) maintain the Back-Up Plan throughout the Term and shall ensure that the Back-Up Plan is executed in accordance with its provisions on and from the Operational Service Commencement Date;

(b) ensure that the Back-Up Plan is fully reviewed and if necessary updated, during Impact Assessments and design work undertaken as part of the Change Control Procedure; and

(c) back-up all Data and on a regular basis (initially utilising the agreed incremental, full, and archive back-up strategy), following the applicable technical Standards and in accordance with the agreed Back-Up Plan, to meet the following:

(i) ensure that the Disaster Recovery requirements of the Service are met (as contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability));

(ii) Authority Data must be retained, secured and disposed of in adherence to the requirements of the DBS Retention and Disposal Schedule; and

(iii) all other Data which does not constitute Authority Data, but upon which the Contractor Systems are dependent in order to deliver the Service, must be backed up alongside the Authority Data; and

(d) each Quarter perform a full restore and recovery test of the back-up capability to test that the technical and procedural processes in place are sufficient to undertake a full data back-up and restore (including all of the Authority Data) in accordance with the requirements of the Bank-Up Plan and, within 10 Working Days, provide to the Authority a report evidencing performance and successful completion of such test against the requirements of the Back-up Plan.

7.4 Should it be necessary, the Contractor shall:

(a) perform any data restore (including all of the Authority Data) within the time periods set out in the Back-Up Plan (to reflect the time periods contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability);

(b) keep the Authority updated with regard to the restoration of data; and

(c) the time period shall be measured from the start of the relevant incident that triggered the recovery requirement, including where it is necessary for the Contractor to use data back-ups stored in a secure off-site location.

7.5 The Back-Up Plan shall contain the following minimum requirements:

(a) the scope of the back-up strategy to include all storage components that encompass the Contractor Systems (to become Appendix 1 to the Back-Up Plan), being:

(i) the primary focus and detail required in the plan will be on the Authority accessed Production Environment; and

(ii) ICT within the Development Environments, Production Environment, and DR environment that make up the Service, but which are not Authority facing, must also be included in the Back-Up Plan;

(b) procedures setting out how the Contractor will regularly perform incremental data back-up operations of the Hardware set out at Appendix 1 of the Back-Up Plan sufficient to ensure the Contractor is able to comply with the data restore timescale in Paragraph 7.4 above (Incremental Back-Up);

(c) procedures setting out how the Contractor shall regularly perform a full data back-up operation of the Hardware set out at Appendix 1 of the Back-Up Plan on Friday of each week sufficient to ensure the Contractor is able to comply with the data restore timescale in Paragraph 7.4 above (Full Back-Up);

(d) procedures setting out how the Contractor shall perform a full, verified, data back-up operation of the Hardware set out at Appendix 1 of the Back-Up Plan on the last working day of each month (Archive Back-Up);

(e) in the event of a critical change (as agreed by the Contractor and the Authority on a case by case basis) to the software application code create a full, verified back-up to back-up media;

(f) ensure the back-up media used by the Contractor to create the data back-up contains no information or data other than the Authority's related back-up data and information including the Authority Data;

(g) ensure that Authority Data (in whatever form) is not available to, or accessible by, any third parties except those to whom the Authority grants permission and those Sub-Contractors permitted to access the Authority data by the provisos of this Agreement;

(h) implement processes to transport securely and confirm in writing, the back-up of the Authority data to and from the secure off-site location approved by the Authority;

(i) ensure that the recording of Authority Data on all data back-up tapes (used for off-site data storage) is verified as successful and complete prior to such back-up media being despatched to the approved secure off-site location;

(j) ensure that the secure off-site storage facilities used for the back-up media containing Authority Data are located at sites deemed suitable after comprehensive threat assessments taking into account security, access/logistics, sustainability, distance from the master copy of the Authority Data and environmental conditions;

(k) the detailed restore and recovery process documents, referenced from the Back-Up Plan and made available to the Authority and detail the steps to be taken to recover and restore all Authority Data;

(l) ensure that data integrity and coherence of Data is maintained for all back-ups;

(m) a non-intrusive and non-destructive data recovery capability is required, at both whole and record level granularity;

(n) ensure that data back-ups are stored at the approved secure off-site storage facility;

(o) ensure there is no unauthorised access to the data back-ups stored at the approved secure off-site storage facility;

(p) unless agreed otherwise with the Authority, ensure that:

(i) the Incremental Back-Up is stored for a period of not less than 24 hours (from when the back-up was taken);

(ii) the Full Back-Up is stored for not less than 28 days (from when the back-up was taken); and

(iii) the Archive Back-Up is stored for not less than 52 weeks (from when the Back-Up was taken);

(q) comply with the BCDR Plans to enable the Contractor, within the RPO and RTO times (contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability)), from the start of the relevant incident, to take data back-ups stored off-site and reconstruct the relevant systems (hosting the Authority data) at an alternative location and continue to provide the Services and the Authority Data in accordance with this Agreement from such alternative location.