

- 5.3 The Supplier shall apply the '*principle of least privilege*' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of the ICT Environment used for the storage, processing and management of Authority Data. Users should only be granted the minimum necessary permissions to access Information Assets and Authority Data and must be automatically logged out of the Supplier System if an account or session is inactive for more than 15 minutes.

6. **DIGITAL CONTINUITY**

The Supplier shall ensure that each Information Asset is held in an appropriate format that is capable of being updated from time to time to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority, including in accordance with any information handling procedures set out in PSI 24/2014 (Information Assurance) if applicable.

7. **PERSONNEL VETTING AND SECURITY**

- 7.1 All Staff shall be subject to pre-employment checks that include, as a minimum, their employment history for at least the last 3 years, identity, unspent criminal convictions and right to work (including nationality and immigration status) and shall be vetted in accordance with:

- (a) the BPSS or BS7858 or equivalent; and
- (b) PSI 07/2014, if applicable, based on their level of access to Information Assets and/or Authority Data.

- 7.2 If the Authority agrees that it is necessary for any Staff to have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL (such as that requiring 'SC' clearance), the Supplier shall obtain the specific government clearances that are required for access to such Information Assets and/or Authority Data.

- 7.3 The Supplier shall prevent Staff who are unable to obtain the required security clearances from accessing Information Assets and/or Authority Data and/or the ICT Environment used to store, process and/or manage such Information Assets or Authority Data.

- 7.4 The Supplier shall procure that all Staff comply with the Security Policy Framework and principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.

- 7.5 The Supplier shall ensure that Staff who can access Information Assets and/or Authority Data and/or the ICT Environment are aware of their responsibilities when handling such information and data and undergo regular training on secure information management principles. Unless otherwise Approved, this training must be undertaken annually.

- 7.6 If the Supplier grants Staff access to Information Assets and/or Authority Data, those individuals shall be granted only such levels of access and permissions that are necessary for them to carry out their duties. Once Staff no longer require such levels of access or permissions or leave the organisation, their access rights shall be changed or revoked (as applicable) within one Working Day.

8. **IDENTITY, AUTHENTICATION AND ACCESS CONTROL**

- 8.1 The Supplier shall operate a robust role-based access control regime, including network controls, to ensure all users and administrators of and those maintaining the ICT Environment are uniquely identified and authenticated when accessing or administering the ICT Environment to prevent unauthorised users from gaining access to Information Assets and/or Authority Data. Applying the '*principle of least privilege*', users and administrators and those responsible for maintenance shall be allowed access only to those parts of the ICT Environment they require. The Supplier shall retain an audit record of accesses and users and disclose this to the Authority upon request.

- 8.2 The Supplier shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy.

9. **PHYSICAL MEDIA**

9.1 The Supplier shall ensure that:

- (a) all OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;
- (b) all physical components of the Supplier System are kept in secure accommodation which conforms to the Security Policy Framework and CESG standards and guidance or equivalent;
- (c) all physical media holding OFFICIAL information is handled in accordance with the Security Policy Framework and CESG standards and guidance or equivalent; and
- (d) all Information Assets and Authority Data held on paper are:
 - (i) kept secure at all times, locked away when not in use on the premises on which they are held and secured and are segregated if the Supplier is co-locating with the Authority; and
 - (ii) only transferred by an approved secure form of transfer with confirmation of receipt obtained.

10. **AUDIT AND MONITORING**

10.1 The Supplier shall implement effective monitoring of its information assurance and security obligations in accordance with Government standards and where appropriate, in accordance with CESG Good Practice Guide 13 – Protective Monitoring or equivalent.

10.2 The Supplier shall collect audit records which relate to security events in the ICT Environment (where this is within the control of the Supplier), including those that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such Supplier audit records shall include:

- (a) logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent it is within the control of the Supplier). To the extent the design of the ICT Environment allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;
- (b) regular reports and alerts giving details of access by users of the ICT Environment (to the extent that it is within the control of the Supplier) to enable the identification of changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data; and
- (c) security events generated in the ICT Environment (to the extent it is within the control of the Supplier) including account logon and logoff events, start and end of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

10.3 The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

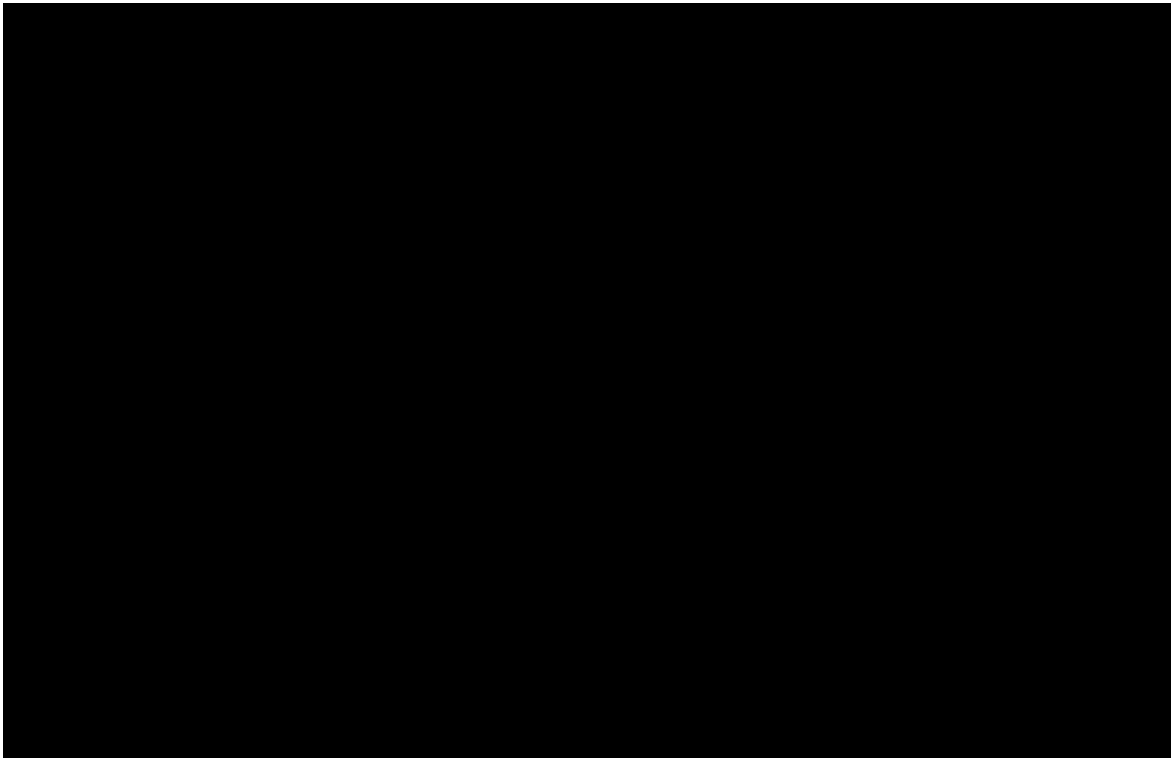
10.4 The Supplier shall retain audit records collected in compliance with paragraph 10.1 for at least 6 months.

SCHEDULE 7 – KEY PERSONNEL

1. KEY PERSONNEL

At the Commencement Date the Key Personnel are:

NAME	ROLE	RESPONSIBILITIES



SCHEDULE 8 – POLICIES AND STANDARDS

1. INTRODUCTION

- 1.1 The Supplier shall at all times comply with the Policies and Standards listed in Annex 1 of this Schedule.
- 1.2 The Parties acknowledge that any standard, policy and/or other document referred to within a Policy or Standard shall be deemed to form part of that Policy or Standard.

2. GENERAL



- 2.1 The Authority shall provide copies of the Policies and Standards from time to time to the Supplier upon request.
- 2.2 Throughout the Contract Period, the Parties shall monitor and notify each other of any new or emergent policies or standards which could affect the Suppliers provision, or the Authority's receipt, of the Services.
- 2.3 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Suppliers provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
- 2.4 Where new versions of the Authority's Policies or Standards are developed and notified to the Supplier, the Supplier shall be responsible for ensuring that the potential impact on the Suppliers provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new version of the Policy or Standard, and the Supplier shall comply with such revised Policy or Standard (and any necessary Variations to the Contract shall be agreed in accordance with clause F4 (Change)).





3. CONFLICTING POLICIES OR STANDARDS

Where Policies or Standards referenced conflict with each other or with Good Industry Practice, then the later Policy or Standard or best practice shall be adopted by the Supplier. Any such alteration to any Policy or Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

ANNEX 1

POLICES AND STANDARDS

Policy or Standard	Description
BPSS / DBS Checks	https://www.gov.uk/government/publications/government-baseline-personnel-security-standard https://www.gov.uk/disclosure-barring-service-check/overview
Civil Service Code of Conduct / MOJ Code of Conduct	https://www.gov.uk/government/collections/civil-service-conduct-and-guidance  conduct-policy.pdf
Civil Service – Good Governance	 governance_standard[1].pdf
Cloud Security / HMG Cloud Security Guidance and the Cloud Security Principles	https://www.gov.uk/digital-marketplace https://www.ncsc.gov.uk/guidance/cloud-security-collection
CPNI – Standard for Secure Destruction of Sensitive Items	https://www.cpni.gov.uk/secure-destruction
Cyber Security	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview https://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf
Domestic Violence Crimes and Victims Act 2004	http://www.legislation.gov.uk/ukpga/2004/28/contents
HM Government Security Classifications (Data Security)	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
HMG policy and guidance on Offshoring	https://www.ncsc.gov.uk/guidance
HMG (Security Policy Framework) and NCSC standards and guidance	https://www.gov.uk/government/collections/government-security https://www.ncsc.gov.uk/guidance
HMG (Cabinet Office and NCSC) guidance on Security Technology at	https://www.gov.uk/government/collections/securing-technology-at-

Policy or Standard	Description
OFFICIAL	official.
HMG Security Policy Framework (SPF)	https://www.gov.uk/government/collections/government-security
Payment Card Industry PCI Data Security Standard	 payment-card-indust ry-pci-data-security-s
Protective Monitoring	 GPG 13 - Protective Monitoring for HMG IC
Public Sector Equality Duty	 psed-guidance.pdf
TCE Act including fees	http://www.legislation.gov.uk/ukpga/2007/15/contents http://www.legislation.gov.uk/uksi/2013/1894/made
Welsh Language Scheme	 welsh-language-sche me-web.pdf

SCHEDULE 9 – BUSINESS CONTINUITY AND DISASTER RECOVERY

1. BCDR PLAN

- 1.1 The Supplier shall develop, implement and maintain a Business Continuity and Disaster Recovery Plan (BCDR Plan) to apply throughout the period of the Contract (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule.
- 1.2 Within 30 days of the Commencement Date the Supplier will deliver to the Authority for approval its proposed final BCDR Plan, which will be based on the draft BCDR Plan set out in Annex 1.
- 1.3 If the BCDR Plan is approved by the Authority it will be adopted immediately. If the BCDR Plan is not approved by the Authority the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the BCDR Plan following its resubmission, the matter will be resolved in accordance with clause 11 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 1.3 may be unreasonably withheld or delayed. Any failure to approve the BCDR Plan on the grounds that it does not comply with the requirements set out in paragraphs 1.1 to 1.3 shall be deemed to be reasonable.
- 1.4 The BCDR Plan shall, as a minimum:
- (a) address a wide range of disaster scenarios are contemplated and a variety of disaster response plans are set out which are appropriate to the occurrence of incidents of varying levels of severity;
 - (b) include an obligation upon the Supplier to liaise with the Authority with respect to issues concerning business continuity and disaster recovery;
 - (c) contain a risk analysis, including:
 - (i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;
 - (ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;
 - (iii) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;
 - (d) provide for documentation of processes, including business processes, and procedures;
 - (e) identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDR Plan; and
 - (f) include details of the procedures and processes to be put in place by the Supplier in order to deal with the occurrence of an emergency or disaster, including but not limited to:
 - (i) backup methodology and details of the Supplier's approach to data backup and data verification;
 - (ii) documentation of processes and procedures;
 - (iii) Service recovery procedures; and
 - (iv) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;

- (g) include details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the BCDR Plan is invoked;
- (h) address testing and management arrangements;
- (i) cover planned and unplanned unavailability of access to the Supplier System;
- (j) set out recovery times for key activities;
- (k) describe minimum office equipment requirements (desks, telephones, PCs, etc. including any non-standard software applications, stand-alone systems and/or other hardware);
- (l) describe Supplier System redundancy and resilience;
- (m) include arrangements for remote access to the service network devices;
- (n) include a Recovery Point Objective of 8 hours and Recovery Time Objective of 24 hours; and
- (o) include the location and integrity of configuration, password, operating manuals and other data and knowledge necessary for the continued operation of the Services.

2. TESTING

- 2.1 The Supplier shall, at no cost to the Authority, conduct a test of the BCDR Plan on an annual basis and on such further occasions as may reasonably be required by the Authority. The scope of such testing shall be agreed between the Parties.
- 2.2 The Supplier shall provide the Authority with a written report summarising the results of all tests carried out pursuant to paragraph 2.1, any failures of the BCDR Plan and any remedial action which the Supplier has taken or intends to take (which may include improvements to the BCDR Plan). The Authority may make recommendations of remedial action and the Supplier shall implement such as soon as practically possible at no cost to the Authority.

3. INVOKING THE BCDR PLAN

- 3.1 If an event occurs which, in the reasonable opinion of the Authority, constitutes an emergency or disaster affecting the Supplier's ability to perform the Services, the Supplier shall:
 - (a) immediately notify the Authority of the full details of the event and its anticipated impact on the Supplier's ability to perform its obligations under the Contract; and
 - (b) as soon as reasonably practicable but within a maximum of 6 hours:
 - (i) implement the BCDR Plan; and
 - (ii) agree with the Authority the steps that it will take to address and mitigate the event with a view to ensuring minimum disruption to the Services.

ANNEX 1
OUTLINE BCDR PLAN

