[1.3] Premises and infrastructure

Please describe your estates strategy in support of the Statement of Requirement and how you will manage your estate over the duration of the contract specifically covering:

- Availability and duration of availability of premises;
- How capacity thresholds are monitored and managed;
- How you will meet the challenge of either increasing or decreasing the capacity of your estate, what timescales this can be achieved in and how you could extend availability to support peaks and varying workloads;
- What percentage level of availability you propose for your estate and how you could extend availability to support back office work/ peaks / backlogs;
- What are your business continuity/disaster recovery arrangements in relation to your estate;
- What mechanisms are in place to maintain service during continuity/disaster periods;

Include details on:

- Confirmation of how secure access to the DWP area will be controlled;
- The security protocols which will be put in place including detail of how these will be maintained and monitored;
- How you will ensure approved staff only, will have appropriate access to DWP data; and
- The mechanisms in place to allow DWP and its nominees access to your estate.

In the event that you propose to operate from multiple sites rather than just one please also detail:

- The number of intended sites and allocation of service lines to each including estimated staff numbers;
- How and when do you propose to allocate the work between the sites;
- How they will work together;
- How will they be managed in real time to maximise available Agent resource.

Supplier Name	*G4S*	**Package**	*Package A*

Present your response within these pre-set margins in Arial font size 12 up to **4** sides of A4, **excluding** the question text and these instructions.

Introduction: Our estates strategy is to use our existing premises (single site) within the UK at Wath-upon-Dearne ({Redacted}). G4S has delivered the DWP {Redacted} service from the ground floor of this site since 2013 and has proven security protocols and protected infrastructure which has been assured by the DWP. We will expand our delivery to the first floor (currently vacant) ensuring a seamless transfer and a fast, low risk safe landing. Our facility is a modern Grade A building with: ■ Four training rooms sufficient to train up to 60 staff. ■ Five break out areas; ■ Offices for 1-2-1's and coaching sessions, ■ Personal lockers for staff ensuring wings remain secure with no mobile devices present; ■ Car parking; ■ Reception, toilets, kitchenettes. The building is Disability Discrimination Act compliant with access ramps, a wheelchair compatible lift and hearing loops. The premises are within an established business park, served by excellent transport links and within proximity to a crèche. The facility is less than a mile from the Incumbent's premises, thus facilitating the TUPE transfer into G4S.

Availability and Duration of availability of premises: Our premise, {Redacted}, has two storeys, each with two wings – we currently lease both ground floor wings. G4S has a protected lease on the ground floor north wing giving us permanent right of occupancy – this wing includes our existing secure comms room. For Package A, we will lease the first floor and extend our current lease on the ground floor south wing to five years. The table below shows service locations:{redacted}

The First Floor is currently vacant and will be refurbished prior to go live. The ground floor south wing is currently used for {Redacted}. There is sufficient additional capacity within the south floor wing to provide 93 Agent seats for Package A with no refurbishment. As the site has an existing secure communication room and DWP connection (subject to survey) this wing would be immediately available to support rapid transition – our plans are to transfer the PCE and PCC lines for July 2018. Once refurbishment is complete on the first floor, it will be dedicated to delivery of the DWP Package A lines. With capacity for 245 Agents this is sufficient for day to day volumes. After August 2018, when the pension lines move to the first floor, the ground floor south wing will provide significant additional space equating to 84 more seats (33%) than the peak winter fuel requirement should all of the available space be utilised.

How capacity thresholds are monitored and managed: The maximum load of the entire premises is 570 staff (equating to 486 Agents), calculated to allow fire regulations to be met. We will use a Workforce Management (WFM) solution from {Redacted}. Using the forecast volumes and historical volume data, it will provide a forecast of Agent numbers needed to meet service levels, for each 15 minute interval. We will use a rolling 6 month forecast, giving us early warning of potential breach of capacity thresholds. Our {Redacted} will be responsible for capacity management of the estate, supported by the {Redacted} and {Redacted}. Each month a dedicated DWP system Administrator will use the WFM tools to forward forecast volumes based on actuals. The forecasts will be updated and the capacity reviewed. We will equip the facility with sufficient infrastructure (e.g. desks, chairs, handsets) to operate at peak load +20%. Therefore we will have sufficient over capacity within the facility to cope with demand, even assuming additional peaks in demand to those forecast.

Increasing or decreasing the estate: If demand requires, after August 2018, we can extend our operations in the ground floor south wing. This offers 33% overflow capacity even in peak month (November 2020). For a higher increase over the long term, we will move to a new building (already with an agreement in principle in place). Alternatively, we would seek to use spare capacity in other existing G4S contact centres, e.g. {Redacted}. To extend the capacity of the premises, the critical task would be the installation of the DWP systems, which can take up to five months (Section 5, SoR). Moving to new premises would require installation of G4S's network, which can take up to 90 days. We can extend opening hours as the DWP request – we have 24 hour access to the premises. In the event that one or more lines' volumes decrease beyond those planned in the ITT, we can reduce their footprint in the building freeing up space to

become available for higher volumes on the remaining lines, other DWP lines or other G4S contracts. With notice, we can subdivide by internal walling the office space and reconfigure security access – e.g. we added a new service {Redacted}into the premises in 2016.
Percentage level of availability of estate & supporting back office work/peaks/backlogs: The majority of space provided for DWP Package A will be dedicated to the contract, allowing us to increase availability for back office work, peaks or backlog with 24 hours' notice. Percentage availability is as follows: First floor south and north wing will be dedicated to the Package A Contact Centre services and will have 100% availability and can be extended to 24/7 working. Ground floor south wing, 93 seats available 24/7 and 24 additional seats would be available 20:15 – 07:45 Mon-Fri and 24/7 at weekends if required.
Business continuity/disaster recovery arrangements and mechanisms: BC/DR: G4S has a corporate UK wide Business Continuity Management (BCM) policy with individual business units having BCM Plans which align to the policy. For this contract, we will undertake a business impact analysis and complete a BCM Plan, in accordance with the DWP Business Continuity Framework and BS25999. Our initial business impact analysis for this contract is shown below: {redacted}
The telephony solution is a cloud based Software-as-a-Service solution provided by {Redacted}. It is hosted in a data centre which has {Redacted} availability and an active-active secondary data centre. During delivery the Operations Manager or Deputy will be available to cover all DWP operational opening hours and to be empowered to enact Business Continuity processes. Should this be necessary we would invoke the approved plan and inform the Authority immediately; and continue to provide the agreed services as soon as practicable. Our BCM documentation are reviewed at least annually and updated accordingly. Business continuity plans and incident management plans are exercised at least annually.
Controlling secure access to DWP area: Our premises are in a business park, with shared vehicle/pedestrian access and car parks. The premises are not shared with other companies Access is on a need to know basis. Each member of staff has their own photo-id swipe card. Entry to the building is via an external and internal door (both via swipe card). Each operational wing has its own entry door, accessed via swipe card. The access control system is managed by G4S. Only DWP services will operate out of the first floor and ground floor south wing floor. Out of hours violation of the system causes a local alarm to sound, an alarm triggered in the landlord's Alarm Receiving Centre, with on-site patrol within 45 minutes. The local security team are informed, who escalate as needed. The hours can be modified to extend availability. Regular DWP staff, whose security details have been passed to G4S, will be given swipe cards, allowing free access to the premises. All visitors sign the visitors' book and are escorted or issued temporary premises passes. G4S security protocols are to challenge all those without passes and to refuse access unless the visitor has management authorisation. The access control approach is working successfully at the premises. We have had no access control violations.
Security protocols: The site security team is responsible for monitoring compliance with all security policies and compliance to ISO 27001. {Redacted}. The site security team is headed by the site {Redacted} and consists of DWP Operation Manager/s and monitoring officers. {Redacted} attends the UK G4S Information Security Management System Business Working Group chaired by {Redacted}. {Redacted} and a {Redacted} representative will also attend.
1) **Physical Security** ■The business park is protected by CCTV in the car park with suspicious activity passed onto G4S. G4S has internal CCTV at the main entry/exit points; ■Physical access control – access via swipe cards as above. Fire exits are alarmed. Ground floor external windows are covered in opaque film to stop external people seeing in; ■Visitor Policy – All visitors must sign in and be either escorted or issued temporary passes. G4S staff will challenge all visitors who have no pass/escort; ■ A clear desk policy operates at all times. Confidential material is locked away when not in use. It is disposed of in Shred-it bins; ■ Mobile phones or

any media/data storage device on the Contact Centre floor is prohibited lockers are provided for all staff.
2) **Personnel Security** ■ All staff screened by G4S, covering references and employment history for the previous five years; ■ All staff are cleared to the BPSS (Baseline Personnel Security Standard); ■ Staff with access to DWP equipment will be DBS checked.
3) **Electronic Media Policy** ■ No data may be removed from G4S telephony system without permission from the Security Team; ■ Removable storage media including mobile phones and smart watches are prohibited in operational areas; ■ USB ports etc. are not permitted; ■ Electronic media is backed up at our secure data centres; ■ G4S will follow the DWP's security protocols.
4) **IT/Telephony Security** ■ Each user will have a unique username and strong passwords. Access to DWP Case Management System will be via smart card; ■ Servers will be in locked data rooms, with need to know access; ■ Telephony and call recording system is hosted by {Redacted} in datacentre – this is certified by ISO27001 and has Cyber Essentials.
5) **Destruction Policy** – Protectively marked/sensitive assets will be handled in accordance with G4S's security policies and the Authority's Sustainability and Security policies. This includes their destruction: a) paper will be shredded using commercial shredding services from Shred-It (meeting current legislation); b) media is destroyed in compliance with CESG best practice.
6) **Segregation of Data** – the DWP Case Management System and G4S's telephony system will have no physical connection, ensuring complete segregation of all data (voice and meta-data). The Call Recording System, within the telephony system, will only be accessible to authorised users of the Contact Centre Services management team, and the DWP.
7) **Security Audit and Compliance** – The site security team will be responsible for security audit and compliance of the contact centre including; ■ Compliance to ISO 27001, risk management and root cause analysis; ■ Working with DWP Security Function, issue the Security Plan as a definitive document; ■ Ensuring G4S training modules cover all the security protocols (these are regularly reviewed); ■ Work with the management team and TMs to ensure they understand their security responsibilities and are communicating them to their teams; ■ Audit compliance against the protocols on a regular basis, including: checking security related documents are completed; checking training logs; checking access control logs; checking leavers have access right revoked; ■ Responding to any security incidents, taking immediate safeguarding actions followed by updating protocols as needed; ■ Liaison with DWP Audit and Compliance; ■ Management of DWP smart cards; ■ Subject access requests; ■ Education and awareness of employees; ■ Screen freeze access audits as per DWP system frequency; ■ Floor walks to check for clear desk and adherence to mobile device policy; ■ Exit checks and bag searches; ■ DWP monthly security and compliance audits; ■ Asset registers; ■ Web site access; ■ Acceptable use policy incidents; ■ Bogus caller reporting; ■ Use of email. The {Redacted} will oversee and govern this activity and a quarterly review will take place as part of the information security management system business working group. ISO 27001 surveillance visits will take place annually.
8) **Maintenance of Protocols** – The {Redacted} will be responsible for maintaining the security protocols. They will review all such protocols; ■ Continuously as BAU; ■ Quarterly Reviews; ■ After any security incident or breach; ■ If security requirements change.
9) Staff awareness. All employees are trained to DWP required security levels and are asked to sign in acknowledgement of their responsibilities. Clear signage within the site will reinforce the security needs as will regular audits.
How you will ensure approved staff only, will have appropriate access to DWP data: The Security Team will maintain a list of approved staff who are authorised to access DWP Data – via the Case Management System. Staff will only be approved when they have been vetted, DBS checked and completed their training. They will then be issued with logon credentials (and

a smartcard. Access will be role based. Access rights and smartcards will be revoked when a user leaves/no longer has a need to know.
The mechanisms in place to allow DWP and its nominees access to your estate: For a regular visitor the process will be: ■ DWP notify G4S of the names and security details of the person requiring access; ■ The security team arranges with the person to come to the site and will issue them a site access pass including photographic ID. Visitors are required to agree to G4S standard security undertakings; ■ If appropriate, we will establish accounts for them on the telephony system. ■ When the user no longer requires regular access to site, their pass will be retrieved and any access rights revoked; ■ In the event that they do not visit the premises in a two month period, their pass and access rights will be revoked; ■ The Security Team will undertake audits of this system. For occasional visitors, the process will be: ■ The visitor welcomed to the premises by their on-site contact and pre-arranged with G4S; ■ . The visitor will be asked to sign the visitors' book and given a temporary pass and escorted; ■ When they leave, they sign out and return any passes.