Annex 4 - IT requirements, the CMS and business continuity

1. IT Specification

In this Annex, the following expressions shall have the following meanings unless the context otherwise requires and any other terms defined in the Standard Terms, the Procedure Regulations and the Specification shall, if used in this Annex, have the meaning in the Standard Terms, the Procedure Regulations and the Specification (as applicable) applied to them:

"*Business Continuity Plan"* means your written plan setting out the processes and arrangements which you will follow to ensure continuity of your business processes and operations following any failure or disruption of any element of the provision of Contract Work and the recovery of the provision of Contract Work in the event of an Unplanned Interruption.

"*Good Industry Practice*" means the degree of skill, care, diligence, prudence, timeliness, efficiency and foresight of a skilled, experienced and professionally managed provider of legal services similar to those provided under the Contract;

"*IT System*" means the configuration of computer components comprising all the software owned by, or licensed to you by a third party (and any updates and enhancements to it), all hardware, telecommunications and network equipment used by you, together with any asset which relies in any respect on computer hardware or other information technology (whether embedded or not) which links the different parts of the system together and which, for the avoidance of doubt, includes your Case management system (as required under Clause 7.15 of the Standard Terms);

1.1 Internet and Telephony

1.1.1 Basic requirements

You are required to install and maintain communications equipment necessary to fulfil your obligations under the Contract and interact with the Operator's system. Your IT System, telephony infrastructure and communications equipment (**"Your Infrastructure"**) must be both robust and resilient; steps should be in place to mitigate any failures of Your Infrastructure. You shall (and you shall procure that those responsible for providing Your Infrastructure and any associated services) comply with the instructions of both the LAA and the Operator Service's IT and telephony staff.

You shall also procure that those responsible for providing Your Infrastructure and any associated services must agree to operate the IPsec connection for data on the specific standards set out in paragraph 1.1.2 below.

You must procure that PSTN access allows the Operator Service to pass calls to your personnel and is of sufficient capacity so that any person calling you in respect of Contract Work (including Clients and the Operator Service) does not receive an "all lines busy" response and are able to either speak to someone or (in the case of calls from Clients only, leave a message). In addition, your personnel must have access to a telephone with a direct, fixed incoming number, outbound PSTN access, and a computer with access to a named email account and the internet, in particular, http://www.direct.gov.uk/en/Dl1/Directories/UsefulContactsByCategory/Governmentcitizensandrightscontacts/DG_195356?CID=Central&PLA=url_mon&CRE=contact_cla

Each of your personnel must also have a standard direct dial telephone connection which must be available if the IPSec VPN is not available.

The Internet, via a secure SSL channel, will be the transmission medium for Case information transferred from the Operator Service. Your Infrastructure must allow access to SSL (Secure Sockets Layer channel) secured websites, in particular https://secure.855.org.uk and https://secure1.855.org.uk, and support IPsec VPN (Internet Protocol security Virtual Private Network) connections as defined by the Internet Engineering Task Force (IETF).

1.1.2 Specific Technical Requirements

1.1.2.1 Security

The following IETF standards define IPsec. Your Infrastructure must support the open standards set out within them in order to connect to the Operator Service:

RFC 4301 Security Architecture for the Internet Protocol
RFC 4302 IP Authentication Header
RFC 4303 IP Encapsulating Security Payload (ESP)
RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security association and Key Management Protocol (ISAKMP)
RFC 4306: The Internet Key Exchange (IKEv2)
RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
RFC 4308 Cryptographic Suites for IPsec
RFC 4609 Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)

Use of Network Address Translation (NAT) and certain operating systems (XP-sp1) could impede the operation of the IPsec VPN: in order for a NAT to function, it must translate either IP addresses or port numbers in the packets that it is forwarding. If a NAT translates IP addresses or port numbers for either Internet Key Exchange (IKE) traffic (which is used to negotiate IPSec security associations) or IPSec-protected traffic, the integrity of the packet is invalidated. If this is used within your infrastructure, you must be able to overcome this issue.

1.1.2.2 Telephony

Standard PSTN connections are required for telephony integration between you and the Operator Service. These may be provided using analogue, ISDN, DASS2 or other non compressed connections to mainstream PSTN providers.

1.1.2.3 Back-up and maintenance

You shall have staff in place throughout the duration of this Contract with the relevant skills to implement and maintain systems that comply with the requirements of this Annex.

You shall have suitable maintenance contract(s) and back-up system(s) in place for Your Infrastructure in the event of malfunction or breakdown, which guarantees swift rectification of any problem within the time periods specified in the table below. It is your responsibility to ensure you have appropriate arrangements in place with a service engineer. You must report any problem to your engineer, and to us and the Operator, in accordance with the time periods specified in the table below.

1.1.2.4 Software

A standard suite of software products are required, which is able to integrate with the Operator Service and be compliant with IPsec and IETF standards, Microsoft Windows 2000, Windows XP, Windows Vista and Windows Server 2003.

1.1.2.5 Connection with the Operator Service

Your Infrastructure must connect and communicate with the communications infrastructure used by the Operator Service. This will enable Case information to be accessed, and calls seamlessly transferred to you. The Operator Service runs a web-based Case Handling System ("**Operator CHS**") which contains data from those individuals calling CLA. It is available through a web browser (referred to in the following paragraph). When your personnel receive calls from the Operator Service, they will log into the Operator CHS to view the individual's data. Your personnel can, at that stage, if they wish, import the information from the Operator CHS into your own Case Management System, (**"Your CMS"**) whatever that is (subject to compatibility) or, your personnel can re-type the details from the Operator CHS into Your CMS.

Access to the Operator CHS is by means of a standard Internet browser (Mozilla Firefox, Internet Explorer, Safari etc). You will then import this data into Your CMS to allow the provision of reports as specified by us in accordance with the Contract. You must comply with our (or the Operator's) reasonable instructions to establish and maintain any data transfers.

On receiving a call from the Operator Service, your personnel are required to access the Operator CHS and look up the Case details using the unique reference number assigned by the Operator Service and adopt the Case (by clicking the relevant area within the drop down box menu on screen). Your personnel must then import a number of the individual caller's data fields into Your CMS.

The Operator CHS will have the data fields set out in paragraph 1.2 below. The exact fields that your personnel will need to import will be specified the CLA Operations Manual.

1.2 Data

1.2.1 Additional data fields for the Provider's CMS

You will be required to capture key Client data from this list (through export or cut and paste into your own system). Your CMS will, in addition, need to have the following fields:

1. Unique reference number for Case
2. Name of organisation
3. Category of Law
4. Matter Type Part 1 (defined in the CLA Operations Manual)
5. Matter Type Part 2 (defined in the CLA Operations Manual)
6. Date Case opened/accepted by Provider
7. Eligibility confirmed
8. Date Case closed by Provider
9. Total time spent
10. Stage Reached (defined in the CLA Operations Manual)
11. Outcome (defined in the CLA Operations Manual)
12. Total cost of Disbursements (defined in the Payments, Disbursements and Reviewing your Claims for Payments (Controlled Work) Annex)
13. Time spent in the current reporting month

1.2.2 Data back up

You are required to maintain a backup copy of all of the Client and Case data. This data must be stored and transferred securely.

1.3 Notification and fix periods

All failures of Your Infrastructure should be notified to us and fixed within the following periods:

Severity Level	Definition	Notification Period (measured from detection of problem)	Fix Period (measured from detection of problem)
1	**Critical** - This would be a defect which was severely affecting Your Infrastructure and the agreed contingency procedures would need to be implemented if not fixed within agreed timescales	Within 1 hour	Within 4 hours
2	**High** - A significant defect which means that the majority of Your Infrastructure was working as expected but there was still detrimental performance	Within 2 hours	Within 24 hours
3	**Medium** - A significant defect which may only be affecting a small area/number of personnel using Your Infrastructure, however this would still need to be fixed quickly	Within 2 hours	Within 48 hours
4	**Low** - A minor defect	Within 24 hours	ASAP - to be agreed on an individual basis

Material or repeated failure to meet this requirement shall be deemed a Fundamental Breach.

1.4 System upgrades

At any time during the Contract Period, the LAA may move the CLA System to an integrated platform where a closed network encompassing both voice and data over secured IP VPN's may be used to support the service and deliver it in a more efficient manner (**"VoIP Upgrade"**). If the LAA choose to implement a VoIP Upgrade you shall also be required to upgrade Your Infrastructure and paragraph 1.5 below shall apply. Notwithstanding any term of the Contract, should the LAA move to a VoIP Upgrade, Your Infrastructure must support VoIP in accordance with the following ITU standards.

Your VoIP connectivity must comply with the International Telecommunications Union (ITU) H.323 suite of standards (as amended or updated from time to time), or such standards that replace or, if superseded, such other equivalent recognised industry standards existing at the time of the VoIP Upgrade:

H.323 - Packet-based multimedia communications systems
H.225 - call control protocol
H.235 - security H.245 - media control protocol
Q.931 - digital subscriber signalling
H.450.1 - Generic functional protocol for the support of supplementary services in H.323
G.711 - PCM audio codec 56/64 kbps
G.722 - audio codec for 7 Khz at 48/56/64 kbps
G.723.1 - speech codec for 5.3 and 6.3 kbps
G.728 - speech codec for 16 kbps
G.729 - speech codec for 8/13 kbps

You must maintain a connection to the Internet of sufficient capacity and quality that for the number of your personnel providing the Contract Work, the additional data transfer must be possible whilst other non CLA day-to-day business Internet use continues. When required by us, you must ensure that any Internet connection is of sufficient capacity to enable each of your personnel to make and receive calls by VoIP.

At any time during the Contract Period, the LAA may replace the current Operator (as defined in the Standard Terms). To the extent that any replacement Operator has a different IT system to that used by the current Operator which requires you to change or upgrade Your Infrastructure to ensure you are able to comply with your obligations in this Contract, (a **"System Upgrade"**), you must upgrade Your Infrastructure and paragraph 1.5 shall apply.

1.5 VoIP Upgrade and System Upgrade procedure

Without prejudice to paragraph 1.4, we may at any time during the Contract Period notify you in writing that we intend to carry out a VoIP Upgrade and/or a System Upgrade. We will, together with such notice, also provide you with the LAA's plan for carrying out the VoIP Upgrade and/or the System Upgrade (the **"Project Plan"**). Within a reasonable period from the date of receipt of such notice, we will meet with you to discuss the Project Plan. Within a reasonable period following such meeting (such period to be agreed between us), you shall submit to us a full written plan which sets out the steps you will take to fulfil that part of the Project Plan which relates to Your Infrastructure, together with a detailed quote which sets out all your costs for implementing your plan so that the relevant upgrade meets the relevant requirements of the Project Plan. We may elect to:

(a) accept your plan and steps detailed in such plan together with your quote in writing; or

(b) negotiate and agree upon a revised plan and quote then accept such revised plan and quote in writing; or

(c) reject such plan and quote in which case the Contract will continue in force unchanged.

Until such time as any plan and quote submitted by you is formally accepted by us, you will, unless otherwise agreed in writing, continue to perform Contract Work and be paid in accordance with the Contract, as if such plan had not been requested.

Once we have accepted your plan and quote in accordance with this paragraph 1.5:

(a) you agree that you will comply with such plan; and

(b) we will pay you your costs for the relevant upgrade as specified in the quote on such terms as we agree in writing.

Unless otherwise agreed in accordance with this paragraph 1.5, you agree that you are not entitled to any costs or expenses for investigating the effect of implementing such plan.

1.6 Disclosure

You must provide us with full, accurate and complete details of Your Infrastructure and associated services (including technical computer systems relating to how Contract Work will be technically delivered to Clients) and Clause 15.8 of the Standard Terms shall apply to such information disclosed to us.

The nature of the technical connection between you and the Operator Service may necessitate giving you a route into the network of the Operator Service; you acknowledge that a lack of security within your network could, therefore, cause a breach of security within the Operator Service, possibly leading to the discovery of sensitive personal information that will be held about Clients.

If you gain entry access to any computer system of the Operator Service or the LAA (**"Access"**):

(c) all Access shall be strictly limited to that part of the computer system, software, hardware or firmware (as the case may be) as is required for the proper provision of Contract Work;

(d) you shall comply with all security audit and other procedures and requirements in the Contract and those of the Operator Service notified to you from time to time in writing in relation to Access and storage; and

(e) all information obtained from time to time in consequence of Access is deemed to be Confidential Information for the purpose of Clause 15 of the Standard Terms, and to the extent that such information is Personal Data (as defined in the Standard Terms) such information is Personal Data of which we are Data Controller (as defined in the Standard Terms) and you shall comply with the provisions of Clause 16 in relation thereto.

2. Business Continuity Requirements

2.1 Business Continuity Plan ("BCP")

You must have at all times a Business Continuity Plan which conforms with Good Industry Practice and make it available to us (or our agents) at our request for inspection. You must use all reasonable endeavours to prevent the loss, disclosure or corruption of any information relating to Contract Work held by you on your IT System. You must make up-to-date daily back-ups of such information which is in electronic format and store such backups on a regular basis offsite.

You are required to operate a disaster recovery site whereby a "warm" recovery site or facility shall be made available to you within a maximum of four hours after the occurrence of any "Disaster". A Disaster means any unplanned interruption (whether of information processing facilities or systems or otherwise) which significantly impairs your ability to perform the Contract Work (in whole or in part) to the standard of the KPIs and/or in accordance with the other terms of the Contract. This is a Severity Level 1 in the table above. If the Disaster is not fixed within 4 hours you shall implement your Business Continuity Plan immediately.

If a Disaster occurs, you shall notify us in accordance with the timescales specified in the table above and provide details of any remedial action including any re-inputting of data. Operation of your Disaster recovery plans must not be contingent on any individual whose role within the disaster recovery process does not have sufficient cover to ensure efficient operation due to absence or other business activities.

Your Disaster recovery site shall:

(a) be located such that it is not simultaneously exposed to other disasters resulting from a single event or a series of related events; and

(b) not be dependant on the same physical infrastructure as supports your primary site, such that a telecommunications, LAN, server or other infrastructure failure at your primary site must not preclude you from offering service from your Disaster recovery site.

You must ensure that:

(a) all Client and Case data held relating to the CLA service held on your computer system or that of any of your permitted sub-contractors or Agents, together with any associated software, can be recovered as soon as reasonably practicable following a Disaster;

(b) operation of the Disaster recovery site to support the CLA service is not dependant on access to the primary site;

(c) you must ensure that your personnel are provided with sufficient training on the Business Continuity Plan requirements set out in this Annex such that the risk of disruption to the CLA service is minimised.

2.2 Business Continuity Plan Testing

You shall test the Business Continuity Plan on a regular basis (and in any event not less than once in every 6 month period) and such tests shall simulate as a minimum recovery from a complete loss of software and data. You shall produce an audit report from each test and ensure that any corrective actions are taken. We may require you to conduct additional tests of the Business Continuity Plan where we consider it necessary, including where there has been any change to the Contract Work or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Business Continuity Plan.

If we require an additional test of the Business Continuity Plan, we shall give you written notice and you shall conduct the test in accordance with our requirements and the relevant provisions of the plan. Your costs of the additional test shall be borne by us unless the plan fails the additional test, in which case your costs of that failed test shall be borne by you.

Following each test, you shall send us a written report summarising the results of the test and shall promptly implement any actions or remedial measures which we consider to be necessary as a result of those tests.

You shall undertake regular risk assessments in relation to the provision of Contract Work not less than once every six months and shall provide the results of, and any recommendations in relation to, those risk assessments to us promptly in writing following each review.

Upon request by us, you shall make your Business Continuity Plan available to individuals suitably authorised by us for inspection and audit.

You shall undertake a regular review of the Business Continuity Plan. The review shall be conducted at least once a year and shall include as a minimum: identification and evaluation of systems assets; identification and assessment of the potential impact of threats to those assets, or to your system as a whole; assessments of the weaknesses and vulnerabilities in the areas of threat; evaluation of the risks arising from the assessed threats and weaknesses; and identification of countermeasures in proportion to the risk.