2026 Criminal Defence Direct Contract

Annex 4 (IT Requirements)

Unless stated otherwise, definitions in this Annex 4 (IT Requirements) shall have the meaning set out in the Contract for Signature, Standard Terms and Specification.

Connection to the ECMS

1. You must connect to the DSCC network in order to receive and process Cases via the ECMS. This will be achieved via a connection from your work device into the DSCC. Further details of the connection will be provided by the DSCC provider during the Implementation Period.

ECMS User Accounts

2. Access to the ECMS is via secure username and password authentication.

3. Each Adviser will require their own account details which include a username and a password. These user accounts will be administered by the DSCC.

4. You must email the DSCC with confirmation of the names of your personnel who require access to the ECMS. Such confirmation must be sent in advance of the date when access to the ECMS is required in order to allow a reasonable period of time for the account to be created. The DSCC will then provide the relevant usernames and generic passwords. All passwords must be changed by the relevant Adviser at first logon (details of this process are included in the ECMS user guide).

5. Usernames and passwords must be kept confidential and must not be used by any other party except the owner.

6. Should any member of your personnel leave your organisation, you must notify the DSCC provider promptly and, in any event, within 2 Business Days so that the relevant user account can be cancelled.

Workstation Information

7. In order to access the ECMS your device must meet the following minimum technical requirements:

   (a) the operating system is patched to the latest version;

   (b) all security updates are up to date;

   (c) your device must run on Microsoft Remote Desktop Version 1.2.6074.0 and newer or Microsoft Remote Desktop Version 10.2.4008.0.

8. The following items detail the basic requirements for workstations required to use the ECMS:

   (a) a personal computer with a Microsoft Windows based operating system that is fully supported, using Windows 10 (for so long as it remains supported

during this Contract), or Windows 11, that is fully patched and updated and is running and up-to-date antivirus and antimalware software; and

(b) the necessary internal network, bandwidth capacity, communications software and configuration such that your personal computers can connect to the DSCC. Further detail on this will be confirmed by the DSCC during mobilisation.

9. You must ensure you have sufficient personal computers or other compatible devices to accommodate the maximum number of Advisers on duty at any one time.

Telephony requirements

10. You are permitted to include a call recording functionality in your telephony system. The caller must be made aware that their call may be recorded and there must be an option for a Client to "opt-out" if they choose to do so.

11. In the course of delivering the CDD Services incoming calls from the Police will be handled by the DSCC and distributed via the ECMS to you. No specialist call management equipment is required to enable the distribution of incoming calls.

12. To assist in the effective delivery of the CDD Services you must meet the following basic telephony requirements:

(a) a phone for each Adviser on duty with the ability to make outgoing calls and support call conferencing. The call conferencing feature is vital to facilitate the use of the Interpretation and Translation Facility; and

(b) a dedicated direct dial contact number to be used by the DSCC or us.

LAA Software

13. The LAA has its own call handling software in the form of an electronic case handling system (ECMS). The ECMS supports the business processes which underlie the effective delivery of the CDD Services. Access to the ECMS will be made available to you from the Service Commencement Date and thereafter throughout the Contract Period. You understand that the ECMS is hosted on third party servers, and whilst we do not anticipate any issues with availability, we will not be liable for any downtime which occurs from time to time. All intellectual property in relation to ECMS will remain with the LAA at all times. No other third-party software is required.

14. You agree that you will not and will not allow anyone else to:

(a) use the ECMS other than in relation to the provision of Contract Work;

(b) copy, modify, or reverse engineer the ECMS; or

(c) operate the ECMS for the benefit of a third party.

Cyber Security Assurance and Accreditation

15. You must comply with the requirements set out in Clause 16.19 of the Standard Terms.

16. An equivalent standard to a Cyber Essentials Certificate must be assessed by a UKAS accredited assessor. More details on acceptable equivalent standards can be found in the Data Security Requirements.

17. The CDD Service must be delivered on corporate devices, i.e. laptops, personal computers, tablets, smartphones etc. that are owned and maintained by your organisation in accordance with the Data Security Requirements and the IT Requirements set out in this Annex.

18. Use of paper for recording details of Clients is prohibited. All manual notes generated in respect of this Contract that contain Personal Data of Clients must be maintained electronically on a corporate device.