Security & Vetting Solutions Ltd
Northfields House
Northfields
Twyford
Winchester
Hampshire
SO21 1NZ

Tel: +44 (0)1962 600 110

enquiries@security-vetting.co.uk
www.security-vetting.co.uk

Security & Vetting Solutions Ltd

These supplementary terms are deemed to be automatically accepted by any user of:

- The Basic criminal record disclosure platform, as set out in Section 1
- The Digital identification platform, as set out in Section 2
- The Standard & Enhanced criminal record disclosure platform, as set out in Section 3

These terms are in addition to the terms as published by Security & Vetting Solutions Ltd at https://www.security-vetting.co.uk/terms-and-conditions/

Section 1: Service – Basic Criminal Record Disclosures

1. Security & Vetting Solutions, (herein known as the Company) is a responsible body for the Disclosure & Barring Service (DBS) and Disclosure Scotland (DS). The Company offers the provision to its Client (you) to process Basic criminal record disclosures for your organisation; to ask an applicant for their criminal record history under the Rehabilitation of Offenders Act 1974 and any subsequent update.
2. Our agreement is to license you to use the platform called AccesSVS, (herein known as the platform) as necessary to perform the relevant checks for persons living or working in England, Wales & Scotland only. You may not share or distribute any aspect of our platform with any third party outside your organisation without the express permission in writing from the Company.
3. Our platform may not be used for submitting applications for persons living or working in Northern Ireland.
4. We will offer guidance and training on how to use our platform; however, we are not responsible for the accuracy of any content you enter onto the platform or how you use the platform.
5. You agree to adhere in full to any instruction issued by the Company or the Disclosure & Barring Service and Disclosure Scotland, including any updates. Specifically, and not limited to, this includes:
    a. The DBS identity checking guidance
    b. The DBS privacy policy
    c. The Disclosure Scotland privacy policy
6. You agree to have written policies for the secure and safe handling of all disclosure information and the recruitment of ex-offenders. Sample policies are supplied upon account activation.
7. For each application submitted to the AccesSVS platform, you will receive either a notification to obtain and download a DBS/DS clear certificate or a notification that the DBS/DS certificate contains information. In all circumstances, an original and single disclosure certificate will be sent to the candidate at their indicated home address.
8. If you are advised to see the disclosure certificate, you are responsible for obtaining this document directly from the candidate.
9. The candidate may only request a re-issue or reprint of a missing disclosure certificate;
    a. Directly from the DBS within 93 days of the electronic notification of issue to you. The DBS will only re-issue a certificate once. Claims, however so caused, outside this timescale will not be accepted.
    b. Directly from Disclosure Scotland within 84 days of the original print date. Claims, however so caused, outside this timescale will not be accepted.

10. You are advised that candidate data is classified as high-risk sensitive personal data in accordance with data protection legislation. You agree to comply with all aspects of data protection legislation. We may access your account on our platform without notice at any time for the purpose of managing your account and compliance audit.
11. You agree that each authorised user shall keep their password secure, confidential and that it will be changed on a regular basis.
12. All candidate personal data will be automatically and securely removed from the platform in accordance with the following criteria;
    - Candidate applications not submitted to the AccesSVS – 12 weeks from the date of entry
    - Candidate application processed to the AccesSVS – 24 weeks from the date of entry
13. Your initial licence is for up to two users. Additional users may be added and are charged at a fee of £10.00 plus VAT per additional user. You are not permitted to share platform access and user access is controlled by the Company.
14. The Company commit that our platform will have an uptime of 95% or more measured on a monthly rolling average. The Company may temporarily or permanently suspend use of our platform at any time if we believe a breach has occurred or emergency maintenance is required. The Company will endeavour to give a minimum of 48 hours' notice for scheduled maintenance.
15. The Company service target is that 80% of all applications submitted to the AccesSVS will be complete within 5 working days. This service target excludes the original certificate posted to the candidate by the DBS or DS.
16. You agree to pay the fee(s) for each application you submit via the AccesSVS to the DBS or DS for processing. Fees cannot be refunded. The Company may terminate a disclosure application upon written confirmation from the Client.
17. Subject to status approval, a credit account may be opened for a Client. In such cases, the Client agrees to pay by direct debit to the Company the relevant fee using British Pounds (£) as set out below for each application submitted to the platform in accordance with clause 18 below.
18. If applicable, the Company will invoice twice monthly. Payment terms are strictly 14 days from the date of invoice. You agree to enable and maintain payment by variable direct debit. If payment is not made within our agreed terms or you exceed your credit limit, we reserve the right to automatically suspend your account until your account status is rectified.
19. This service may be terminated with 1 months' notice in writing by either party. At the termination date, all account and candidate data will be automatically and securely removed from the platform, regardless of application status, unless otherwise expressly agreed in writing by the Company.
20. You agree that you will not copy or reverse engineer any aspect of our platform(s) and that all intellectual property rights are wholly owned by the Company.
21. Data Retention Period: Data may only be retained on the DBS processing platform for up to a maximum period of 6 months, after which it will be securely destroyed using industry best practice methods, except for records associated with how a candidate's identity was confirmed. This will be retained for a period of 2 years from the date of application in accordance with the DBS auditing requirement.
22. You agree to secure any information you require from the platform within 3 months of the disclosure completion, after which access will be revoked. You agree that the Company cannot be liable for any data that you do not secure within the relevant timescale.

Section 2: Service – Digital Identity Verification

1. Our Digital Identity Verification platform, (herein known as the DIV platform) users and their organisation, (herein known as the Client) accept these terms in full as of the account initiation date, with terms remaining in force for the duration of the account holders' access plus one calendar year following account closure.

2. You agree to use the DIV platform for the purpose of digital identity verification. The DIV platform will enable the user and/or their organisation to conduct digital identity checks in compliance with stated Government guidelines as follows:

    - DBS/DS Basic ID Check
    - DBS Standard/Enhanced ID Check
    - Right to Work (RTW)
    - Right to Rent (RTR)
    - RTW/RTR with DBS/DS Basic ID Check
    - RTW/RTR with DBS Standard/Enhanced ID Check

3. This service provider has attained UKAS accreditation for the purpose of approval that the checks are compliant with the relevant identity checking policies as issued by the Home Office for Right to Work and Right to Rent checks and the criminal record identity checking policies as issued by the Disclosure & Barring Service (DBS) and Disclosure Scotland (DS).

4. The Client remains liable for undertaking their own due diligence. The use of the UKAS accredited DIV platform will, where checks are completed in accordance with the stated guidelines, verify an identity in accordance with stated government polices by achieving a confidence score.

5. A Client will not need to undertake additional due diligence on the DIV platform or verify identity by other methods if the level of confidence score meets the required level in accordance with the compliance checks as follows:

    - DBS Basic ID Check
    - DBS Standard/Enhanced ID Check
    - Right to Work (RTW)
    - Right to Rent (RTR)
    - RTW/RTR with DBS Basic ID Check
    - RTW/RTR with DBS Standard/Enhanced ID Check

6. The UKAS accredited DIV platform will allow a user to onboard themselves and share verified attributes with a Client. The service includes sharing with you an identity and current address, which can meet the requirements of the confidence score policies as stipulated by the Home Office. The DIV platform can be configured to either meet the DBS/DS requirements, the Right to Work/Right to Rent requirements or both DBS/DS and Right to Work requirements on an individual candidate basis.

7. If a candidate is unable to meet the requirements of the DIV platform, in-person checks will be provided by the Post Office Limited in-branch and facilitated by the UKAS accredited provider, which can help the candidate meet the requirements of the DBS/DS document checking policy only. Right to Work checks and Right to Rent checks are not available via the in-person checks at the Post Office.

8. For the purpose of Right to Work/Right to Rent checks, the DIV platform may only be used by UK and Irish passport holders. For information only, foreign nationals may provide their confirmation via an official government share code process.

9. The DIV platform embedded identity verification service will allow a user to prove their identity and current address to the level required by the policy.

10. The DIV platform will have an uptime of 95% or more measured on a monthly rolling average.

11. Fees are as agreed in the fee schedule and may be amended by the Company with 1 months' notice in writing.

12. An annual licence fee, if stated in the fee schedule, is automatically invoiced on the anniversary date unless you give us at least 1 months' notice in writing that you wish to terminate the service. The DIV platform terms may be updated without notice.

13. Transaction fees are deemed to have been incurred by the Client as soon as the candidate has completed any aspect of their identity verification process.

14. Subject to credit status, transaction fees shall be paid by variable direct debit mandate to the Company 14 days from the date of invoice. The Client must accept and maintain acceptance of a variable direct debit mandate or other in writing agreed payment method or terms, to maintain access to the DIV platform.

15. A requested transaction for Right to Work check only provides a GPG45 compliant identity, which may be used for other Human Resource vetting transactions. However, this check on its own cannot be used for DBS/DS checks due to the differences in the DBS/DS and RTW/R policies.

16. DBS/DS checks for employment purposes must be made as a combined DBS/DS & RTW check. Failure to do so will void the check. The transaction fee will still apply.

General

1. Payment may not be withheld for any delay caused by any act, omission or delay by the DBS, DS or other third party.
2. Fees may be increased without notice to account for any industry standard or legislative increase forced upon the Company, subject to satisfactory and reasonable evidence.
3. You agree that the services are subject to the limitations and issues inherent in the use of the public network (including denial of service) and that the Company is not responsible for and shall not be liable to you for breach of this agreement due to any problems or other damages resulting from such limitations or issues.
4. You agree that the Company shall have no liability arising from any failure on the part of the Client to comply with its obligations in relation to Right to Work/Right to Rent checks and DBS/DS checks.
5. You agree that you will not copy or reverse engineer any aspect of our platform(s) and that all intellectual property rights are wholly owned by the Company.

Data Protection

1. When using the DIV platform under the Government Department for Digital, Cultural, Media and Sport (DCMS) Framework, the UKAS accredited provider is a data controller in its own right and when the UKAS accredited provider transfers the data to you, then you become a data controller in your own right. When using the DIV platform for you outside of the DCMS Framework and when storing any Attributes for you the UKAS accredited provider is acting as your Data Processor and UKAS accredited provider will do so in accordance with our standard data protection policies.

2. When using the DIV platform under the DCMS Framework, you must not use the DIV platform as the only method for identity verification. You must offer an alternative method. This is to ensure that the UKAS accredited provider can collect valid consent to biometric processing.

3. If the UKAS accredited provider receives a data subject access request from a data subject, you will give the UKAS accredited provider reasonable assistance in complying with the request where you are able to, for example, using the user's email address or other identifier to provide UKAS accredited provider with a session ID number. The UKAS accredited provider will take the responsibility for and incur the cost in verifying the data subject's identity.

4. The Company's privacy and data protection policies are published at www.security-vetting.co.uk. For any personal data processing query, subject access request, or data correction request, please email governance@security-vetting.co.uk.

Section 3: Service – Standard & Enhanced Criminal Record Disclosures

Purpose

1. The aim of the Disclosure & Barring Service, (herein known as the Disclosure Body) is to help organisations in the public, private and voluntary sectors by identifying candidates who may be unsuitable to work with children or other vulnerable members of society.

2. Security & Vetting Solutions, (herein known as the Company) is an umbrella body. It is our role to enable non registered bodies, employers and organisations, (herein known as the Client) to gain access to the Disclosure Body for the purpose of evidencing an applicants' criminal record when entitled to ask an applicant for their criminal record history under the Exemptions Order of the Rehabilitation of Offenders Act 1974.

The Role of the Company

1. To confirm that the Client is entitled to ask an applicant for their criminal record under the Exemption Order of the Rehabilitation of Offenders Act 1974.

2. To confirm that the Client will process all disclosure applications and information in accordance with the Disclosure Body Code of Practice.

3. The Company may offer guidance on using a Disclosure Body and associated matters. Any guidance that may be given is offered strictly on the basis that it is without any liability whatsoever. It is your responsibility to make sure that you obtain the relevant Standard or Enhanced Disclosure for the needs of your organisation. The Company strongly recommend that legal advice be sought by the Client with regard to all matters associated with implementing Disclosure Body checks within the Clients' organisation. The Company cannot be held responsible for the disclosure level that you elect.

4. The Company reserves the right to reject any application it believes the application fails to attain the DBS eligibility criteria without refund.

5. Upon receipt of a selected service request from the Client, the Company will supply the Client with the necessary application procedures to enable them to submit online applications.

6. The Client will establish a protocol with the Company to enable a candidates' identity to be confirmed by either method stated in clause 7 below: (Note: This is required as a mandatory part of the Disclosure Body application process.)

7. A nominated person within the Clients' organisation will be appointed by the Client at their own expense to become a Data Processor for the purpose of conducting the identity verification process in accordance with the Disclosure Body identity checking requirements. You may also elect to use the digital identity verification process in accordance with the stated terms above.

8. The Company may assist with guidance where appropriate for the Data Processor to perform the required duties associated with the Identity Verification Process.

9. Upon receipt of a submitted online application, the Company will check the eligibility criteria detailed within the form to ensure it is complete to the correct standard. If applicable, the application form together with the reason for failure may be returned to the Client, which then must be corrected by the Client before the application may be submitted.

10. The Client may track their applications through the online process. A candidate-only certificate will be issued by the DBS. The Client will be advised of the following certificate status:

    - A "Clear" certificate has been issued
    - "Await disclosure certificate" – This means that the disclosure certificate may contain information of relevance and you must see the candidate's disclosure certificate before making any recruitment decision

11. The Company will have no access to any certificates and it is entirely the responsibility of the Client to see the candidate only disclosure certificate, where applicable.

Role of the Client

1. The Client will facilitate a nominated Data Processor at the Clients' own expense for the purpose of candidate identity verification. The Data Processor within the Clients' organisation must be independent from the applicant and cannot verify their own identity. The Client's nominated Data Processor will be notified to the Company and the Data Processor must agree to strictly implement the DBS identity checking guidance.

2. You agree to adhere in full to any instruction issued by us or the Disclosure & Barring Service, including any update. Specifically, and not limited to, this includes:

    a. The DBS identity checking guidance
    b. The DBS privacy policy

3. You agree to have written policies for the secure and safe handling of all disclosure information and the recruitment of ex-offenders. Sample policies are supplied upon account activation.

4. The Client, during the recruitment process and before appointment, must make it known to any candidate that a Standard or Enhanced criminal record disclosure may be requested in accordance with the Exemptions Order of the Rehabilitation of Offenders Act 1974.

5. The Client will ask each candidate to complete an online application form.

6. The Client is entirely responsible for the accuracy of the data submitted in each application form. Incorrect data submitted to the Company and processed to the DBS cannot be corrected and fees will remain applicable.

7. The Clients' Data Processor (DBS platform user) may undertake the identity verification process and submit completed application forms to the Company.

8. You agree that each authorised user shall keep their password secure, confidential and that it will be changed on a regular basis.

9. Subject to status approval, a credit account may be opened for a Client. In such cases, the Client agrees to pay to the Company the relevant fee for each processed application form submitted to the Company. Weekly invoice payment terms are strictly 14 days from the date of invoice.

10. The Client agrees that each application form submitted to the Company will incur the relevant fee. Fees cannot be refunded once an application has been submitted to the Company; however, the Company may terminate a disclosure application upon written confirmation from the Client.

11. Should you determine that any candidate falls within the Disclosure Body definition of Volunteer Status, you agree to indemnify the Company for the cost of the disclosure fee if the Volunteer Status decision is overturned by the Disclosure Body, plus any additional cost reasonably incurred by the Company for this debt recovery.

12. The candidate may only request a re-issue of a missing disclosure certificate directly from the DBS within 90 days of the electronic notification of issue to you. The DBS will only re-issue a certificate once. Claims, however so caused outside this timescale will not be accepted.

13. Subject to status approval, a credit account may be opened for a Client. In such cases, the Client agrees to pay by direct debit to the Company the relevant fee using British Pounds (£) as set out below for each application submitted to the DBS platform in accordance with the clause below.

14. If applicable, the Company will invoice twice monthly. Payment terms are strictly 14 days from the date of invoice. You agree to enable and maintain payment by variable direct debit. If payment is not made within our agreed terms or you exceed your credit limit, we reserve the right to automatically suspend your account until your account status is rectified.

15. This service may be terminated with 1 months' notice in writing by either party. At the termination date, all account and candidate data will be automatically and securely removed from the platform, regardless of application status, unless otherwise expressly agreed in writing by the Company.

16. Payment may not be withheld for any delay caused by an act, omission or delay by the Disclosure Body or other third party.

17. Fees may be amended without notice to account for any industry standard or legislative increase forced upon the Company, subject to satisfactory and reasonable evidence.

18. You agree that the services are subject to the limitations and issues inherent in the use of the public network (including denial of service) and that the Company is not responsible for and shall not be liable to you for breach of this agreement due to any problems or other damages resulting from such limitations or issues.

19. You agree that the Company shall have no liability arising from any failure on the part of the Client to comply with its obligations in relation to Right to Work checks.

20. The Company's privacy and data protection policies are published at www.security-vetting.co.uk. For any personal data processing query, subject access request, data correction request, please email governance@security-vetting.co.uk.

23. Data Retention Period: Data may only be retained on the DBS processing platform for up to a maximum period of 6 months, after which it will be securely destroyed using industry best practice methods, except for records associated with how a candidate's identity was confirmed. This will be retained for a period of 2 years from the date of application in accordance with the DBS auditing requirement.

21. You agree to secure any information you require from the platform within 3 months of the disclosure completion, after which access will be revoked. You agree that the Company cannot be liable for any data that you do not secure within the relevant timescale.

General

1. Payment may not be withheld for any delay caused by any act, omission or delay by the DBS, DS or other third party.
2. Fees may be increased without notice to account for any industry standard or legislative increase forced upon the Company, subject to satisfactory and reasonable evidence.
3. You agree that the services are subject to the limitations and issues inherent in the use of the public network (including denial of service) and that the Company is not responsible for and shall not be liable to you for breach of this agreement due to any problems or other damages resulting from such limitations or issues.
4. You agree that you will not copy or reverse engineer any aspect of our platform(s) and that all intellectual property rights are wholly owned by the Company.

End.