Terms and Conditions

PARTIES

(1) **CANDIDATE MANAGER LIMITED** trading as "CANDIDATE MANAGER", incorporated and registered in Ireland with company number 376720 whose registered office is at Orchard House, Clonskeagh Square, Dublin 14, Ireland (**Supplier** or **Candidate Manager**).

(2) The company or person named in the offer or order confirmation or contract form as the Customer (**Customer**).

INTRODUCTION

The Supplier is the owner and licensor of Software defined in these Terms and Conditions and is willing to license the Customer to use these products.

The subject matter of the agreement between the Supplier and the Customer is the content of the respective order confirmation from the Supplier with the documents referred to therein, including the Terms and Conditions in the version valid at the point of the conclusion of the agreement.

Any of the Customer's contractual terms that deviate from/contradict these Terms and Conditions shall not be recognised, regardless of whether they represent a substantial amendment of the order confirmation. Any varying stipulations shall only apply if Supplier expressly agrees to them in writing.

AGREED TERMS

1. **INTERPRETATION**

1.1 The definitions and rules of interpretation in this Clause apply in this Terms and Conditions.

Agreement: means the contract between the Supplier and the Customer which governs the legal relationship. The Agreement consist of the order confirmation from the Supplier or the contract form from the Supplier which respectively contains the service description, the price, and the name of the contracting parties.

Applicable Law: means in relation to any particular person (all as amended, supplemented or replaced from time to time) any laws and any rules, regulations, orders, directives, announcements, guidance, decisions, procedures, terms and other requirements (whether any of the foregoing has the force of law or not) made, given or issued by, or published under the authority of, any regulatory body, exchange, market, clearing house or clearing system, applicable to that person or persons.

Business Day: Monday to Friday, not including Irish public holidays.

Business Hours: 8.30am to 5.30pm, Irish time, on a Business Day, and "Non-Business Hours" shall be all other times.

Change Control Procedure: means the procedure for varying this Terms and Conditions set out in Schedule 3.

Commencement Date: means the beginning of the Agreement, and that date is set out in the order confirmation or contract form.

Contract Form: means the form accompanying this Agreement, which forms part of this Agreement.

Customer Data: means information, logos, trade marks, content and data, including but not limited to Personal Data, processed or intended to be processed by the Customer using the Software or by Candidate Manager pursuant to this Agreement, including any data submitted by prospective candidates to the Customer, or by the Customer to Candidate Manager.

Consumer Price Index: the most recent Consumer Price Index published by the Irish Central Statistics Office.

Data Protection Legislation: the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) ("GDPR") and any other EU regulations, directives, decisions, opinions, codes of practice, guidelines or guidance on data protection, implementing legislation and all amendments, extensions or replacements thereto, as amended from time to time, or any other applicable data protection laws.

Defect: failure of the Software to perform in all material respects to the Specification, or to Documentation issued by the Supplier during the Term to reflect any modification, new version or update of the Software.

Documentation: any documentation or material provided by the Supplier to the Customer in any format in connection with thes Agreement.

Fees: the licence fee payable by the Customer to the Supplier under Clause 8.

Go-Live Date: means the date upon which the Customer first accesses and uses the Software in live use (i.e. not using the Software solely in the course of testing).

Intellectual Property Rights: patents, rights to inventions, copyright and related rights, trade marks and service marks, trade names and domain names, rights in get-up, rights to goodwill or to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

Personal Data: means personal data as defined by the Data Protection Legislation.

Service means any service provided or to be provided by the Supplier pursuant to these Terms and Conditions, including the Software Support Services.

Specification: the document detailing the functions and feature of the Software which forms Schedule 1.

Software: the computer programs known as "Candidate Manager" as described in the Specification. and any modification, new version or update of those computer programs which the Supplier, at its sole discretion, decides to make during the Term.

Software Support Services: the form of Software support and maintenance Services set out in Schedule 2.

Video Interview Service: the service to create recorded or conduct live job interviews set out in Schedule 4.

Term: means the term of thes Agreement as set out in Clause 11 in these Terms and Conditions.

1.2   The headings in these Terms and Conditions do not affect its interpretation. Save where the context otherwise requires, references to Clauses and schedules are to Clauses and schedules of these Terms and Conditions.

1.3   Unless the context otherwise requires:

(a)   references to the Supplier and the Customer include their permitted successors and assigns;

(b)   references to statutory provisions include those statutory provisions as amended or re-enacted; and

(c)   references to any gender include all genders.

1.4   Words in the singular include the pluraland in the plural include the singular.

2.   Licence and term

2.1   In consideration of the Fees paid by the Customer to the Supplier, the Supplier grants to the Customer a non-exclusive, personal, non-transferable licence to use and access the Software and the Documentation during the Term for the

sole purpose of processing the Customer Data.

2.2 In relation to scope of use for the purposes of Clause 2.1, "use" of and "access" to the Software shall be restricted to:

(a) accessing and using the Software on a Supplier owned or controlled server for the purpose of processing the Customer Data for the normal business purposes of the Customer (which shall not include allowing the use of the Software by, or for the benefit of, any person other than an employee of the Customer);

(b) granting access to and the right to use the Software to such of its employees, agents and subcontractors as may be reasonably necessary to process the Customer Data; and

(c) accessing the Software solely via www.candidatemanager/cm/ or such other URL that may be notified to the Customer by Candidate Manager from time to time

and the Customer shall be responsible and liable for the acts and omissions of any employee, agent or subcontractor referred to in 2.2(b) above as if they were the acts and omissions of the Customer pursuant to these Terms and Conditions.

3. Supplier obligations

3.1 Within 5 Business Days of the Commencement Date the Supplier shall commence the process of implementing and adapting the Software for access and use by the Customer. The Customer acknowledges and agrees that this process requires information and assistance from the Customer and the Customer shall co-operate with the Supplier in providing such information and assistance by attending meetings (including by conference call) as

reasonably requested by the Supplier or by submitting information reasonably requested by the Supplier to the Supplier in a timely way. As part of the process the Supplier shall issue a unique username to the Customer and the Supplier shall ensure that any user passwords chosen by the Customer or a Customer user of the Software shall not be provided to any third party by the Supplier.

3.2 As part of the Services, the Supplier agrees to:

(a) provide the training Services to the Customer set out in Schedule 2,

(b) assist the Customer carry out the Acceptance Tests;

(c) use reasonable endeavours to ensure that the Software is capable of being used by the Customer for live use (i.e. not in testing) by the Live Date; and

on the terms and conditions set out in the Agreement.

3.3 The Supplier shall perform the Services during the Term with reasonable care and skill.

3.4 The Supplier will be responsible for taking reasonable steps to implement and enforce reasonable procedures to protect the Software, any Customer Data held by it, its hardware and its systems from unauthorised access, and the downloading of and effects of any computer virus. The Supplier will be responsible for taking reasonable steps to implement and enforce firewall and other security procedures with which the Customer shall comply with when accessing and using the Software. Such steps include taking steps to counter the top ten application security vulnerabilities according to the Open Web Application Security Project (OWASP).

3.5 The Customer may from time to time request the Supplier to supply additional Services to the Customer. Any request to change the scope of the Services shall be processed in accordance with the Change Control Procedure set out in Schedule 3.

4. Customer obligations

4.1 Ireland or the United Kingdom shall be jurisdictions from which the Customer will principally access and use the Software. Prior written approval of the Supplier is required should the Customer wish to principally access and use the Software from any other jurisdiction.

4.2 The Customer shall notify the Supplier promptly if the Customer becomes aware of any unauthorised access to, use or copying of any part of the Services, Software or Documentation by any person.

4.3 The Customer shall be responsible for:

(a) obtaining and maintaining, at its own expense, such computer hardware, telecommunications lines and facilities as is necessary (including any back-up hardware, lines and facilities) in connection with the Customer's access to and use of the Software and the Services; and

(b) providing such information and doing such other things as is reasonably necessary and requested to enable the Supplier to perform its duties and obligations under these Terms and Conditions [, provided that this shall not require the Customer to expend unreasonable costs, time or resources

4.4 The Customer shall be responsible for the accuracy and completeness of the Customer Data it submits for processing by the Software.

5. Security, Access to and Use of the Services

5.1 Upon receipt of a username pursuant to Clause 3.2 the Customer will set up user passwords using the Software and shall be solely responsible for the use and access to the Software via those username and passwords.

5.2 The Customer will not use or permit anyone else to use the Services, Software or Documentation for any purpose contrary to Applicable Law, will use them only in the ordinary course of its business and will use them in accordance with this Agreement.

5.3 The Customer will monitor access and use of the Software and will ensure that the persons who access and use the Services, Software and Documentation for and on the Customer's behalf are suitably authorised in relation to the permissions provided to them by the Customer in relation to such access and use.

5.4 The Customer will be responsible for ensuring the integrity of such of its systems, hardware and software that interface with the Software or Services, and, in particular, will take reasonable steps to implement and enforce reasonable procedures to protect such systems and software from unauthorised access and the downloading of and effects of any computer virus.

5.5 Due to the inherent risks of internet usage, the Supplier does not accept any liability for loss to the Customer as a result of connecting to the Software and Services through the medium of the internet or any other telecommunications system.

6. Suspensions, etc.

6.1 The Supplier may, from time to time, suspend or otherwise limit the

Customer's access to and use of any one or more of the Services or the Software (including that of any particular person given permission by the Customer to such access and use), provided that in so doing the Supplier must act reasonably and in good faith. The Supplier shall use reasonable endeavours to notify the Customer of its intention to ***impose any suspension or limitation, and the reason for such, before it imposes*** such suspension or limitation, but if such notification is impracticable will otherwise notify the Customer as soon as reasonably practicable thereafter and in any event within 14 Business Days. Account shall be taken by the Supplier of the duration of any suspension or substantial limitation made by the Supplier in respect of the Software pursuant to this Clause for the purposes of calculating the availability levels for the Software set out in Schedule 2.

7. **Warranties**

7.1 Each party warrants to the other that:

(a) it is fully authorised to enter into, and to perform its obligations under, the Agreement;

(b) the Agreement constitute valid, legal and binding obligations enforceable against it, except for the effect of bankruptcy, insolvency, re-organisation, moratorium and other similar laws relating to or affecting creditors' rights generally and to general equitable principles; and

(c) it holds and will comply with all consents, authorisations and licences (including, without limitation, governmental and regulatory consents) necessary for the exercise and performance of its rights and obligations under this Agreement.

8. **Fees**

8.1 In consideration of the Services and the licence of the Software the Customer shall pay to the Supplier the Fees set out on the Contract Form. All sums payable under this Agreement are exclusive of VAT, for which the Customer shall be responsible. Such Fees shall be paid annually in advance by the Customer to the Supplier within 30 days of the date of the Supplier's invoice.

8.2 If the Customer fails to pay any amount payable by it under the Agreement, the Supplier shall be entitled (but not obliged) to charge the Customer interest on the overdue amount, payable by the Customer forthwith on demand, from the due date up to the date of actual payment, after as well as before judgment, at the rate of [2]% per annum above the base rate for the time being of [Bank of Ireland]. Such interest shall accrue on a daily basis and be compounded quarterly.

8.3 The Supplier shall be entitled to increase the Fees as from each anniversary of Commencement Date to take account of any increase in CPI during the previous year or since the last adjustment of the Fees by the Supplier pursuant to this Clause, whichever is the longer. Any such increase shall be notified to the Customer at least 30 days prior to such anniversary. The Customer may terminate the Agreement on giving notice to the Supplier at least 10 days prior to such anniversary should it not be agreeable to paying any increased Fees notified by the Supplier to the Customer pursuant to this Clause.

9. **Software Support Services**

9.1 From the date of providing the Customer with the user name referred to in Clause 3.2 the Supplier shall provide the Software Support Services to the Customer with a view to ensuring that

the Software performs in all material respects to the Specification or Documentation. During the Term the Customer shall notify the Supplier in writing of any Defect in accordance with Schedule 2 and the Supplier agrees to provide the Software Support Services to the Customer in respect of any Defects in accordance with the Software Support Services levels set out in Schedule 2.

9.2 When providing the Software Support Services the Supplier may, at the Supplier's option, do one of the following:

(a) repair the Software; or

(b) replace the Software; or

(c) terminate the Agreement immediately by notice in writing to the Customer and refund any of the Fees paid by the Customer (less a sum calculated on a pro rata basis having regards to the period to which the Fees related);

provided the Customer provides all the information that may be necessary to assist the Supplier in resolving the Defect, including sufficient information to enable the Supplier to re-create the Defect.

9.3 The Supplier shall not be obliged to provide the Software Support Services to the Customer in respect of any Defect that results from the Customer, or anyone acting with the authority of the Customer, having misused, incorrectly used or damaged the Software or from any breach of the Customer's obligations under the Agreement.

9.4 The Supplier does not warrant that the use of the Software will be uninterrupted or error-free. The Customer accepts responsibility for the selection of the Software to achieve its intended results.

9.5 All other conditions, warranties or other terms which might have effect between the parties or be implied or incorporated into the Agreement or any collateral contract, whether by statute, common law or otherwise, are hereby excluded, including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or the use of reasonable skill and care.

9.6 Except as expressly stated in Clause 9.8 , the Supplier shall have no liability for any losses or damages which may be suffered by the Customer (or any person claiming under or through the Customer), whether the same are suffered directly or indirectly or are immediate or consequential, loss of profits, anticipated savings, business opportunity or goodwill, loss of data or special damage even though the Supplier was aware of the circumstances in which such special damage could arise.

9.7 Except as expressly stated in Clause 9.8 the total liability of the Supplier, whether in contract, tort or otherwise and whether in connection with the Agreement or any collateral contract, shall in no circumstances exceed a sum equal to the Fees payable in the year of the Term in which the liability arises.

9.8 The exclusions in Clause 9.6 shall apply to the fullest extent permissible at law, but the Supplier does not exclude liability for death or personal injury caused by the negligence of the Supplier, its officers, employees, contractors or agents for fraud, or any other liability which may not be excluded by law.

9.9 The Customer acknowledges that it is solely responsible for:

(a) all computer hardware, software, telecommunications lines and facilities which it obtains, has and/or operates;

(b) using any particular supplier of such hardware, lines and facilities; and

(c) taking reasonable steps to ensure that such hardware, lines and facilities are compatible with, and do not detrimentally affect the provision or performance of, the Services, Software or, where relevant, Documentation.

9.10 The Customer acknowledges that no representations were made prior to entering into the Agreement. The Customer agrees that, in entering into the Agreement, it did not rely on any representations (whether written or oral) of any kind or of any person other that those expressly set out in the Agreement. The Customer shall have no remedy in respect of any representation (whether written or oral) made to it on which it relied in entering into the Agreement and the Supplier shall have no liability otherwise than pursuant to the express terms of the Agreement.

9.11 The Customer shall indemnify and keep fully and effectively indemnified and hold harmless the Supplier against any and all loss, damages, demands, liability, costs, claims or expenses (including legal costs and expenses) which the Supplier may suffer or incur by reason of the breach of any of the provisions of the Agreement by the Customer, its employees, agents or subcontractors howsoever caused or the acts, omissions or negligence of employees, agents and subcontractors who are permitted access to and/or use of the Software.

10. Intellectual property rights

10.1 The Customer retains all Intellectual Property Rights in the Customer Data, and grants the Supplier a licence to such Intellectual Property Rights to the extent required to perform its obligations pursuant to the Agreement. The Customer shall indemnify the Supplier against all damages, losses and expenses arising as a result of any action or claim that the Customer Data infringe any Intellectual Property Rights of a third party. The Supplier reserves the right to return specific Customer Data to the Customer where it receives notice of an action, claim, allegation or complaint from a third party in respect of the specific Customer Data and shall notify the Customer if it becomes aware of any such an action, claim, allegation or complaint.

10.2 The Customer acknowledges that all Intellectual Property Rights in the Software and Documentation belong and shall belong to the Supplier, and the Customer shall have no rights in or to the Software and Documentation other than the right to use them in accordance with the terms of the Agreement.

10.3 Subject to Clauses 10.4 and 10.5, the Supplier shall, at all times during and after the Term, indemnify the Customer and keep the Customer indemnified against all losses, damages, costs or expenses and other liabilities incurred by, awarded against or agreed to be paid by the Customer arising from any claim that the Software or Documentation infringe a third party's Intellectual Property Rights (an "Infringement Claim").

10.4 The Customer shall:

(a) notify the Supplier immediately in writing of any Infringement Claim;

(b) allow the Supplier the sole conduct all negotiations, settlement or proceedings and provide the Supplier with such reasonable assistance as is required by the Supplier, each at the Supplier's cost, regarding the Infringement Claim; and

(c) not, without prior consultation with the Supplier, make any admission relating to the Infringement Claim or attempt to settle it;

10.5 If an Infringement Claim is made, or the Supplier anticipates that an Infringement Claim might be made, the Supplier may, at its own expense and sole option, no additional cost to the Customer either:

(a) procure for the Customer the right to continue using the part of the material which is subject to the Infringement Claim; or

(b) replace or modify, or procure the replacement or modification of, such material, provided that the performance and functionality of the replaced or modified item is substantially equivalent to the performance and functionality of the original item;

11. Term

The initial term of the Agreement begins on the Commencement Date and continues for the period specified in the Contract Form (the "Initial Term"), unless terminated earlier pursuant to these Terms and Conditions or rather the Agreement. At the end of the Initial Term, it shall be renewed automatically for further periods of one year unless terminated by either party giving to the other party not less than ten Business Days written notice of termination prior to the commencement of the next one year period, unless terminated earlier pursuant to the Agreement.

12. Termination

12.1 Either party may terminate the Agreement at any time on written notice to the other if the other:

(a) is in material or persistent breach of any of the terms of the Agreement and either that breach is incapable of remedy, or the other party fails to remedy that breach within thirty days after receiving written notice requiring it to remedy that breach; or

(b) is unable to pay its debts, or becomes insolvent, or is subject to an order or a resolution for its liquidation, administration, winding-up or dissolution (otherwise than for the purposes of a solvent amalgamation or reconstruction), or has an administrative or other receiver, manager, trustee, liquidator, administrator or similar officer appointed over all or any substantial part of its assets, or enters into or proposes any composition or arrangement with its creditors generally, or is subject to any analogous event or proceeding in any applicable jurisdiction.

12.2 In the event that the Customer has defaulted in payment of the Fees, the Supplier may, in its sole discretion and in addition to any other remedies available to it pursuant to the Agreement or otherwise:

(a) furnish the Customer with fourteen (14) days prior written notice of its intention to terminate the Agreement; and

(b) may terminate the Agreement should the Customer not remedy this default within that notice period.

12.3 Termination by either party in accordance with the rights contained in Clause 11 shall be without prejudice to any other rights or remedies of that party accrued prior to termination.

12.4 On termination for any reason:

(a) all rights granted to the Customer under the Agreement shall cease;

(b) the Customer shall cease all activities authorised by the Agreement; and

(c) the Customer shall immediately destroy or return to the Supplier (at

the Supplier's option) all copies of the Documentation then in its possession, custody or control and, in the case of destruction, certify to the Supplier that it has done so.

12.5 Within 30 days of termination of the Agreement the Supplier shall return to the Customer the Customer Data in live use which it possesses. The Customer agrees and acknowledges that the Supplier may retain archival or back-up copies of the Customer Data that is not in live use on termination because of the technical difficulties in accessing and deleting all back-up copies of the Supplier's databases provided that, following termination of the Agreement the Supplier shall cease all use of the Customer Data for any purpose other than retaining archival or back-up copies of the Customer Data. The Supplier agrees and acknowledges that Clauses 10.1, 14 and 15 shall continue to apply to the Customer Data following termination of the Agreement.

13. Force majeure

No party shall be liable to the other for any delay or non-performance of its obligations under the Agreement arising from any cause beyond its control including, without limitation, any of the following: act of God, governmental act, war, fire, flood, explosion, power surges or outages, strikes or employment disputes, or civil commotion. For the avoidance of doubt, nothing in Clause 13 shall excuse the Customer from any payment obligations under the Agreement.

14. Data Protection

14.1 The Supplier agrees that, to the extent it processes any Personal Data on behalf of the Customer:

(a) it does so only as a Data Processor for the Customer;

(b) it shall act only on instructions from the Customer; and

(c) it has in place appropriate technical and organisational security measures against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

14.2 The Customer warrants that it has full capacity, authority, appropriate legal bases, and where relevant, consents to disclose the Customer Data, any user and any Personal Data to the Supplier, including but not limited to, pursuant to the Data Protection Legislation.

14.3 The Customer acknowledges that it is the Data Controller within the meaning of Data Protection Legislation in respect of Customer Data. Accordingly, the Customer warrants that is has in place, and complies with the terms of, an appropriate data protection notice with data subjects whose personal data is processed in the course of the provision of the Services, pursuant to Data Protection Legislation, and the Customer undertakes to continue to do so for so long as Services are provided under the Agreement.

14.4 The Customer and the Supplier may from time to time enter into a Data Processing Agreement in order to provide further detail on these provisions, in substitution for this Clause, and if they do, the terms of such Data Processing Agreement, provided only that it is in the Supplier's then current standard form for such agreements, shall prevail over this clause of the Agreement.

15. Confidentiality and publicity

15.1 Each party shall, during the term of the Agreement and thereafter, keep confidential all, and shall not use for its own purposes nor without the prior

written consent of the other disclose to any third party any, information of a confidential nature (including, without limitation, the Software, Documentation trade secrets and information of commercial value) which may become known to such party from the other party and which relates to the other party, unless such information is public knowledge or already known to such party at the time of disclosure, or subsequently becomes public knowledge other than by breach of the Agreement, or subsequently comes lawfully into the possession of such party from a third party.

15.2 The terms of the Agreement are confidential and may not be disclosed by the Customer without the prior written consent of the Supplier.

15.3 The provisions of Clause 15 shall remain in full force and effect notwithstanding termination of the Agreement for any reason.

16. Waiver

No forbearance or delay by either party in enforcing its rights shall prejudice or restrict the rights of that party, and no waiver of any such rights or of any breach of any contractual terms shall be deemed to be a waiver of any other right or of any later breach.

17. Severability

If any provision of the Agreement is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions shall not be prejudiced.

18. Amendments

Any amendment, waiver or variation of the Agreement shall not be binding on the parties unless set out in writing, expressed to amend the Agreement and

signed by or on behalf of each of the parties.

19. Notices

Any notice required to be given pursuant to the Agreement shall be in writing, and shall be sent to the other party marked for the attention of the person at the address set out for such party in the Agreement. Notices may be sent by first-class mail or fax, provided that faxes are confirmed within [24 hours] by first-class mailed confirmation of a copy. Correctly addressed notices sent by first-class mail shall be deemed to have been delivered 72 hours after posting and correctly directed faxes shall be deemed to have been received instantaneously on transmission, provided that they are confirmed as set out in Clause 19.

20. Remedies

The Customer agrees that damages will be an inadequate remedy for any breach of its obligations the Agreement and that the Supplier will be entitled to apply for and obtain relief to restrain the breach or threatened breach of, or otherwise specifically to enforce, the Customer's obligations under the Agreement.

21. Entire agreement

21.1 These Terms and Conditions, including its Schedules and the Contract Form/or the order confirmation contain the whole agreement between the parties relating to the subject matter hereof and supersede all prior agreements, arrangements and understandings between the parties relating to that subject matter.

22. Assignment and subcontracting

22.1 In relation to assignment and subcontracting:

(a) the Customer has no right to subcontract or to assign the benefit or burden of the Agreement in whole or in part, or to allow the Software to become the subject of any charge, lien or encumbrance without the prior written consent of the Supplier.

(b) the Supplier may sub-license, assign, charge, subcontract or otherwise transfer any of its rights or obligations under the Agreement, provided it gives written notice to the Customer of any sub-licence, assignment, charge, subcontract or other transfer.

23. **Governing law and jurisdiction**

These Terms and Conditions as well as the Agreement shall be governed by and construed in accordance with Irish law and each party hereby submits to the non-exclusive jurisdiction of the Irish courts.

Schedule 1- Specifications: Functions and Features of the Software

<u>Product Description (Modules)</u>

<u>Calendar Management Module</u>
Core Functionality
      - Ability to create & track scheduled appointments
      - Ability to synchronize CM calendar with corporate email system
      - Ability to view calendar in multiple formats (Day, Week, Month & Classic view)

<u>Jobs Module</u>
Objective: To give the client the ability to post jobs to all configured recruitment media.
Core Functionality:
      - Job creation/ editing/ copying & deleting
      - Job filtering by division/ business unit/ reference/ job ID, recruiter or by date range
      - Real-time job publishing to careers microsite and third party sources.
      - Job history tracking
      - Job archiving/ storage

<u>Form Builder Module</u>
Objective: To offer the client the ability to create, store, edit & copy individual application/ employment forms, adding ranking, screening pre-profiling questions.

Core Functionality:
      - Application Form creation/ editing/ copying & deleting
      - Ability to create & store 6 question types
      - Ability to categorise questions
      - Ability to create & store sections
      - Ability to export application form into word format
      - Application Form storage

<u>Reports Module</u>
Objective: To offer the client the ability to run detailed real-time reports on the entire recruitment process.
Core Functionality:

      - Real-time report generation
      - Reports framework categorised into 3 types (Jobs, Applicants & User based reports)
      - Reports manipulation (Ability to run reports across predetermined criteria)
      - Reports exported into Excel format
          *Report list available upon request<u>Applicants module</u>
Objective: To enable the client to process applicants through the stages in the recruitment process. Recruiters will have the ability to run keyword CV searches across the applicant talent pool.

Core Functionality:
      - Applicant tracking across hiring process (Real-time applicant progress interface)
      - Applicant Record Search
      - Ability to run CV Search facility across talent pool (Based on key words/ skills)
      - Applicant source tracking
      - Applicant screening/ ranking

                                              4023.9032.5023006v2

- Applicant date/ time stamp
- Recruiter subjective rating
- Ability to progress individual/ bulk applicant records to predefined selection stages
- Ability to generate/ send email templates to individual/ bulk applicants
- Ability to forward individual/ multiple applicants to hiring Manager
- Ability to sort applicants by rank/ rating
- Ability to track applicants by selection status
- Ability to copy applicants
- Ability to track job by status
- Ability to store/ archive jobs & associated applicants
- Applicant Record

  - o CV/ Application form, personal details storage
  - o Applicant history tracking
  - o Ability to create applicant related tasks
  - o Ability to upload documents
  - o Ability to capture applicant related notes

Admin Module

Objective: To enable the client to manage internal access and use of candidate Manager Core Functionality
- Ability to create/ edit/ lock-out/ delete system users & assign access rights (7 rights available)
- Ability to edit/ create & delete Division/ Business unit structure
- Ability to create/ edit/ copy/ delete emails/ letter templates
- Ability to edit/ delete & track agency details
- Ability to add/ delete consultants to created agencies
- Ability to define system options/ preferences

Schedule 2- Software Support Services and Training Services

A. Software Support Services
Software Availability:

Delivery over a one year period: 99.9% availability of the use and access to the Software to the Customer during Business Hours.

Delivery over a one year period: 99.1% availability of the Candidate Manager Service to the Customer during Business Hours and Non-Business Hours.

The first "year" for measurement of the Software availability shall be the Go-Live Date to the first anniversary of the Commencement Date, and each "year" after that shall be from one anniversary of the Commencement Date to the next.

The Software will be available to the Customer's users to whom passwords have been allocated to log in and use the Software for managing job/vacancy recruitment processes within the Software availability range specified above. Planned maintenance is normally scheduled by the Supplier outside of Business Hours.

Reporting Procedures:

Where the Supplier plans maintenance or support of the Software, or a modification, new version or update of the Software the Supplier will use reasonable endeavours to inform the Customer four weeks before the date of such Services. Where the Supplier carries out unplanned Software maintenance or support of the Software it will use reasonable endeavours to inform the Customer in advance, but in any event will inform the Customer as soon as is practicable and major Software Defects will be reported to the Customer within 2 Business Days of the Supplier becoming aware of the Defect.

Customer Support & Escalation Procedures:

As part of the Software Support Services the Customer shall receive re-active assistance from the Supplier through a structured 3 levels helpdesk support framework during Business Hours.

Should the Customer wish to receive the Software Support Services during Non-Business Hours it may request this from the Supplier and the Supplier shall provide such Software Support Services to the Customer at an additional cost to the Customer payable in advance.

As part of the Software Support Services the Customer shall receive pro-active assistance from a nominated Supplier Account Manager during Business Hours. The Supplier shall notify the Customer in writing promptly in the event of any proposed change to the appointed nominated Supplier Account Manager.

The Supplier Account Manager shall have the following responsibilities as part of the Software Support Services:

-        To build a strong rapport with the Customer and to ensure that the Software meets all service level expectations;

4023.9032.5023006v2

- To assist in the dissemination of information in relation to use of the Software and the Services and in helping communicate the change in procedures to the Customer's Hiring Managers & to Staffing Firms/ Recruitment Agencies acting as the Customer agent which/who the Customer has notified to the Supplier;
- To offer consultancy & advice on best practice procedures/ process in using and accessing the Software upon the Customer requesting such advice
- To provide the Customer with periodical updates on new developments/ functionality carried out by the Supplier in respect of the Software; and
- To ensure that the Customer is utilising the Software functionality to it's maximum potential having regards to the Customer's needs and uses that the Customer has informed the Supplier of.

Escalation Procedures:

To receive the Software Support Services the Customer shall promptly report any Defect to the Supplier into Level 1 Helpdesk Support by telephone/ email or captured within the support tracking system. The Supplier's Level 1 Helpdesk Support shall also provide first-line technical support to the Customer users. The Supplier will inform the Customer of the relevant contact details in respect of such Level 1 Helpdesk Support.

The Defect shall be queued and evaluated by the Supplier, and either resolved or escalated to Level 2 Support.

Where the Supplier, in its sole discretion, escalates a Defect to Level 2 Support as part of the Software Support Services a more technical focused resolution is typically required to be implemented by the Supplier.

The Supplier shall respond to the Customer regarding all reported Defects within 1 Business Day. If the Defect cannot be fixed or resolved by the Supplier within 1 Business Day the Supplier will inform the Customer of the estimated resolution timeframe for remedying the Defects.

The Supplier will take all reasonable measures to ensure that the Customer Data is accessible at all times by the Customer.

User Security

The Customer agrees and acknowledges that all activity using its user name and user passwords is logged. The Supplier shall ensure that all editing or deleting action taken in respect of the Customer Data using the Software is tracked by the Supplier in a database and can be queried to give full accountability of what user name or password holder did what such action. The Supplier shall ensure that the Customer user passwords are encrypted and shall determine specific user levels for the Software from time to time. The Customer is responsible for ensuring that appropriate users are given appropriate user levels and for ensuring that the Customer user's passwords have an appropriate expiry period. The Supplier shall ensure that user accounts accessing the Software are locked after 3 false login attempts using incorrect passwords.

The Supplier continuously monitors all servers upon which the Customer Data is hosted with a view to identifying any irregularities in access or use of the Customer Data.

B Training Services

User training

4023.9032.5023006v2

User training will be provided by the Supplier to the number of the Customer's users set out in the Contract Form as part of the Services. This user training will cover the core functionality of the Software and users will be given a complete and comprehensive understanding of the functionality of the Software. The number of the Customer's users set out in the Contract Form as "Administrators" will be given additional training by the Supplier on the "Administrator" user function of the Software by the Supplier as part of the Services

Schedule 3 - Change Control Procedure

1. The Supplier and the Customer shall discuss any change to this Agreement (Change) proposed by the other and such discussion shall result in either:

    (a) a written request for a Change by the Customer; or
    (b) a written recommendation for a Change by the Supplier,

or, if neither of the Customer nor the Supplier wishes to submit a request or recommendation, the proposal for the Change will not proceed.

2. Where a written request for a Change is received from the Customer, the Supplier shall, unless otherwise agreed, submit a Change control note (CCN) to the Customer within the period agreed between them or, if no such period is agreed, within five Business Days from the date of receipt of such request for a Change.

3. A written recommendation for a Change by the Supplier shall be submitted as a CCN direct to the Customer at the time of such recommendation.

4. Each CCN shall contain:

    (a) the title of the Change;
    (b) the originator and the date of the request or recommendation for the Change;
    (c) the reason for the Change;
    (d) the full details of the Change;
    (e) the price, if any, of or associated with the Change;
    (f) a timetable for implementation, together with any proposals for acceptance of the Change;
    (g) the impact, if any, of the Change on other aspects of this agreement, including:
    (i) the change to the Fees;
    (j) the contractual documentation;
    (k) the date of expiry of validity of the CCN
    (l) provision for signature of the CCN by the Customer and the Supplier.

5. For each CCN submitted, the Customer shall, within the period of validity of the CCN as set out in paragraph 4(h) of this Schedule 3:

    (a) allocate a sequential number to the CCN;
    (b) evaluate the CCN, and as appropriate either:
            (i) request further information; or
            (ii) approve the CCN; or
            (iii) notify the Supplier of the rejection of the CCN; and
    (c) if approved, arrange for two copies of the approved CCN to be signed for or on behalf of the Customer and the Supplier. The signing of the CCN shall signify acceptance of a Change by both the Customer and the Supplier.

6. Once signed by the Customer and the Supplier in accordance with paragraph 5 of this Schedule 3, the Change shall be immediately effective and the Customer and the Supplier shall perform their respective obligations on the basis of the agreed amendment.

4023.9032.5023006v2

Schedule 4 – VIDEO INTERVIEW SERVICE

1. The video job interview service ("VIDEO INTERVIEW SERVICE") allows customers to create a) customized automated and/or b) live job interviews for any time zone, level of seniority and interview stage (the "VIDEO INTERVIEW"). An automated job interview is a structured way of interviewing where the customers' candidate ("CANDIDATE") answers a pre-recorded set of questions with a video recording at their convenience. The live job interview is a real-time interactive online conversation between a CANDIDATE and one, or multiple, interviewer(s).

2. The web-based software system on which the VIDEO INTERVIEWS are generated (the "SYSTEM"), stored in a database specific to the customer and are made available to the customer. This SYSTEM can be accessed by the customer through an internet connection, using a username and password.

3. Candidate Manager shall offer the customer access to the SYSTEM through an internet connection, making use of a username and password, and the customer will be able to make use of the SYSTEM as described in the user documentation (which can be found in the tutorial area within the SYSTEM) and create a database with the recorded videos. The database means the collection of VIDEO INTERVIEWs put in the SYSTEM for the customer.

4. The SYSTEM may also be used by to put the CANDIDATE and the customer in contact with each other using a webcam connection over the internet. Candidate Manager shall make an effort to support as effectively as possible the technology for the VIDEO INTERVIEW recorded in this way, but cannot be held liable if a video interview is not realised completely or at all.

5. The customer is not permitted to give third parties access to the SYSTEM e.g. by letting them perform VIDEO INTERVIEWs with its CANDIDATEs, unless expressly agreed otherwise in the agreement.

6. To make use of the VIDEO INTERVIEW SERVICE, the purchase of credits is necessary. One credit represents one VIDEO INTERVIEW. Every time a VIDEO INTERVIEW has been conducted, the relevant amount of credits are depleted from customers' account within the SYSTEM. A VIDEO INTERVIEW has been conducted if a) the CANDIDATE provided its recorded video or b) the customer has carried out the live job interview with the CANDIDATE. All credits which have purchased are valid for twelve (12) months from date of purchase. The payment is made in advance after the issue of the invoice.

7. (Personal) Data of the CANDIDATE must be treated confidentially by both, Candidate Manager and the customer. Personal Data of the CANDIDATE which Candidate Manager shall not record videos of a CANDIDATE without the CANDIDATE's advance permission. Candidate Manager has the right to delete the recorded VIDEO INTERVIEWs from the SYSTEM after one (1) year, unless agreed otherwise with the customer. Personal Data provided by the CANDIDATE for the purpose of conducting the VIDEO INTERVIEW may include CANDIDATEs Name, email address and (recorded) video.

8. Candidate Manager shall make every reasonable effort to secure the SYSTEM against loss and/or any form of improper use, and shall use the suitable technical and organisational measures for this purpose.

4023.9032.5023006v2

9. If communication between Candidate Manager and the CUSTOMER takes place using electronic resources, such as email and other forms of data traffic, both of the parties shall bear responsibility for standard virus protection. Candidate Manager is not liable vis-à-vis the customer for any loss or damage that arises from transmitting viruses and/or other irregularities in the electronic communication, or for any messages not received or which were received in a damaged state.

Schedule 5 – Data processing Addendum

1. Subject matter and duration of the Order or Contract

(1) By placing an order Candidate Manager (processor) and customer enter into a data processor agreement according to Art. 28 GDPR. Candidate Manager acts as processor for customer according to Schedule 2 (SaaS/ATS) and Schedule 4 (VIDEO INTERVIEW SERVICE) of the terms and conditions. For the avoidance of doubt this data processor agreement shall only take effect if customer has ordered and used service defined in these schedules of the terms and conditions.

(2) Duration of this Order or Contract corresponds to the duration of the Service Agreement.

2 Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data

Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the Supplier: The purpose of the processing within the Video Job Interview Service is to transmit the Video Interview created by the applicant to the customer.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

(2) The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)
   - For Video Interview:
     o Recordings of video interviews, video pitches and live interviews
     o Personal data of the client's candidates (candidate name and email address and video are stored). Depending on the interview set up by the Controller (pursuant Schedule 4 section 1 in the terms and conditions).

   - For ATS
     o The Supplier operates the applicant tracking system Candidate Manager where candidates can apply for a vacant job with Client. The processing of Personal Data necessary and incidental to the provision of the Candidate Manager Applicant Tracking Software by the Supplier to the Client.

   - The category of Data Subjects whose Personal Data is processed in the context of performing:
     o Video Interview: are applicants, who apply to the Controller as well as employees of the Controller who act as an interviewer. In addition, the communication data of Controller's contacts will be processed.
     o ATS: Application data, such as First Name, Last name, Address, Email, Phone number, CV and optionally Education, Work experience, Visa status, References,

4023.9032.5023006v2

Cover letter, if the applicant is over 18, answers to scenario based questions and any other personal data an applicant provides in the application or documents submitted therewith.

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Appendix technical and organizational measures]

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

The Supplier has appointed a data protection officer who can be contacted under info@candidatemanger.net. The Client shall be informed immediately of any change of Data Protection Officer. Contact details are always available and easily accessible on the website of the Supplier.

Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

a. Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in section technical and organizational measures].

b. The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

c. The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

d. Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

e. The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

f. Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) If Supplier intents to use a new Subprocessor supplier will inform the client prior the implementation. New Subprocessors shall be deemed as agreed if Client does not object the use of new subprocessors within 4 weeks after notification. Client shall not have the right to object the new use of subprocessors without good cause and shall justify his concerns. If Client objects the new Subprocessor and if it is not possible to offer the service without the new subprocessor, the Client shall not use the service anymore.

a) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR: StepStone GmbH, Axel- Springer-Str. 65, 10969 Berlin, Hosting and performance of the service.

b) StepStone Continental Europe GmbH, Völklinger Straße 1, 40219 Düsseldorf, Germany for the provision of hosting and associated security services

c) Akamai Technologies GmbH, Parkring 20-22, 85748 Garching, Germany who additionally use Akamai Technologies, Inc, 150 Broadway, Cambridge, 02142 MA, USA as further processor as

a web application firewall and in this context the analysis of traffic data to identify malicious web traffic.

    d) Amazon Web Services, Inc, 410 Terry Drive Ave North, WA 98109-5210 Seattle, USA providing hosting services (in the EU)

    e) StepStone N.V., Koningsstraat 47 Rue Royale, 1000 Brussels, Belgium providing hosting and associated security services

    f) Esendex, 20 Wollaton Street, Nottingham, NG1 5FW , provide SMS service (*only applicable if client uses this service)*

    g) NIJobs.com Limited, Suite 2A, Cadogan House, 322 Lisburn Road, Belfast, BT9 6GH, consultation

    h) Cammio GmbH, Philipp-Franck-Weg 19, 14109 Berlin, Germany, performance of video interview platform

    i) Outsourcing to subcontractors or changing the existing subcontractor are permissible when:
- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subprocessor and the subprocessors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subprocessor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

If supplier transfers personal data outside of the EU/EEA and has entered into model clause with the subcontractor the client joins the Standard Contractual Clauses entered into by Supplier and the Subprocessor as an independent owner of rights and obligations ("Accession Model").

(5) Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor or a suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

   a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
   b) The obligation to report a personal data breach immediately to the Client
   c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
   d) Supporting the Client with its data protection impact assessment
   e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Appendix - Technical and Organisational Measures

4023.9032.5023006v2

Confidentiality

All data is hosted within AWS data center which is ISO 27001 certified and state of the art, utilizing innovative architectural and engineering approaches. Data centers are housed in nondescript facilities. Physical access is strictly controlled by professional security staff utilizing and video surveillance, intrusion detection systems, and other electronic means. Only authorized staff can enter buildings using MFA to enter data center floors. Authorized visitors are required to present identification and are signed in and continually escorted by authorized staff.

Secure VPN, MFA (multi-factor authentication), and role-based access is enforced for systems management by our DevOps team. User data is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. We set a session cookie only to record encrypted authentication information for the duration of a specific session. Passwords are individually salted and hashed. Brute Force protection: 3 incorrect attempts = 60 minutes lockout.

API interfaces are only privately accessible and protected by security credentials.

Additionally, MFA can also be used for recruiter users to add an extra layer of security. The end user can choose to receive the security code using text messages or use a standard One-Time-Password (OTP) app such as Google Authenticator.

Access control to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. We use AWS Identity and Access Management (IAM) to manage access to all services and resources securely. AWS users and groups have been configured with dedicated permissions to allow or deny access to the resources. Central logging systems capture and archive all internal systems access, including any failed authentication attempts. Transmitted data is tracked and logged.

Candidate data is only stored for as long as is necessary for the purpose of video interviews. Automatic processes ensure that candidate subject data is deleted entirely from the system when a retention period is reached. This is an irreversible process. Database records are anonymised to allow for continuous statistics monitoring. No customer or candidate data is stored on portable media devices.

Data of Client is logically separated; we use an internal multi-tenant architecture. File names used are fully obscured and anonymised and cannot be directly related to data subjects.

All data storage is encrypted. The platform provides a separate development sandbox environment. All test data is fully separated from live data. Production data is not used during develop and test processes. Production data can not be copied to other environments.

Integrity

Logging, Intrusion detection and IP Restrictions and VPN access

All user interactions, including logins, are stored in system-based logs. Logs are stored on AWS storage using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. Several techniques are in place to prevent unauthorised access. All resources require proper user authorisation to access data. All systems are protected by AWS firewalls and other best practices related to infrastructure security. Web Access Firewall (WAF) mitigates the risk of SQL injection threads. Administrative operational tasks can only performed from known IP addresses. VPN tunnels and MFA are used to gain access to the infrastructure configuration by the DevOps team. Data is encrypted at rest and in transit using server-Side Encryptions (SSE) using AES-256 encryption at rest and TLS 1.2 in transit.

Availability

4023.9032.5023006v2

Hosting within ISO 27001 certified data centers including support for repairing, replacing and refreshing the infrastructure. Contractual agreements with ISPs to provide Internet connectivity that can sustain bandwidth utilisation under full load Server capacity to run mission-critical services, including storage appliances and other services. Fire detection and suppression equipment installed to reduce the risk of fire.

Highly durable storage redundantly stored on multiple devices across multiple facilities.

Further protection for data retention and archiving through versioning in Amazon S3, AWS multi-factor authentication (AWS MFA), bucket policies, and AWS Identity Management (IAM).

Scheduled snapshots of data volumes are created to protect the data from loss in case of a disaster.

The snapshot off-instance storage persists independently from any instance and is replicated across multiple servers to prevent the loss of data from the failure of a single component. Rapid recovery through virtual machines.

AWS provides fully redundant IP network connections with multiple independent connection to a range of Tier 1 Internet access providers. AWS Route53 is used as scalable DNS web service. We make use of Elastic IP, which are static IP's that can be remapped do other instances.

Routine, emergency, and configuration changes to existing infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems.

When conducting updates on the Cammio infrastructure, we try and ensure limited impact on the customer and their use of the services.

We have a continuous development cycle where we develop, test and deploy changes on a regular basis without any fixed intervals. Development, testing and production environments are clearly separated. Usually a deployment to our production environment does not result in any system downtime.

Procesures for regular testing assessment and evaluation
All employees authorised to access personal data have received relevant technical and security trainings.

We maintain internal information security policies including incident response plans and regularly review and update them. Our engineers use best practices and industrystandard secure coding guidelines. Environments are scanned on a regular basis using breed security tools, vulnerability assessments and penetration test.

Continuous monitoring of service system and capacity utilisation is deployed.

Backup concepts, Recovery of IT systems. We periodically test our data