Cornerstone OnDemand – Licenses Terms (Agreement)

1. Definitions.
   1.1 "**Affiliate**" means a party that partially (at least 50%) or fully controls, is partially or fully controlled by, or is under partial (at least 50%) or full common control with, another party.
   1.2 "**Customer Content**" means any and all courses, learning objects, certifications, quizzes, tests, materials, instructor-led sessions, documents, or URLs created and/or introduced by Customer or its Affiliates that reside in the Software.
   1.3 "**Customer Data**" means personal data regarding Customer's or its Affiliates' Users which is uploaded to the Software pursuant to this Agreement.
   1.4 "**Documentation"** means the standard online functional documentation available for the Software.
   1.5 "**Order**" means a purchase made by Customer hereunder in an order, schedule, statement of work, addendum, or amendment signed by both parties.
   1.6 "**Services**" means any services rendered by Cornerstone to Customer, including, but not limited to: (i) hosting and making available the Software; (ii) hosting, delivery, and/or distribution of eLearning content; (iii) provision of technical support for the Software; and/or (iv) consulting, assistance or training services, each as specified on an Order.
   1.7 "**Software**" means (i) any and all of Cornerstone's and its Affiliates' proprietary web-based applications, including, without limitation, all updates, revisions, bug-fixes, upgrades, and enhancements thereto; and (ii) application functionality and eLearning content provided by Cornerstone and/or Cornerstone-contracted third parties.
   1.8 "**User**" means an individual with credentials issued by Customer to log on to the Software and with a designation of "*active*" unless otherwise described in the applicable Order. Users may be employees or non-employees.
2. Rights; Usage. In accordance with the terms and conditions of the Agreement, Cornerstone gives Customer the non-transferable and non-assignable right for the duration of applicable Orders to use, and to permit its and its Affiliates' Users to use, the Software items listed therein on a non-exclusive basis via the Internet, subject to the maximum quantities set forth therein. Cornerstone may review Customer's compliance with the terms of each Order and, for clarity, reserves the right to charge for any quantity overages.
3. Use Restrictions. The Software and Services may be used only for Customer's and its Affiliates' own lawful business purposes. Customer shall not: (a) use or deploy the Software in violation of applicable laws or this Agreement; (b) store, process, publish or transmit any threatening, infringing or offensive material, or material that constitutes a security risk or a violation of any party's privacy, intellectual property or other rights; (c) resell any Software or Services or operate a service bureau, outsource, rent, sublicense or use in a time-sharing capacity except as expressly permitted by Cornerstone; (e) create any derivative works based upon the Software; (f) reverse engineer, reverse assemble, decompile or otherwise attempt to derive source code from the Software or any part thereof (except to the extent that such restriction is not permitted under applicable law); (g) upload any data not required to use the Software as generally intended; (h) make any Software or Services available to any unauthorized parties; (i) perform penetration or similar tests (for example, network discovery, port and service identification, vulnerability scanning, password cracking or remote access testing) on the Software or Services; or (j) publicly release the results of benchmark tests or other comparisons of any Software or Services with other software, services, or materials. Customer will be responsible for Users' compliance with the Agreement and liable for Users' breach thereof. In the event of a breach of any of the foregoing prohibitions, Cornerstone reserves the right to suspend access to the Software, to the extent and for so long as reasonably necessary, to prevent harm to Cornerstone, Customer, other Customers, and/or Cornerstone's partners, vendors and suppliers with such notice as may be reasonable in the context of the prospective harm. Customer will ensure that it has obtained all necessary consents and approvals for Cornerstone to access Customer Data for the purposes permitted under this Agreement. Upon expiration or termination of this Agreement, Customer shall cease using all Software and Services.

   Cornerstone shall have a royalty-free, worldwide, perpetual, irrevocable license to use or incorporate into the Software and Services any suggestions, ideas, enhancement requests, feedback, recommendations, or other information provided by Customer or its users relating to the operation of the Software and Services.
4. Statistical Data. Without limiting the confidentiality rights and intellectual property rights protections set forth in this Agreement, Cornerstone has the perpetual right to use aggregated, anonymized, statistical data ("**Statistical Data**") derived from the operation of the Software, and nothing herein shall be construed as prohibiting Cornerstone from utilizing the Statistical Data for product optimization, improving Customer experience and other internal business and/or operating purposes, provided that Cornerstone does not share with any third party Statistical Data which reveals the identity of Customer, Customer's users, or Customer's Confidential Information.

5. Privacy and Security. Cornerstone will: (a) according to ISO 27001 and 27701 (or successor/equivalent) standards and solely its own security policies, maintain appropriate safeguards for protection of Customer Data, including regular back-ups, security and incident response protocols, and application and infrastructure monitoring; (b) process Customer Data in accordance with the parties' then-current data processing agreement, and applicable data protection laws and regulations to which it is subject; and (c) not access, modify, or disclose Customer Data, except as compelled by law, to prevent or address service or technical issues, or if otherwise permitted by Customer. Customer may retrieve Customer Data any time during the term of the Agreement. If requested, at a scope and price to be agreed, Cornerstone will assist with such data retrieval.
6. Support. Cornerstone shall provide the technical support stated in the applicable Order. Only the number of administrators set forth in the applicable support package description (i.e., not all Users) who have completed the requisite training may contact Cornerstone for support. Customer agrees to promptly provide Cornerstone with sufficient documentation, data and assistance with respect to any

reported errors, and to reasonably cooperate with Cornerstone, in order for Cornerstone to comply with its support obligations hereunder. In no event shall Cornerstone be responsible or liable for any errors, bugs or other problems contained in or originating from hardware or software not provided by Cornerstone. Should use of the Software result in denial of service (DoS) with respect to the Software, Cornerstone may disable the implicated Customer Content and/or suspend access to the Software only if and for so long as necessary to restore service. Cornerstone may give general notices applicable to all of its customers by means of a notice on the portal for the Services,

8. Intellectual Property. As between the parties, (i) Customer retains all proprietary and intellectual property rights, title and interest in and to Customer Data and Customer Content and (ii) Cornerstone, its Affiliates and suppliers will and do retain all proprietary and intellectual property rights, title and interest in and to the Software and Services.
9. Warranties.
   a) Cornerstone warrants that the Software will perform substantially in material accordance with the Agreement and applicable Documentation regarding existing functionality provided by Cornerstone; no new or different functionality is promised hereunder.
   b) In the event of a breach of the warranty set forth in Section 11.2, Customer's sole and exclusive remedy will be that Cornerstone shall, upon receipt of written notice of breach, make diligent efforts to become compliant with the warranty set forth in Section 11.2, and if Cornerstone does not do so within a reasonable period of time, Customer will be entitled to terminate this Agreement.
   c) To the extent permitted by applicable law, Cornerstone disclaims all other warranties, express or implied, statutory or otherwise, including without limitation warranties of merchantability, fitness for a particular purpose, and any warranties arising from a course of dealing, usage or trade practice. Cornerstone does not warrant that the services will be uninterrupted or error-free.
10. Miscellaneous Provisions.
    a) Third-Party Applications and Service Providers.
       i) External Applications. Cornerstone shall not be responsible for Customer's access to, or operation of, third-party applications purchased separately by Customer from a third party, including without limitation those that may be capable of interoperating with the Software.
       ii) Optional Features. Cornerstone's Software may include certain optional features provided by third parties ("**Optional Features**"). A list of such Optional Features, including information regarding the security, privacy, and/or support policies of those third parties, is available upon request.
       iii) Service Providers. Cornerstone has certified a select group of third-party service providers that implement, configure, and/or administer Software ("**Certified Consultants**"). A list of Certified Consultants is available upon request. Customer may not permit any non-Certified Consultant to implement and/or configure Software. None of the warranties or support obligations hereunder shall apply to any Software implemented or configured by any non-Certified Consultant.

    b) Trade Controls. Customer understands that use of the Software and Services is subject to export controls, trade and economic sanctions, and anti-boycott laws and regulations to which the parties or Software and Services may be subject. Customer shall not, and shall not permit users of the Software and Services to, access or use the Software or Services in violation of any such laws and regulations, including, without limitation, the Export Administration Regulations maintained by the U.S. Department of Commerce, and the trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control.

DATA PROCESSING ADDENDUM

BETWEEN

[CUSTOMER/BUYER NAME] (“CUSTOMER” OR “CLIENT”)

AND

[CORNERSTONE/SUPPLIER NAME] (“CORNERSTONE”)

Preamble

This Data Processing Addendum (the "**Addendum**") forms part of and is subject to the terms of the master agreement (or similar designation) executed by Customer and Cornerstone (the "**Master Agreement**") concerning the provisioning of human capital management software by Cornerstone (hereinafter also the "**Processor**") to Customer (hereinafter also the "**Controller**"). It applies to all activities carried out by the Processor within the framework of the Master Agreement whereby the Processor's employees or third parties commissioned by the Processor might Process Personal Data of the Controller and/or its users. In the event of any conflict between the terms of the Master Agreement and the terms of this Addendum, the terms of this Addendum shall prevail.

1 Definitions

Capitalized terms used, but not otherwise defined, herein shall have the same meanings assigned to those terms in the Master Agreement.

1.1 "**Data Protection Legislation**" means any privacy and data protection law or regulation to which Cornerstone is subject as a data processor when providing the Services to the Customer as amended from time to time, such as but not limited to Regulation (EU) 2016/679 of 27 April 2016 (GDPR), the U.K. Data Protection Act 2018, the UK General Data Protection Regulation (Regulation (EU) (2016/679)) (UK GDPR), .

1.2 "**Personal Data**" means any information Processed by Cornerstone on behalf of Customer relating to an identified or identifiable natural person.

1.3 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.4 "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2 Scope of the Addendum

Cornerstone acts as a processor for Customer, who acts as the controller. Personal Data may include the categories of Personal Data, the categories of data subjects and the purposes of the Processing set out in Annex 1.

3 Processing of Personal Data

3.1 Cornerstone shall Process Personal Data for the purposes of providing services under the Master Agreement only in accordance with the Master Agreement and this Addendum, and in accordance with documented instructions listed in this Addendum and the Master Agreement. Customer may issue further documented instructions consistent with and in the scope of this Addendum and the Master Agreement. Cornerstone shall immediately inform Customer if, in Cornerstone's opinion, an instruction infringes Data Protection Legislation. In case Cornerstone is required to Process Personal Data by Data Protection Legislation to which Cornerstone is subject, Cornerstone shall inform Customer of that legal requirement before Processing, unless that law prohibits such informing on grounds of important public interest.

3.2 Cornerstone must limit the access to Personal Data to its employees and Subprocessors for whom access to said data is reasonably necessary to fulfill Cornerstone's obligations to Customer. Cornerstone must ensure that persons authorized to Process Personal Data are bound by the same

or equivalent confidentiality obligations as Cornerstone and/or are under an appropriate statutory obligation of confidentiality.

3.3 Cornerstone shall implement and maintain appropriate technical and organizational measures in line with Data Protection Legislation. For this purpose, the parties agree on the security measures set forth in Annex 2 for the Processing of Personal Data.

3.4 The appropriate technical and organizational security measures must be determined with due regard to:

(i) the state of the art,
(ii) the cost of their implementation, and
(iii) the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

3.5 Cornerstone shall make available to Customer upon request information necessary to demonstrate compliance with Processor's obligations set forth in Data Protection Legislation, and allow for and reasonably assist with audits, including inspections, conducted by the Controller or an independent third party auditor appointed by the Controller, as follows:

(i) Cornerstone shall at its own cost obtain and make available upon Customer's request an audit report from an independent auditor regarding Cornerstone's compliance with the data security requirements of the controls defined in SSAE 18 or ISO 27001 (or equivalent standard). Such audit report must be issued on the basis of a recognized standard for such reports.

(ii) In addition, Customer is entitled, at a time and scope to be agreed by the parties, to conduct or have conducted an annual audit, including an inspection, if and to the extent the audit report set forth in the preceding paragraph does not meet the requirements set forth in Data Protection Legislation. Any third party auditor shall not be a competitor of Cornerstone, and shall, upon Cornerstone's request, sign a customary non-disclosure agreement to treat all information obtained or received from Cornerstone confidentially, and may share any such information obtained or received only with Customer and Cornerstone. Customer shall be responsible for costs of the audit, and agrees to pay Cornerstone a reasonable fee per audit to be mutually agreed by the parties to cover Cornerstone assistance with the audit. An additional audit may take place: (i) if required by a competent legal supervisory authority of Customer; or (ii) following a Personal Data Breach.

3.6 Cornerstone shall without undue delay, unless such notification is prohibited under applicable law, notify Customer about any:

(i) request by a legal authority for disclosure of Personal Data Processed under the Agreement; or

(ii) request for access to Personal Data received regarding an identified data subject.

3.7 Cornerstone shall notify Customer without undue delay after becoming aware of a Personal Data Breach. The notification shall at least describe the nature of the Personal Data Breach (including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned) and the measures taken or proposed by Cornerstone to address the Personal Data Breach.

3.8 Cornerstone shall provide reasonable and timely assistance to Customer to help enable Customer to respond to: (i) any request from a data subject to exercise any of the data subject's rights under applicable data protection laws (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the Processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Cornerstone, Cornerstone shall promptly inform Customer and provide full details of the same, except to the extent prohibited by law.

3.9 Cornerstone shall, upon Customer's request, reasonably assist the Controller in ensuring compliance with Controller's obligations under applicable Data Protection Legislation (including security of Processing, notification of Personal Data breach, data protection impact assessment and prior consultation), based on the nature of Processing and the information available to Cornerstone

3.10 In the event Customer's designated account manager at Cornerstone cannot assist with a data privacy enquiry, Customer may contact Cornerstone's data protection officer at dpo@csod.com.

3.11 Assistance contemplated by this Section 3 shall be provided to Customer at no charge if the request can be fulfilled by providing information via Customer's portal and/or by supplying readily available documentation in Cornerstone's possession.

4 Customer's General Obligations

Customer will comply with all its obligations under applicable data protection laws and regulations.

5 Other Data Processors

5.1 Cornerstone may engage other processors (each a "**Subprocessor**") for the Processing of Personal Data under this Addendum, provided Cornerstone ensures such Subprocessors' compliance with the terms of this Addendum. As of the effective date of the Addendum, Cornerstone relies on the Subprocessors listed in the Order as well as on https://trustcenter.cornerstoneondemand.com/ to provide the Services.

5.2 Prior to the engagement of another Subprocessor, Cornerstone shall inform Customer's administrator and Customer's contact registered on https://trustcenter.cornerstoneondemand.com/ of the intended subprocessing at least 30 days prior thereto, thereby giving Customer the opportunity to object to such change on reasonable grounds.

5.3 Customer authorizes Cornerstone to transfer Personal Data to Cornerstone Affiliates and/or other Subprocessors located in locations outside the European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the Master Agreement, provided that, to the extent applicable, either: (i) such locations are recognized by the European Commission and/or the UK as providing adequate data protection or (ii) Cornerstone has executed Processor to Processor EU or UK (as applicable) Standard Contractual Clauses with such required Affiliates and/or other Subprocessors including where appropriate supplementary measures.

5.4 Cornerstone shall remain fully liable to Customer for the performance of its Subprocessors' obligations hereunder.

6 Data Retrieval and Deletion

6.1 Customer may retrieve its Personal Data at any time prior to termination of the Master Agreement as set forth therein.

6.2 Promptly upon the expiration or earlier termination of the Master Agreement, or earlier upon Customer's request, Cornerstone shall securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Cornerstone's possession, custody or control.

6.3 Notwithstanding section 6.2, backups of Personal Data are to be deleted according to and in compliance with Cornerstone's general backup cycle, which means that backups will be deleted at the latest within approximately six (6) months from the decommissioning of Customer's portal, which occurs generally within 30 days following termination or expiration of the Agreement.

6.4 Cornerstone shall provide to Customer, upon Customer's request, written confirmation that deletion has occurred in accordance with this section 6.

6.5 In the event applicable law does not permit Cornerstone to comply with delivery or destruction of Personal Data as set forth herein, Cornerstone shall ensure the privacy, confidentiality and security of Personal Data in accordance with the standards agreed in this Addendum and shall not use or disclose any Personal Data after termination of the Master Agreement.

7 Miscellaneous

The parties may agree in good faith on any reasonable amendment to the Addendum required to maintain compliance with the applicable law. Such amendment may include additional fees to be reasonably agreed by the parties.

Agreed and accepted:

Customer		**Cornerstone**	
Signature:		Signature:	
Name:		Name:	
Title:		Title:	
Date:		Date:	

Approved as to form:

ANNEX 1

I. Categories of data, categories of data subjects and purposes of the Processing

a) Categories of Personal Data

The Personal Data being Processed by Processor may concern the following categories of data:

- Learning, performance, recruiting, and/or HR data

b) Categories of data subjects

The Personal Data Processed by Processor may concern the following categories of data subjects:

- Employees, suppliers, contractors, agents, directors, officers, customers, members, and/or partners of the Controller and/or its affiliates

c) Purpose and nature of the Processing operations

Personal Data may be Processed by Processor for the following purposes:

- Delivery and use of human capital management software;
- Implementation services related to configuration of human capital management software;
- Product support; and
- Technical projects

as further described in Processor's audit reports and IT security policy.

d) Special categories of data

None.

ANNEX 2

Security measures

(1) Processor shall Process Personal Data in accordance with applicable law to which Processor is subject and in accordance with the data security requirements of the controls defined by latest available SSAE 18 SOC 2 or ISO 27001 implemented controls (or equivalent standard).

(2) Processor shall appoint a fixed contact point for Customer to carry out any matters in relation to the Processing of Personal Data.

(3) Processor shall ensure that Processor's employees receive adequate training and instructions, including, but not limited to, education on general safety awareness, relevant security policies and procedures, and Personal Data Processing.

(4) Processor shall maintain organizational and technical measures to ensure separation of data between clients and systems.

(5) Access Control of Processing Areas

Processor shall maintain suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data is Processed or used. This is accomplished by measures like:

- establishing security areas;
- protection and restriction of access paths;
- securing the decentralized telephones, data Processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations on card-keys;
- restriction on card-keys;
- all access to the data centre where Personal Data is hosted is logged, monitored, and tracked;
- the data centre where Personal Data is hosted is secured by a security alarm system; and
- other appropriate security measures.

(6) Access Control to Data Processing Systems

Processor shall maintain suitable measures to prevent its Personal Data Processing systems from being used by unauthorized persons. This is accomplished by measures like:

- identification of the terminal and/or the terminal user to the Processor systems;
- automatic time-out of user terminal if left idle, with identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered;
- log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;
- dedication of individual terminals and/or terminal users, and identification characteristics exclusive to specific functions;
- employee policies and training with respect to each employee's access rights to Personal Data (if any), including informing employees about their obligations and the consequences of any violations of such obligations, to ensure that employees will only access Personal Data and resources required to perform their job duties; and
- all access to data content is logged and monitored.

(7) Access Control to Use Specific Areas of Data Processing Systems

Processor commits that the persons entitled to use its Personal Data Processing system are only able to access the data within the scope and to the extent covered by its access permission (role or authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- employee policies and training with respect to each employee's access rights to the Personal Data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of Personal Data only to authorized persons;
- control of files, controlled and documented destruction of Personal Data; and
- policies controlling the retention of back-up copies.

(8) Availability Control

Processor shall maintain suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy;
- tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for database server;
- complying with Processor's business continuity policy; and
- any detected security incident is recorded.

For all applications supported by the Processor, the following controls will be implemented:

(9) Transmission Control

Processor shall maintain suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of industry standard firewall and encryption technologies to protect the gateways and pipelines through which the data travels (e.g. TLS/SSL);
- encryption of certain highly confidential data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) within system transmission; and
- logging relevant security metadata for data transmissions.

(10) Input Control

Processor implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into Personal Data Processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and disposal of stored Personal Data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and disposal of stored Personal Data;

- utilization of user codes (passwords);
- following a policy according to which all employees of Processor who have access to Personal Data Processed for Customer shall reset their passwords at a minimum once in a 180 day period, or as defined in Processor's IT Security Policy and in line with potential multi-factors of authentication;
- providing that entries to Data Processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user IDs that have not been used for a substantial period of time;
- proof established within Processor's organization of the input authorization; and
- electronic recording of entries.

(11) Processor system administrators (if any):

Processor shall maintain measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by importer and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

(12) Separation of Processing for different Purposes

Processor shall maintain suitable measures to ensure that Personal Data collected for different purposes can be Processed separately. This is accomplished by:

- access to Personal Data is separated through application security for the appropriate users; and
- modules within Processor's database separate which data is used for which purpose, i.e., by functionality and function.

Customer acknowledges and agrees that Processor may change its security policies and related security measures, provided that Processor maintains, at all times, an overall level of security at least as stringent as the one set forth in this Addendum.

Supplementary License Terms for requested additional Software or Content

In the event the Customer/Buyer purchases "EasyGenerator" licenses, the following Licensing terms shall apply *:*

Easygenerator ("Easygenerator") is a functionality provided by Easygenerator LLC-FZ, a third-party provider. Original content created by Customer using Easygenerator will be deemed Customer Content. Any proprietary Cornerstone or Cornerstone contracted third parties content as adapted or modified by Customer using Easygenerator will be deemed Software. Easygenerator LLC-FZ may process personal information only as necessary to provide the Easygenerator functionality including from countries outside the European Economic Area and United Kingdom. The applicable security and privacy policies of Easygenerator LLC-FZ as well as the list of its subprocessors are available upon request.

In the event Buyer/Customer purchases Content

Some Content is hosted by third-party content providers. These providers may process personal information (e.g., Active User identification, course tracking, etc.) only as necessary to provide the Content in accordance with AICC, SCORM, or equivalent standards. The list, locations, and security and privacy policies of such providers are available upon request.

Purchased course(s) shall be available from the Effective Date, through the earlier of: (i) the agreed end date for content; or (ii) termination/ expiration of the Agreement as a whole; after which time all access / course registrations shall be terminated or expire without refund. Course loading and hosting services are included as a part of this purchase. Content subscriptions are non-transferable; they are unique to individual users. Notwithstanding the foregoing, where Customer has purchased the Enterprise Content subscription, these subscriptions may each be reassigned one time per year. Subject to the foregoing. Cornerstone reserves the right to invoice Clients automatically for each subscription/registration exceeding the number purchased, based on the total Content price set forth in this Agreement, divided by the total number of Active Users subscribed to/registered for that Content.

Following additional services can be purchase in combination with TalentLink subject to additional License and the conditions terms below:

Cornerstone TalentLink Insight – by QlikTech

Cornerstone offers reporting solutions through its partnership with QlikTech UK Limited, 1020 Eskdale Road, IQ Winnersh, Wokingham,
RG41 5TS, United Kingdom ("QlikTech"). Insight delivers data in a way that intuitive and effective analytics can easily be built for Customer's business requirements based on Customer's data. Customer will have the Insight Standard offering. Optionally Customers can purchase Insight Premium.

- **Insight Access:** Cornerstone offers the ability for Customers to connect to their data mart in order for the Customer to build their own reports using their own BI tool “Insight Access”. The data mart has a daily data refresh. The data mart is built upon Amazon Cloud services, using Amazon RDS. Custom views of the data can be built for the Customer for an additional charge.

Cornerstone TalentLink Distribute – by eQuest

Cornerstone offers a job distribution service (“Cornerstone TalentLink Distribute by eQuest”) through its partnership with eQuest LLC, 2010 Crow Canyon Place, M/S 100-10016, San Ramon, Califor-nia 94583 USA (“eQuest”). The Job Distribution Service allows the Customer to post job requisitions to a number of job boards using one interface. The amount of job requisitions that can be posted is unlimited. If a Customer wishes to use this solution to post to a job board that is not supported by the eQuest interface, then this will be handled manually; the price and invoicing interval for such manual handling is outlined in the applicable Order

Cornerstone TalentLink Source – by Textkernel

Cornerstone offers an intelligent search functionality to find relevant candidate profiles through its partnership with Textkernel B.V., Nieuwendammerkade 26a5, 1022 AB Amsterdam, Netherlands (“Textkernel”). The Customer can choose from the following bundles (of increasing functionalities), precisely:

- **Source External:** allows you to search social media such as LinkedIn, Viadeo and Xing, and job sites such as Career Builder or CV Library to help you find the right candidate.No data from these external sources will be integrated into the Software and no Cus-tomer data will be transmitted to these networks and/or cv databases. To fully use this functionality some networks or data bases do require a standalone contract with such network or cv database.

SERVICE LEVEL AGREEMENT TALENTLINK

CONTENTS

1. DEFINITIONS
2. SERVICE AVAILABILITY
3. INCIDENT MANAGEMENT
4. MAINTENANCE AND RELEASES
5. TECHNICAL SERVICES
6. ACCEPTABLE USE POLICY

1 DEFINITIONS

All defined terms in this SLA shall have the meaning set out in the Agreement and Order, unless specified otherwise below.

"**Agreed Service Time**" means absolute total minutes within a month minus total minutes Scheduled Maintenance in this month;

'Availability of the Software' means that the Software is accessible for the Customer to use as set out in section 2.1 below. Any planned maintenance shall be excluded from the calculation of Availability of the Software;

'Defect' means an error that causes unexpected behaviour against the design of the Software;

'Disaster' means that the hosting centre where the Software is hosted becomes unusable with no expected resolution date/time;

'**Incident**' means an event whereby the Software is not operating as expected, and (if raised by the Customer) notified to Company in accordance with clause 3.2 below;

'**Patch**' means a mechanism for delivering a minor change to the Software;

'**Release**' means a change or enhancement in the functionality of the Software and/or the delivery of new features and functionality, or amended features and resolutions to Defects;

'Scheduled Maintenance' means the scheduled and/or preventative maintenance performed during the Scheduled Maintenance Window;

'Scheduled Maintenance Window' means the time between the hours of 00:00 and 05:00hrs (GMT/BST) every Sunday;

'**Support Day(s) & Hour(s)**' means Monday to Friday 08:00 to 18:00 hours local time in the country given in the Company's address on the Order (excluding any local public holidays);

2 SERVICE AVAILABILITY

2.1 Service Commitment

Company will take all reasonable measures in terms of redundancy, monitoring and platform management to provide Availability of the Software.

Availability of the Software through the internet shall be 99.9 % of the Agreed Service Time. The Availability of the Software is calculated per calendar month and measured based on the successful completion of the following transaction:

- Loading the Software login page for user access;
- Loading to the Software management account;
- Logout from the Software;

A transaction is deemed successful when the above is completed without error or timeout as measured by an external automated 'end to end' transaction response time monitor provided by a 3rd party monitoring service. Actual service time is calculated by the monitoring service based on the frequency of successful transaction attempts within the service period to be measured.

Availability of the Software is calculated as minutes Actual Service Time per month divided by the minutes Agreed Service Time within a month and expressed as a percentage.

Using January, a 31 day month, as an example with 40 minutes of reported downtime:

- Absolute total minutes within the month = 31 days x 24 hours x 60 minutes = 44,640 minutes

- Total minutes identified downtime = 40 minutes
- Total minutes of Scheduled Maintenance = 60 minutes
- Agreed Service Time = 44,640 minutes – 60 minutes = 44,580 minutes
- Actual Service Time = 44,580 minutes – 40 minutes = 44,540 minutes

- 44,540 minutes (Actual Service Time) / 44,580 minutes (Agreed Service Time) x 100 = 99.9% (Availability of the Service)

The following service credits shall apply if the Availability of the Software is less than 99.9 %:

Availability of the Service (per month)	Service credit
between 99.8 and 99.89 %	3 %
between 97 and 99.79 %	6 %
between 96 and 96.99 %	9 %
between 95 and 95.99 %	12 %
less than 95 %	15 %
less than 90 %	40 %

Service credits are expressed as a percentage of the monthly subscription fee. A Customer must make a claim for any service credit due within 60 days of notification of entitlement to such service credit. Service credits will be credited to the next invoice issued to the Customer after the claim.

3 INCIDENT MANAGEMENT

3.1 Support Coverage

Customer support for the Software is provided during Support Days & Hours. Access to Customer support is provided for up to four named Customer contacts. Contacts can be updated or changed by contacting your account manager. Customer support can be provided in English, French and German.

3.2 Incident Notification

Incidents should be reported and tracked using:

- The support community portal https://www.cornerstoneondemand.com/community-and-support/ or
- Telephone https://www.cornerstoneondemand.com/community-and-support/
- Outside of Support Days & Hours, the Customer may, for severity 1 issues (as defined below), invoke the emergency services by telephoning the local support number for their region and following the instructions given.

Company will review the severity level assigned and may change it in consultation with the Customer, to a higher or lower severity, if it is reasonable to do so. The Customer may track and update the progress of issues via the support community portal or by telephone.

3.3 Security Incident Notification

In the event of a data security breach affecting the Customer, Company will notify the primary Customer contact noted in the community portal without undue delay after the information security office of Company is made aware of such a breach.

3.4 Incident Commitment

All Incidents are assigned a unique case reference number and categorised by severity according to the following definitions:

SEVERITY 1 – Service unavailable	
Definition	Critical production issue affecting all users, including infrastructure failure, Software unavailability or data integrity issues with no work-around available.
Response	Company will respond within 1 (one) hour, emergency support will be in English.
Service level commitment	Company will provide continuous support (24 x 7) until a resolution has been delivered or a work-around implemented.

SEVERITY 2 – Critical	
Definition	A severe business impact affecting many users, limiting the usage of one or more major functions of the Software or causing performance degradation. The Software are operational, but restricted.
Response	Company will respond within 2 (two) Support Hours.
Service level commitment	Company will provide continuous support during local Support Hours until a resolution has been provided or a work-around implemented. If the problem is determined to be a Defect and a Patch is required, this will be progressed during the working hours of the assigned development centre, located in EMEA.

SEVERITY 3 – Major	
Definition	The Software are operational, but there are functional limitations or errors that are not critical for daily business.
Response	Company will respond within 1 (one) Support Day.
Service level commitment	Company will work during Support Hours until a resolution has been provided or a work-around implemented. If the problem is determined to be a Defect, it will be targeted for correction in the next available Release.

SEVERITY 4 – Minor	
Definition	Minor Incident affecting a small number of users, technical inquiry or 'how to' question relating to Software functionality.
Response	Company will respond within 2 (two) Support Days.
Service level commitment	Company will work during Support Hours until a resolution has been provided or a work-around implemented. If the problem is determined to be a Defect, this will be considered for correction in a future Release.

4 MAINTENANCE AND RELEASES

4.1 Maintenance

Resolutions to Defects and essential data centre infrastructure and/or Software platform work will be conducted during a Scheduled Maintenance Window.

During the Scheduled Maintenance Window, the Software and some or all Services may be unavailable.

Company reserves the right to:

i) Change the timing of a Scheduled Maintenance Window;
ii) Permanently change the Scheduled Maintenance Window;
iii) Perform urgent preventative maintenance activities outside of the Scheduled Maintenance Window to ensure the continuity of the Software.

In all cases, Company will provide the maximum amount of advance notice possible for changes to the Scheduled Maintenance Window.

4.2 Releases

Releases contain new features and enhancements, as well as resolutions for any known software Defects. There may be some need for configuration and additional user training in order to obtain the maximum benefit of a Release. Documentation will be made available to Customers via the Cornerstone community portal.

Company reserves the right to issue Releases outside of Scheduled Maintenance. Company agrees to provide at least 30 days' prior notice for any scheduled Release that may result in unavailability of the Software. Company reserves the right to issue periodic Releases that correct product defects or performance issues deemed urgent by Company. Company will provide the maximum amount of advance notice as possible for such periodic product Releases.

5 TECHNICAL SERVICES

5.1 Data Centres

The Software is currently hosted in Australia, Canada, China, Germany, Russia, Singapore, the United States and the UK, the required hosting location/s to be selected by the Customer.

Where it is agreed that the Software shall be provided from Europe, Company shall ensure this is hosted from within the European Economic Area (EEA). In accordance with the DPA Company reserves the right to change the data centres within the EEA, provided that any new hosting centre provides at least the same level of services and security as the current data centre.

5.2 Disaster Recovery

In the event of a Disaster within a data centre used for the delivery of the Software, Company will initiate its Disaster recovery procedure. Disasters shall be notified to the Customer within 4 (four) hours of Company being notified of a Disaster.

Where it is agreed that the Software shall be provided from Europe, Company shall ensure that replicated data to provide Disaster Recovery shall remain within the EEA.

In all cases Company shall ensure that replicated data and other assets shall be available to support Disaster Recovery within the respective hosting country used for production service delivery. Data shall not be exported from the hosting country to support Disaster Recovery.

In the event of a Disaster, recovery time is expected to be less than 24 hours and recovery point is expected to be less than 1 hour. The procedures for Disaster Recovery are tested by the Company once a year.

5.3 System Backup

Full database backups are performed daily and transaction logs are secured throughout the day. File stores are held on high availability storage infrastructures and backups are automatically taken and secured independent of a single data centre location. Backup generations are retained for 6 (six) months throughout the Agreement and for 6 (six) months from the termination date of the Agreement.

All data backups shall remain within the country used for hosting and secured by encryption to AES-256 standard.

5.4 Data Repatriation

A written request for the return of Customer data stored in the Company's database will be executed in either CSV or XML format. This request must be received within 60 Business Days of the expiry of this Agreement, and the data will be delivered to the Customer within 30 Business Days of the request being made. The Customer agrees to pay for this service as set forth in the Order.

If a request is made for the data to be returned in a format other than CSV or XML or later than 60 Business Days after the expiry of the Agreement, an additional fee will be charged on a time and materials basis.

5.5 Penetration Testing

The Software is penetration-tested annually by a third party.

On request, Company will provide the Customer with a summary overview of all penetration tests, security and certification audits that are performed against Company's facilities and applications or any third parties contracted by Company as part of Company's Services.

On request, Company will further provide the Customer with a letter of opinion from the auditing organisation that confirms whether any material deficiencies were identified. If any material deficiencies are identified, then Company will identify the steps and timeframes to address such deficiencies and, once such deficiencies have been remediated, provide a letter of opinion from the auditing organisation confirming that remediation has been performed and that the material deficiency is no longer a concern.

5.6 Browser Support

Details of supported browsers can be found within the Cornerstone Support Dashboard at https://www.cornerstoneondemand.com/community-and-support/

6 Acceptable Use Policy

6.1 Acceptable Use Policy

The Customer shall not use the Software or Services:

- To threaten, violate or encourage the violation of the legal rights of others;
- For any unlawful, invasive, infringing, defamatory or fraudulent purpose;
- To intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes or other items of a destructive or deceptive nature;
- To remove, modify or obscure any copyrights, links or notices appearing in the Software;
- The Customer shall keep any received credentials/API keys secure and are not to be provided to any third party.

If the Customer breaches these rules, Company may suspend or terminate the Customer's access to the Software and the Customer will be liable for any damage caused.

Company reserves the right to alter the above acceptable use statement with 1 (one) month's prior notice.