DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") to the CCH Software and Services agreement (the "**Agreement**") between the undersigned Customer ("**Customer** ") and Wolters Kluwer (UK) Limited (company number 450650, incorporated in England & Wales) of 145 London Road, Kingston upon Thames, KT2 6SR, United Kingdom ("**CCH**", "**Processor**") is effective on the date of Processor's receipt of a valid and fully executed version (the "**Addendum Effective Date**") and is hereby incorporated into and forms a part of the Agreement.

The parties acknowledge and agree that this Addendum forms an integral part of the Agreement and shall supersede and prevail over the Agreement to the extent of any conflict or inconsistency relating to the processing of Customer Personal Data.

1. Definitions. Capitalized terms used but not defined in this Addendum will have the same meanings as set forth in the Agreement. In this Addendum, the following terms shall have the meaning set out below:

a. "**Affiliate**" means, with respect to any entity, any other entity that controls, is controlled by or under the control of such first entity.

b. "**Agreement**" means the agreement concluded between the Customer and the Processor setting out the terms and conditions for the provision of the Services.

c. "**Applicable Data Protection Law**" means GDPR (and UK GDPR, as applicable, and including the UK Data Protection Act 2018) and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the processing of Personal Data (including, without limitation, the privacy of electronic communications) (as applicable);

d. "**Customer Personal Data**" means the personal data described in Annex 1 of this Addendum of the category of data subjects set forth in Annex 1 that is processed by CCH on behalf of Customer to perform the Services under the Agreement.

e. "**control**" (or variants of it) means the ability, whether directly or indirectly, to direct the management and action of an entity by means of ownership, contract or otherwise.

f. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 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.

g. "**Member State**" means mean a country belonging to the European Union.

h. "**Services**" means the services provided to Customer by CCH and described under 'nature and purpose of the processing' in Annex 1 of this Addendum.

i. "**Subprocessor**" means any party (including CCH's Affiliates and any other third parties) appointed by CCH (who agrees to receive from CCH the Customer Personal Data exclusively intended for processing activities to be carried out on behalf of the Controller in accordance with its instructions, the terms of this Addendum and the terms of a written subcontract to process Customer Personal Data) to perform the Services.

j. "Technical and Organizational Measures" means those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, as set out in Annex 2.

k. "Third Country" means a country where the European Commission and/or the UK's Information Commissioner ("ICO") has not decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection.

l. "UK GDPR" means the retained EU law version of the GDPR, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018) and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

m. "Wolters Kluwer group" means CCH and its Affiliates engaged in the processing of Customer Personal Data.

n. The terms "controller", "data subject", "personal data", "special categories of data", "personal data breach", "processor", "processing", and "supervisory authority" shall have the meanings ascribed to them in the Applicable Data Protection Law, and their cognate terms shall be construed accordingly.

2. Customer Warranties.

a. Customer warrants that:

i. Customer's processing of the Customer Personal Data is based on legal grounds for processing as may be required by Applicable Data Protection Law and it has made and shall maintain throughout the term of the Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by the Applicable Data Protection Law with respect to CCH's processing of Customer Personal Data under this Addendum and the Agreement; and

ii. It is entitled to and has all necessary rights, permissions and consents to transfer the Customer Personal Data to CCH and otherwise permit CCH to process the Customer Personal Data on its behalf, so that CCH may lawfully use, process and transfer the Customer Personal Data in order to carry out the Services and perform CCH's other rights and obligations under this Addendum and the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

3. Controller and Processor. For purposes of this Addendum, Customer is the controller of the Customer Personal Data and CCH is the processor of such data, except if and when Customer acts as a processor of Customer Personal Data, in which case CCH is a subprocessor. Customer and its Affiliates, as their respective controllers, shall determine

the purposes of collecting and processing Customer Personal Data. Customer remains the responsible controller for the processing of the Customer Personal Data as instructed to CCH based on the Agreement, this Addendum and as otherwise instructed. Customer is entitled and obliged to instruct CCH in connection with the processing of Customer Personal Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Customer Personal Data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Customer in writing without delay. To the extent that the implementation of an instruction results in costs for CCH, CCH will first inform the Customer about such costs. Only after the Customer's confirmation to bear such costs for the implementation of an instruction, CCH is required to implement such instruction

4. Scope of Processing.

a. In order for CCH to provide the Services, CCH will process Customer Personal Data. Annex 1 to this Addendum sets out certain information regarding the processing of Customer Personal Data as required by Article 28(3) of the GDPR and/or UK GDPR. The parties may amend Annex 1 from time to time as the parties may reasonably consider necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this Section 4(a)) confers any right or imposes any obligation on any party to this Addendum.

b. CCH shall only process Customer Personal Data (i) in accordance with the documented instructions or as otherwise described in this Addendum. If Applicable Data Protection Law to which CCH is subject requires CCH to process Customer Personal Data in a manner contrary to Customer's instructions, CCH shall inform Customer in advance of any relevant processing of the affected Customer Personal Data, unless the relevant Applicable Data Protection Law prohibits this on important grounds of public interest.

c. CCH shall inform Customer if, in CCH's opinion, an instruction given by Customer under this Section 4 infringes Applicable Data Protection Law. CCH shall have the right to suspend processing of Customer Personal Data until Customer's instruction is clarified to the extent that it no longer infringes Applicable Data Protection Law.

5. Confidentiality.

CCH shall ensure that each of its personnel that is authorised to process Customer Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security.

a. CCH shall, in relation to Customer Personal Data, (a) take, as appropriate, measures required pursuant to Article 32 of the GDPR and/or UK GDPR, and (b) on reasonable request at Customer's cost, assist Customer in ensuring compliance with Customer's obligations pursuant to Article 32 of the GDPR and/or UK GDPR, taking into account the nature of the processing and the information available to CCH.

b. CCH shall maintain the security practices and policies for the protection of Customer Personal Data in accordance with the Technical and Organisational Measures as set forth in Annex 2 (INFORMATION SECURITY) of this Addendum. Customer warrants that it has assessed the security measures set out in Annex 2 of this Addendum and has

determined that they satisfy the requirements of Article 32 GDPR and/or UK GDPR in respect of CCH's processing of Customer Personal Data.

7. Subprocessors. Customer hereby authorises the use of Subprocessor(s) engaged by CCH for the provision of the Services. Customer approves the following Subprocessor(s) of CCH:

Name	Address	Purpose of use
Microsoft Azure	North Europe (Dublin) West Europe (Amsterdam)	Cloud hosting
Wolters Kluwer group	As applicable from time to time/various	Performance of CCH obligations under the Agreement, delivery of software, support and/or professional services

a. Customer acknowledges and agrees that (i) Wolters Kluwer group may be retained as Sub-processors; and (ii) CCH and Wolters Kluwer group respectively may engage third-party Sub-processors (and permit each Sub-Processor appointed under this Section 7 to appoint sub-processors) in connection with the provision of the Service.

b. In case CCH intends to engage new or additional Sub-processors, CCH shall inform Customer of such addition or replacement of Sub-processors in writing ("Sub-processor Notice") (which may be by email to the email address(es) on record in CCH's account information for Customer). If Customer has a reasonable basis to object to the use of any such new or additional Sub-processor because Customer is able to prove that significant risks for the protection of its Customer Personal Data exist with such Sub-processor, Customer will notify CCH in writing within fourteen (14) days of the date of the Sub-processor Notice detailing the basis for such objection. CCH will work with Customer in good faith and endeavour to make available a commercially reasonable change in the provision of the Services or recommend a commercially reasonable change to such Customer's configuration or use of the Services to avoid processing of Customer Personal Data by the objected-to new or additional Sub-processor without unreasonably burdening Customer, in either case which avoids the use of the Sub-processor. Where such a change cannot be made within 90 days from CCH's receipt of Customer's objection notice, notwithstanding anything in the Agreement, Customer, may, as its sole remedy, by written notice to CCH with immediate effect terminate that portion of the Agreement that relates to the Services that require the use of such new or additional Sub-processor. CCH will bind Sub-processors with written agreements that require them to provide at least the level of data protection required of CCH by this Addendum relative to the Sub-processor's activities relating to the Services. CCH shall be responsible for the acts and omissions of any Sub-processors. CCH shall not be liable for damages and claims that ensue from the Customer's instructions to Sub-processors. The provisions of this Section 7 shall not apply to the extent Customer instructs CCH to allow a third party to Process Customer Personal Data pursuant to a contract that Customer has directly with the third party.

8. Data Subject Requests.
To the extent legally permitted, CCH will promptly notify Customer if CCH or any Sub-processor receives any complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to Applicable Data Protection Law related to

Customer Personal Data. Taking into account the nature of the processing, CCH shall assist Customer at Customer's cost and request, by appropriate Technical and Organizational Measures, insofar as this is reasonably possible, for the fulfillment of Customer's obligation to respond to requests for exercising such data subjects' rights.

9. Data Breach.
CCH shall notify Customer without undue delay once CCH becomes aware of a personal data breach affecting Customer Personal Data. CCH shall, taking into account the nature of the processing and the information available to CCH, use commercially reasonable efforts to provide Customer with sufficient information to allow Customer, at Customer's cost, to meet any obligations to notify or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required by Applicable Data Protection Law.

10. Data Protection Impact Assessments.
CCH shall, taking into account the nature of the processing and the information available to CCH, provide reasonable assistance to Customer, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for Customer to fulfill its obligations under the Applicable Data Protection Law.

11. Term, termination & Destruction or return of Customer Personal Data.

a. The terms of this Addendum supplement the terms of the Agreement. The term of this Addendum shall automatically expire upon the termination of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.

b. Subject to Section 11c. below, or as otherwise required by applicable law, CCH will promptly and in any event by the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data; (ii) termination of the Agreement, and (iii) expiration of the time period for which Customer Personal Data is maintained by CCH pursuant to CCH's applicable disaster recovery and/or data retention practices for the Services, to the extent reasonably practicable, delete/or return all copies of Customer Personal Data processed by CCH. For the avoidance of doubt, CCH may retain Customer Personal Data if CCH is required by applicable law to retain such personal data.

c. For so long as CCH and each Sub-processor retains Customer Personal Data in accordance with this Section 11, CCH shall observe the obligations of confidentiality with respect to such Customer Personal Data and CCH will ensure that such Customer Personal Data is only processed as necessary and for no other purpose.

12. Audits.

a. Subject to Section 12b, CCH shall make available to Customer upon reasonable written request, information that is reasonably necessary to demonstrate CCH's compliance with this Addendum. Customer shall be responsible for any costs and expenses of CCH arising from the provision of such information or being incurred by the exercise of audit rights.

b. The Customer is aware that any in-person on-site audits may significantly disturb CCH's business operations and may entail high expenditure in terms of cost and time. Hence,

the Customer may only carry out an in-person on-site audit if the Customer reimburses CCH for any costs and expenditures incurred by CCH due to the business operation disturbance. Each requested audit shall meet the following requirements:

i. no more than one audit per calendar year shall be requested or conducted and upon no less than 90 days' notice to CCH;

ii. be conducted by an internationally recognized independent auditing firm reasonably acceptable to CCH;

iii. take place during CCH's regular business hours, pursuant to a mutually agreed upon scope of audit;

iv. the duration of the audit must be reasonable;

v. no access shall be given to the data of other customers; audits will not be permitted if they interfere with CCH's ability to provide the Services to any customers;

vi. audits shall be subject to any confidentiality or other contractual obligations of CCH or CCH's Affiliates (including any confidentiality obligations to other customers, vendors or other third parties);

vii. any non-affiliated third parties participating in the audit shall execute a confidentiality agreement reasonably acceptable to CCH;

viii. all costs and expenses of any audit shall be borne by Customer; and

ix. any audit of a facility will be conducted as an escorted and structured walkthrough and shall be subject to CCH's security policies.

13. Data Transfers.

CCH and/or Wolters Kluwer group shall impose the same data protection obligations as set out in this Addendum on any Subprocessor by contract. The contract between CCH and the Subprocessor shall in particular provide sufficient guarantees to implement the Technical and Organizational Security Measures as specified in Annex 2, to the extent such Technical and Organizational Security Measures are relevant for the services provided by the Sub-processor.

The Customer agrees that in respect of transfers of Personal Data under this Addeundum from the UK, EU, the European Economic Area ("EEA") and/or their Member States to Third Countries, to the extent such transfers are subject to the Applicable Data Protection Law, CCH shall secure the transfer under the terms of:

i. where GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs");

ii. where the UK GDPR applies, the applicable standard data protection clauses

adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and/or

iii. such other mechanism approved by the European Commission and/or the ICO and valid from time to time.

Should CCH, established within the EU, European Economic Area or the UK, engage with a sub-processor in a Third Country for which no adequacy decision from the European Commission and/or the ICO has been issued, the Customer hereby authorizes CCH, representing the Customer, to conclude a contract with the sub-processor which incorporates the EU SCCs or the UK SCCs. The Customer acknowledges that as at the Effective Date of this Addendum CCH may have validated such transfer under such mechanisms authorised in accordance with the Applicable Data Protection Law.

14. In relation to on premise/ self-hosted products (where applicable).

a. The Customer acknowledges and agrees that it: a) processes such categories of personal data and such special categories of data as it wishes from time to time; b) may transfer any such personal data and/or special categories of data to any country subject to Customer's own validation of the data transfer mechanisms used; c) is responsible for implementing and maintaining its own technical and organizational security measures for the on premise/self-hosted products to securely protect the personal data created, collected, received, or otherwise processed by the Customer which it hosts on its servers or under the arrangements Customer has made independent of CCH. Except at specified at Section 14b below, CCH does NOT access and does not process any personal data stored on the on premises/self-hosted products.

b. Occasionally, at the Customer's request (and with its express permission at all times) CCH may process such personal data and/or special categories of data as the Customer determines and provides, transfers or permits (including via screen sharing/ remote access), in connection with CCH's provision of support services and/or consultancy services from time to time. In that case CCH will process such personal data as detailed Annex 1.

15. Limitation of liability

The liability of CCH and/or its Affiliates taken together in the aggregate, arising out of or related to this Addendum whether in contract, tort or under any other theory of liability shall be exclusively governed by the liability provisions set forth in, or otherwise applicable to, the relevant Agreement applicable to the Services. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this Addendum shall be deemed to occur under the Agreement and be subject to the 'Limitation of Liability' section of the Agreement.

16. Miscellaneous.

a. Except as otherwise set forth herein, all terms and conditions of the Agreement will continue in full force and effect as set forth therein. Nothing in this Addendum reduces CCH's obligations under the Agreement in relation to the protection of Customer Personal Data or permits CCH to process (or permit the processing of) Customer Personal Data in a manner that is prohibited by the Agreement.

b. Notwithstanding any terms of the Agreement to the contrary, in the event and to the extent

of any conflict between the terms and conditions of (i) this Addendum and applicable law, the provision(s) of the applicable law shall govern; (ii) this Addendum and the UK SCCs and/or EU SCCs the provision(s) of the UK SCCs and/or EU SCCs respectively shall govern; and (iii) this Addendum and the Agreement, the provision(s) of this Addendum shall govern. CCH shall comply with the terms of this Addendum during the term of the Agreement and during any period during which CCH may have access to Personal Data.

c. CCH may modify or supplement this Addendum, with reasonable notice to Customer:

   i. If required to do so by a supervisory authority or other government or regulatory entity;

   ii. If necessary to comply with applicable law or the Applicable Data Protection Law;

   iii. To implement new or updated standard contractual clauses approved by the European Commission and/or the ICO; or

   iv. To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR and/or UK GDPR.

d. This Addendum shall be governed by the law of England and Wales except to the extent that mandatory Applicable Data Protection Law applies.

e. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

f. This Addendum and the documents referred to in it including the Agreement constitute the entire understanding and agreement of the parties in relation to the processing of Customer Personal Data and supersede all prior agreements, discussions, negotiations, arrangements and understandings of the parties and/or their representatives in relation to such processing.

g. This Addendum may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. Transmission of the executed signature page of a counterpart of this Agreement by email (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. No counterpart shall be effective until each party has executed at least one counterpart. Each party warrants it has full capacity and authority to enter into and perform its obligations under this Addendum.

   h. CCH has provided a signed copy of this Addendum to Customer. If Customer makes any addition, deletion or other revision to this CCH signed Addendum (other than completing the information on the signature page), then this Addendum will be null and void.

IN WITNESS WHEREOF, this Data Processing Addendum is entered into and becomes a binding part

of the Agreement with effect as of the Addendum Effective Date.

Executed by the parties on the dates shown below:

ANNEX 1

DETAILS OF PROCESSING OF PERSONAL DATA

This Annex includes certain details of the processing of Personal Data:

Subject matter and duration of the processing of Personal Data

Performance of CCH obligations under the Agreement (provision of the CCH Integrator Software and related Services).

CCH will process the Customer Personal Data during the term of the Agreement (including any renewal) and until the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data, (ii) the expiration of any continuing obligations of CCH to retain Customer Personal Data under the Agreement, and (iii) the expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery and/or data retention practices for the Services.

The nature and purpose of the processing of Personal Data

Hosting, storing and processing of Personal Data required for the provision of the CCH Integrator Software and related Services pursuant to the Agreement.

The types/ categories of Personal Data to be processed

name
surname
business email address

Special categories of Personal Data to be processed

-none-

The categories of data subject to whom the Personal Data relates

Customer's authorised users namely its employees.

ANNEX 2

INFORMATION SECURITY

Confidential and Proprietary Information of CCH

Information Security for the CCH Integrator Application

The following sets forth CCH information security policies and procedures for the CCH Integrator application as of January 2022. CCH reserves the right to modify its policies and procedures from time to time, provided CCH agrees not to modify its polices or procedures in a manner that would materially diminish the protections for Customer Personal Data set forth herein.

CCH Integrator is currently hosted at the following datacenters: Azure Australia East (primary) and Azure Australia Southeast (DR). CCH reserves the right to change its hosting locations and/or hosting providers from time to time in its sole discretion.

1. Information Security Policy

1.1. CCH has implemented an Information Security Policy (ISEC) that encompasses a variety of policies for managing information and technology assets intended to protect underlying applications and data.

1.2. Information Security Risk Assessment – On an annual basis, CCH conducts an information security risk assessment of, among other things, our security strategy, technical capabilities and performance with respect to the CCH Integrator application, including a tabletop walk-through exercise of our business continuity plan with respect thereto.

1.3. Life Cycle Management – Also on an annual basis, CCH reviews, and updates as needed, its personnel policies relevant to information security, including its ISEC and Acceptable Use policies.

2. Human Resources

2.1. Background Checks – CCH currently executes background checks during the hiring process for all full time employees. In addition, CCH contractually requires its data center Service Providers to conduct background checks on their respective full time employees who provide services to CCH.

2.2. Acceptable Use Policy – CCH has an Acceptable Use Policy (AUP) for its employees defining acceptable use and access to CCH and its affiliates' information systems.

2.2.1. CCH requires all employees to read and accept the terms of the AUP upon hire date.

2.3. Security Awareness Training – CCH has an information security awareness training program for its employees.

3. CCH Integrator Infrastructure Credentials

3.1. Provisioning – All credentials used in conjunction with the infrastructure, operating systems, or databases supporting the CCH Integrator application are provisioned using an identity management request based system that requires applicable management approval for access and privilege changes.

3.2. Termination – All such credentials are to be disabled within 24 hours of an employee's

termination date.

3.3. Quarterly Review – All such credentials are reviewed quarterly by management for appropriate role assignment, appropriate privilege level, inactivity, and necessity.

3.4. Privilege Revocation – CCH revokes unnecessary privileges if an employee shifts roles and no longer needs the prior level of privilege. When an employee shifts to a role that does not require any access to such infrastructure assets, systems or databases, the credential for such access will be revoked.

3.5. Passwords – CCH implements a minimum standard password policy for access to such systems and databases.

3.5.1. Complexity – Password complexity will be enforced and all passwords must meet three of the following
five criteria.

3.6.1.1. One upper case character.

3.6.1.2. One lower case character.

3.6.1.3. One number.

3.6.1.4. One special character.

3.6.1.5. One Unicode character.

3.6.2. Length – Passwords must contain a minimum of eight characters.

3.6.3. Age – The minimum password age is one day (i.e., passwords cannot be changed more than once a day). The maximum password age is sixty (60) days (i.e., passwords must be changed at least every sixty (60) days)

3.6.4. History – The minimum password history maintained is ten.

3.6.5. Reset – Passwords can only be reset through the applicable data center Service Desk.

3.6.6. Lockout – Accounts will be locked after five consecutive invalid login attempts. Thereafter, accounts can only be unlocked by the applicable data center Service Desk, or once the lockout timer has expired.

3.6. Application Credentials for CCH Integrator Customers - Application credentials are managed by the Customer. The Customer's administrator account can create, delete and modify application User IDs (UID), and can delegate account control to one or more UID account(s) associated with that Customer's application account. The application UIDs are only valid when used with the CCH Integrator application.

4. Role Separation

4.1. Defined Duties and Responsibilities – CCH, together with its applicable data center Service Providers, define the roles and responsibilities for the employees of CCH and its Service Providers who support infrastructure and services for CCH Integrator in the Process Interface Manual (PIM) that is in place between CCH and each of the data center Service Providers. For Azure Integrator systems, Wolters Kluwer Global Business Services fills the service role. Each such person/function will be given the amount of privilege necessary in order for such person/function to fulfill the duties of the role he or she is currently assigned, as follows:

4.2. Network – Network engineers will have access to network switches, routers, firewalls, load balancers, intrusion detection systems, and network intrusion prevention systems.

4.3. Storage – Storage engineers will have access to storage frames and volumes.

4.4. Intel/Server Systems– Intel/Server Systems Engineers will have access to physical hosts, hypervisor hosts, operating systems, connected storage volumes, monitoring systems, and the active directory.

4.5. Backup – Backup technicians will have access to storage volumes, and backup control software consoles.
4.6. Release Management – Release Management engineers will have access to operating systems, connected storage volumes, IT automation systems, monitoring systems, and active directory.
4.7. Database Administrators – Database administrators will have access to database server operating systems, databases, connected storage volumes, and monitoring systems.
4.8. Management and Governance – Applicable management personnel will have access to IT automation and monitoring systems as needed for purposes of their management and governance responsibilities.

5. Environment Separation

5.1. Environments – CCH maintains physical and/or logical environment separation for the CCH Integrator application as described below in this Section 5.
5.2. Corporate – CCH maintains a corporate network supporting general employee and internal business activities. This network is physically and logically separated from networks supporting hosted applications such as CCH Integrator.
5.3. Core – CCH implements a core network supporting routing between office locations, data centers, corporate, testing, stage, and production networks.
5.4. Development and Test – CCH maintains development and testing environments that are physically and logically separate from stage and production environments.
5.5. Stage – CCH maintains a staging environment that is physically and logically separate from development and test environments and also logically separate from production environments.
5.6. Production – CCH maintains two dedicated environments (Primary and Disaster Recovery) for CCH Integrator. The production environments are physically and logically separated from the corporate, development, and test environments. The production environments are logically (but not physically) separated from the staging environment.

6. Physical Hosted Environment

6.1. Tier 3 or above data center – CCH will only host CCH Integrator at a Tier 3 or above data center with the following characteristics:
6.1.1. Isolated Raised Floor Facility – Computing equipment is housed in a dedicated raised floor data center.
6.1.2. Access Control – Access to the data center floor is restricted and applicable management approval and valid Service ticket is required to gain access.
6.1.3. Security – Onsite security is on duty 24x7x365 with access to monitored CCTV of ingress doors and data center floors.
6.1.4. Fire Suppression – A non-liquid fire suppression system has been installed.
6.1.5. Redundant Pathways – All redundant systems also have redundant pathways.
6.1.6. Redundant Components – All computing components have a redundant standby.
6.1.7. Redundant Power – The facility has a redundant power source with at minimum two separate utility power feeds into data center building.

6.1.8. Redundant Chilling Capacity of N+1 – The cooling system has sufficient capacity to maintain appropriate temperatures in the event of a failure of one system.

6.1.9. Uninterruptable Power Supply – Computing systems are connected to an uninterruptable power source with sufficient energy to maintain the systems during generator start-up.

6.1.9.1. Backup Generator – A backup generator capable of maintaining all systems necessary for CCH Integrator for at least 40 hours.

7. Data Protection

7.1. Backup – Customer Data is backed up at least once per day. Backups are retained for 14 days.

7.2. Retention – Customer Data that is not deleted by the Customer is currently retained for at least seven (7) years whilst this agreement is in effect. Data that is deleted by the Customer would be retained according to CCH's then current retention policy. The following is CCH's current retention policy for data on CCH Integrator:9

7.2.1. Daily backups of data are retained for 14 days.

7.2.2. Data on the production site that is older than seven years may be removed from the production site.

7.3. Data Encryption – All Customer Data is encrypted in transit and at rest. Databases are encrypted.

7.4. Backup Encryption – All Customer Backup Data is encrypted in transit and at rest.

8. Environment Availability

8.1. Redundancy – CCH deploys all computing components for CCH Integrator within redundant Availability Zones. Failover testing from the primary to the secondary device is performed at least annually.

8.2. Active-Active (within local region) Azure Availability Zones – CCH maintains, for the CCH Integrator application, a highly available database environment configuration. In this configuration, each region contains three separate data centers that are separated but part of the same Azure Region, with low latency and high bandwidth communication channels.

8.3 Disaster recovery environment - Active-Passive (between geographical region) Azure DR region pairs – Integrator will have separate datacenter regions for the CCH Integrator application. Both regions can process data. Failover to the standby environment will be conducted at CCH's discretion.

8.4 Health Monitoring – CCH also maintains automated health monitoring of all computing systems supporting the CCH Integrator application. The monitoring system is intended to automatically generate alerts when monitoring thresholds have been exceeded.

8.5 Performance Monitoring – CCH maintains automated performance monitoring of all computing systems supporting CCH Integrator. The monitoring system is intended to automatically generate alerts when monitoring thresholds have been exceeded.

8.6 Performance Testing – CCH maintains a formal performance and scalability testing process. All major code changes undergo formal performance testing before being deployed to the production environment.

8.7 Capacity Planning – CCH maintains a formal capacity planning process to assess baseline load and can be expanded to meet increased demand leveraging Azure cloud platform capabilities.

9. Operations Management

9.1. Release Management – CCH maintains a release management and code promotion process for the CCH Integrator application. This process is intended to ensure code is tested in a controlled environment, which mimics the production environment, using realistic test cases. Code will be promoted from the testing environment to the staging environment to allow for IT automation and source image validation before being promoted to production.

9.2. Change Management – CCH maintains a change management process. All changes to infrastructure hosting CCH Integrator will be detailed in a change request, be scheduled in predetermined change window, and require applicable management approval.

9.3. Incident Management – CCH, with its applicable Service Providers, maintains an incident management process. The incident management process is intended to facilitate the resolution of, provide for a root cause analysis for, and ensure remediation steps are completed for any service disruption to the CCH Integrator application.

9.4. Security Management – CCH, with its applicable Service Providers, maintains a security incident management process. This process defines steps for minimizing loss of data, preserving evidence, escalation of support to a specialized information technology forensics team, vulnerability identification, vulnerability remediation, and notification guidelines.

9.5. Runbooks – Role and processes related documentation are maintained in IT Operation runbooks that are maintained by the Service Provider. The Runbooks define the scope of responsibilities for both CCH's employees and its data center Service Provider's employees in a specific role, detail the steps of a specific process, and detail steps to accomplish a specific task. Runbooks are reviewed regularly with CCH's data center Service Provider and updated as needed. For CCH Integrator, Wolters Kluwer Cloud Managed Services fills the service role.

9.6. Key Performance Indicators – CCH tracks application uptime, service disruptions, the root cause of material disruptions, and the implementation of any remediation.

10. Additional Security Measures

10.1. Antivirus and Malware – CCH utilizes antivirus and malware protection software designed to protect computing equipment hosting the CCH Integrator application.

10.1.1. Endpoints are configured to automatically update the signature file no less than twice weekly.

10.1.2. Endpoints are configured for real-time scanning.

10.1.3. Endpoints are configured for a full rescan once per week.

10.1.4. All Virus notifications and alerts are transferred to service desk teams for review.

10.2. Intrusion Detection tools – CCH maintains Intrusion Detection tools designed to provide certain protections for all environments.

10.3. Intrusion Prevention Tools – CCH maintains Intrusion prevention tools designed to provide certain protections for all environments.

10.4. Web Application Firewall (WAF) – CCH Integrator maintains a WAF that includes Distributed Denial of Service (DDOS) protection.

10.5. Vulnerability Scans – CCH conducts, at a minimum, quarterly internal and external vulnerability scans. The results are not made available to Customers.

10.6. Penetration Testing – CCH will commission a third party external penetration test annually. An executive summary of results may be made available to Customers upon request and subject to confidentiality requirements.

10.7. Security and Event Log Management – CCH maintains the following security and event logs for all computing equipment for a minimum of thirty days.

10.7.1. Security Logs

10.7.1.1. Routers, Switches, Firewalls, and Load Balancers – Allow changes to router configuration to be tracked as a unique SYSLOG message.

10.7.1.2. Servers – Allows users login events to be tracked as individual messages.

10.7.2. Event Logs

10.7.2.1. Routers, Switches, Firewalls, and Load Balancers - Allows configured system events such as memory utilization, CPU utilization, rule utilization, network errors, packet loss, and other messages designed to provide administrators with information regarding the health and performance of the device to be captured as unique SYSLOG messages.

10.7.2.2. Servers – Allows configured system events such as application errors, application events, service start and stop events, and other messages designed to provide administrators with information regarding the health and functionality of the server and the applications hosted on the server.