FTW DATA PROCESSING ADDENDUM

This FTW Data Processing Addendum (this "**Addendum**") is effective as of November 1, 2021("**Addendum Effective Date**") and forms a part of either the CCH License Agreement for ftwilliam.com Site and Products between CCH Incorporated, a Wolters Kluwer company ("**CCH**") and an individual, institution or organization ("**Customer**") subscribing to ftwilliam.com ("**FTW**") Products pursuant to an order form or agreement or an agreement signed between CCH and a Customer establishing terms for the Customer's use of Products by the Customer, as the case may be (such terms, and as may be amended from time to time, the "**Agreement**"). In the course of providing the Services (as defined below), CCH may process personal data (as defined below) on behalf of Customer, and CCH agrees to comply with the following provisions with respect to any such 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**" has the meaning given to such term in the Agreement.

b. "**Customer Personal Data**" means any personal data of a data subject that is processed by CCH on behalf of Customer to perform the Services under the Agreement.

c. "**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.

d. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (with effect from May 25, 2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

e. "**EU Laws**" means European Union or Member State law, including EU Data Protection Laws.

f. "**GDPR**" means EU General Data Protection Regulation 2016/679.

g. "**Restricted Transfer**" means a transfer of Customer Personal Data from CCH to a Subprocessor where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws) in the absence of appropriate safeguards required for such transfers under EU Data Protection Laws.

h. "**Services**" means the FTW Subscription Services, as well as all related services (such as Support services), provided to Customer by CCH pursuant to the Agreement.

i. "**Standard Contractual Clauses**" means the Annex to the Commission implementing decision 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 C/2021/3972 (Module Two which is attached to and incorporated herein as Annex @) or any

subsequent version thereof published by the European Commission (which will automatically apply).

j. "**Subprocessor**" means any party (including CCH's Affiliates and any other third parties) appointed by CCH to process Customer Personal Data to perform the Services.

k. The terms "**controller**", "**data subject**", "**personal data**", "**personal data breach**", "**processor**", "**processing**", and "**supervisory authority**" shall have the meanings ascribed to them in the GDPR, and their cognate terms shall be construed accordingly.

2. Customer Warranties. Customer warrants that:

a. Customer's processing of the Customer Personal Data is based on legal grounds for processing as may be required by EU Data Protection Laws 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 EU Data Protection Laws with respect to CCH's processing of Customer Personal Data under this Addendum and the Agreement; and

b. 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.

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 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.

4. Scope of Processing.

a. In order for CCH to provide the Services under the Agreement, 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. 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 described in this Addendum, and (ii) for the purposes of fulfilling its obligations under the Agreement. If EU 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 EU 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 EU 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 EU Law.

5. Confidentiality. CCH shall ensure that each of its personnel that is authorized 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 (b) on reasonable request at Customer's cost, assist Customer in ensuring compliance with Customer's obligations pursuant to Article 32 of the 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 as set forth in Annex 2 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 in respect of CCH's processing of Customer Personal Data.

7. Subprocessors. Customer hereby authorizes CCH to appoint Subprocessors in accordance with this Section 7, subject to any restrictions in the Agreement. CCH will bind Subprocessors with written agreements that require them to provide at least the level of data protection required of CCH by this Addendum relative to the Subprocessor's activities relating to the Services. Customer authorizes CCH's engagement of CCH's Affiliates, and the third party(ies) listed in Annex 1, as Subprocessors. In case CCH intends to engage new or additional Subprocessors, CCH will inform Customer in writing (which may be by email or other Product-enabled notification to Customer's Product Administrator) of such additions or replacements (the "**Subprocessor Notice**"). If Customer has reasonable grounds proving that significant risks for the protection of its Customer Personal Data exist with such new or additional Subprocessor(s), Customer will notify CCH in writing within 30 days of the date of the Subprocessor Notice, detailing the basis for the objection. CCH will work with Customer in good faith 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 Subprocessor(s) without unreasonably burdening Customer, in either case which avoids the use of the Subprocessor(s). 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 Processor. CCH shall be responsible for the acts and omissions of any Subprocessors as it is to Customer for its own acts and omissions in relation to the matters provided in this Addendum. 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 Subprocessor receives any complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to EU Data Protection Laws) 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 under EU Data Protection Laws.

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, at Customer's cost, 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 EU Data Protection Laws.

11. Destruction of Customer Personal Data.

a. Subject to Section 11.b. 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 pursuant to applicable disaster recovery practices for the Services, to the extent reasonably practicable, delete and procure the deletion of all copies of Customer Personal Data processed by CCH. For the avoidance of doubt, CCH may retain Customer Personal Data as required by EU Laws.

b. For so long as CCH and each Subprocessor retains Customer Personal Data in accordance with this Section 11, CCH's obligations of confidentiality with respect to such Customer Personal Data will continue and CCH will ensure that such Customer Personal Data is only processed as necessary and for no other purpose.

12. Audit.

a. Subject to Sections 12(b) and (c), 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 and audit rights.

b. Customer's information and audit rights only arise under Section 12(a) above to the extent that the Agreement and/or any other information available to Customer in relation to the Services does not otherwise give Customer information and audit rights meeting the requirements of Section 12(a) above.

c. Customer is aware that any in-person on-site audits are likely to significantly disturb CCH's business operations, including operations relating to the Services being provided pursuant to the Agreement. Customer shall ensure that its auditors make reasonable efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to CCH's premises, equipment, personnel and business while its auditor personnel are on those premises in the course of such an audit or inspection. 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. shall 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 and in any event shall not exceed two business days;

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.

d. CCH shall immediately inform Customer if, in CCH's opinion, an instruction in relation to Customer's rights under this Section 12 infringes EU 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 EU Law.

13. Data Transfer.

CCH and Customer hereby enter into the Standard Contractual Clauses in the form set forth in Annex 3 in respect of any Restricted Transfer. If CCH's arrangement with a Subprocessor involves a Restricted Transfer, CCH shall incorporate the onward transfer provisions of the Standard Contractual Clauses into the agreement entered into between CCH (who shall be permitted to enter the Standard Contractual Clauses on behalf of Customer) and the Subprocessor or, if the Subprocessor is Privacy Shield certified or operating under binding corporate rules, a requirement that the Subprocessor maintain its Privacy Shield certification or binding corporate rules, as applicable, throughout the term of the Agreement. Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing CCH to conduct the audit set out in Section 12.

14. 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 and amended thereby. 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 Standard Contractual Clauses, the provision(s) of the Standard Contractual Clauses shall govern; and (iii) this Addendum and the Agreement, the provision(s) that are more protective of Customer Personal Data 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;

iii. To implement new or updated Standard Contractual Clauses approved by the European Commission; or

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

d. Without prejudice to the Standard Contractual Clauses, this Addendum will be governed by the laws of the country or territory stipulated in the Agreement.

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.

[End of Addendum; Annexes follow]

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

This Addendum addresses the processing of Customer Personal Data in connection with Customer's subscription to, and CCH's hosting and provision of, the FTW Subscription Service pursuant to the terms of the Agreement. FTW is a software-as-a service application for professionals managing United States-based employee benefit plans of their clients (such as defined contribution plans). CCH will process the Customer Personal Data during the term of the Agreement (including any renewals) 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 in connection with the Agreement, and (iii) the expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery practices for the Services.

The nature and purpose of the processing of Personal Data

CCH will process Customer Personal Data as necessary to perform the Services and fulfill Customer's subscription to the FTW Service, as further instructed by Customer, and including:

- For the operation, maintenance and development of the FTW Service,
- To perform Services and fulfill Customer's subscription to the FTW Service, as further instructed by Customer,
- For providing Services related to the inherent functionality of the FTW Service (such as sending tax forms to plan participants),
- For hosting the Product,
- For implementation services,
- For Support, and
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes).

The types of Personal Data to be processed

Customer may input Customer Personal Data into the FTW Service or otherwise provide Customer Personal Data in connection with its subscription to the FTW Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include in its standard configuration, the following basic categories of Personal Data:

- First and last names of natural persons who are employee benefit plan participants (including retirees) and of natural persons related to such persons

- Contact information (including home street and email addresses and telephone numbers)
- User IP addresses
- United States Social Security Identification Numbers
- Employment information including compensation details for plan participants

The categories of data subject to whom the Personal Data relates

Customer may input Customer Personal Data into the FTW Service or otherwise provide Customer Personal Data in connection with its subscription to the FTW Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees and retirees, related persons, and plan advisors of Customers' clients.

List of current Subprocessors:

- Microsoft Azure (hosting providing, United States)
- Factor Systems, Inc. dba Billtrust (print and mailing fulfillment, United States)
- Nelco Inc. (electronic 1099 correction filings, United States)
- Wolters Kluwer affiliates, including Wolters Kluwer Technology B.V., Wolters Kluwer R&D U.S. LP, Wolters Kluwer Global Business Services B.V. and Wolters Kluwer United States Inc. (systems development and support and other software application and related services, United States and Europe)

ANNEX 2

MODULE 2: CONTROLLER TO PROCESSOR

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing)not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional. This option is not used – left void on purpose

SECTION II– OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further

information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2].(in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least thirty days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements maybe considered as part of an overall assessment. Such elements may include relevant and documented practicalexperience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whethertheir practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14 and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State where the data exporter "Customer" (as defined in that certain ftwilliam.com Platform and Products Terms and Conditions) is established. In the event that such law does not allow for third-party rights these clauses shall be governed by the laws of the Netherlands, where the data importer's ultimate parent company, Wolters Kluwer N.V., is based.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State where the data exporter "Customer" (as defined in that certain ftwilliam.com Platform and Products Terms and Conditions) is established. In the event that these Clauses are governed by the laws of the Netherlands under Clause 17, then the Parties agree the competent court in Amsterdam, the Netherlands shall resolve any dispute arising under these Clauses.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The subscribing Customer (as defined in the ftwilliam.com Platform and Products Terms and Conditions) to the ftwilliam.com online service (or an affiliate of such Customer, if applicable).

- Contact details: data exporter can be contacted through the contact details set forth in the Order Document (as defined in the ftwilliam.com Platform and Products Terms and Conditions).
- Activities relevant to the data transferred under these Clauses: entering into the Order Document and utilizing the ftwilliam.com online services for its internal business purposes
- Signature and date: as reflected in the Order Document
- Role: controller

Data importer(s): CCH Incorporated

- Contact details:

  2700 Lake Cook Road, Riverwoods Illinois 60015 United States of America

  Phone: 1-800-596-0714

  Email: support@ftwilliam.com (support)

  wklrus-privacy@wolterskluwer.com (privacy)
- Activities relevant to the data transferred under these Clauses: entering into the Order Document and fulfilling Customer's subscription to the ftwilliam.com online services
- Signature and date: as reflected in the Order Document
- Role: processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may input Customer Personal Data into the ftwilliam.com online service or otherwise provide Customer Personal Data in connection with its subscription to the ftwilliam.com online service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees and retirees, related persons, and plan advisors of Customers' clients.

Categories of personal data transferred

Customer may input Customer Personal Data into the ftwilliam.com online service or otherwise provide Customer Personal Data in connection with its subscription to the ftwilliam.com online service, the extent of which is determined and controlled by Customer in its sole discretion, but

which may include in its standard configuration, the following basic fields that can be filled in by Customer:

- First and last names of natural persons who are employee benefit plan participants (including retirees) and of natural persons related to such persons
- Contact information (including home street and email addresses and telephone numbers)
- IP addresses
- United States Social Security Identification Numbers
- Employment information including compensation details for plan participants

As Data Controller, Customer can add other personal data with the "additional fields" function.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Use of the ftwilliam.com online service doesn't anticipate the transfer of special categories of data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis as necessary for the purposes of the transfer detailed below.

Nature of the processing

See description of the purposes below.

Purpose(s) of the data transfer and further processing

The data exporter, or an affiliate of data exporter, may transfer personal data to the data importer which will then process the personal data transferred for the following processing activities:

- For the operation, maintenance, and development of the ftwilliam.com online service
- To perform services and fulfill Customer's subscription to the ftwilliam.com online service, as further instructed by Customer
- For providing services related to the inherent functionality of the ftwilliam.com online service
- For hosting the Product
- For implementation services
- For Support
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes)

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subscribing Customer Personal Data may be processed during the time term agreed to with the subscribing Customer (including the period of subscription and 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 practices for the ftwilliam.com online services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers may be made to service providers or processors who perform certain functions on data importer's behalf, such as hosting of the ftwilliam.com online service and other services related to the operation of the data importer's business. Transfers may also be made to affiliates of data importer who support the data importer's products.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the supervisory authority of the Member State where the data exporter is established.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

CCH currently maintains the security practices with respect to its ftwilliam.com software as a service product that are described in this Annex. Notwithstanding any provision to the contrary, CCH may update or change these security practices from time to time at its discretion. The ftwilliam.com software is currently hosted with Microsoft Azure in the United States.

The ftwilliam.com security program is designed to (i) maintain the availability of the ftwilliam.com Subscription Services and its systems and customer information, (ii) control access to the ftwilliam.com Subscription Services and its systems and customer information, and (iii) maintain the confidentiality of Customer Data within the ftwilliam.com Products. Mechanisms of the information security program include, risk management, including vendor risk review, logging and monitoring, internal and external audits/assessments, internal controls assessment, penetration and vulnerability assessments, contract management, security awareness. More specifically, the ftwilliam.com Subscription Service security program is comprised of the following:

1. Policies and Risk Assessment. CCH has implemented an information security program that encompasses a variety of policies for managing information and technology assets intended to protect underlying applications and data. Policies are reviewed on a periodic basis. Information security risk assessments are also conducted on a periodic basis.

2. Human Resources. CCH employees undergo background checks and all employees participate in security awareness training on a regular basis.

3. ftwilliam.com Infrastructure & Role Separation. Resources that support infrastructure and application services are delineated access privileges based on job responsibilities limiting access privileges to that necessary to perform responsibilities. Infrastructure credentialing requires management approval and business processes are implemented to periodically review level of privileges and address changes in role, privilege revocation and termination. CCH implements minimum standard password policy addressing complexity, age and history of password controls.

4. Customer Credential Management. Application credentials are managed by customers and include at the customer's option the ability to use two-factor authentication and IP address filters.

5. Data Protection. All Customer Data is encrypted in transit and at rest. Revisional (point in time) backup datasets of Customer Data are kept for 21 days. Additional annual and monthly backups are generated and kept until subsequent backups are created. Customer Data is destroyed using secure techniques.

6. Environment Separation. ftwilliam.com maintains physical and/or logical environment separation for the ftwilliam.com software application, including separate development, testing, staging and production environments. The production application and disaster recovery instances are hosted with Microsoft Azure, in the

United States, which includes access controls, onsite security, fire suppression, uninterruptable power supply, backup generators, redundant pathways, components, power and cooling systems.

7. Availability. The computing components are deployed with one or more redundant clones in a high available environment configuration, which includes a disaster recovery environment. Health and performance monitoring is conducted on all computing systems. Capacity planning is periodically assessed.

8. Operations Management. CCH maintains release management, change management, incident management and security management processes.

9. Vulnerability and Penetration Testing. CCH conducts vulnerability and penetration testing of the ftwilliam.com software application and infrastructure on a periodic basis