Cendyn™

Knowland

Controller to Controller Data Sharing Agreement

CONTROLLER TO CONTROLLER DATA SHARING AGREEMENT

Updated on: July 1, 2025

This Cendyn Controller to Controller Data Sharing Agreement, including its exhibits ("**DSA**"), is entered into between Cendyn Group, LLC, a limited liability company incorporated under the laws of the State of Delaware, and its relevant Affiliates (collectively, "**Cendyn**") and Cendyn's counterparty ("**Customer**") to the Master Service Agreement and an order form or statement of work ("**Agreement**") to purchase or subscribe to Cendyn's Knowland Product (as defined in the Knowland Product Annex to Cendyn Master Service Agreement). Cendyn and Customer are referred to individually in this DSA as a "**Party**" and, collectively, the "**Parties**."

This DSA is effective when the last Party signs/assents to the Agreement (the "**DSA Effective Date**").

1. SCOPE, DEFINITIONS AND APPLICABLE LAW

1.1. Duration. This DSA begins on the DSA Effective Date. Cendyn's obligations under this DSA shall continue for as long as Cendyn processes Customer Personal Data (defined below) under the Agreement. Customer's obligations under this DSA shall continue for as long as Customer processes Knowland Data (defined below) under the Agreement.

1.2. Scope. This DSA is expressly incorporated by reference and forms part of the Agreement and applies to the personal data contained in Readerboard Data (as defined in the Agreement) you provide to Cendyn ("**Customer Personal Data**"). This DSA also applies to the extent that Customer receives, accesses, or otherwise processes Knowland's Data from Cendyn in connection with the Agreement.

1.3. For the purposes of this DSA, "**Knowland Data**" means any personal data, or personal information that is included in the Knowland Content (as defined in the Knowland Product Annex to the Master Service Agreement) such as business contact data, which may include but is not limited to, name, job title, email address, and phone number that Customer may receive, access, or process from Cendyn pursuant to the Agreement. Knowland Content does not typically contain personal data. However, in some cases, limited contact or identifying information, including but not limited to, names of group organizers or booking contacts publicly associated with events, may be included, particularly where such information is publicly displayed.

1.4. Terms and expressions used herein that are not otherwise defined, including, without limitation, "personal information," "personal data," "controller," "processing," and "processor," and their respective derivative terms, shall have the meanings set forth in the privacy and data protection laws, regulations, and decisions applicable to a Party to this DSA ("**Applicable Data Protection Law**"), which may include, without limitation, the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et seq. and its implementing regulations, and the EU General Data Protection Regulation (2016/679) (the "**GDPR**"), as amended, superseded or replaced from time to time.

2. ROLES AND RESTRICTIONS

2.1. Each Party to this DSA:

(a) is an independent controller of or business of Customer Personal Data and Knowland Data under Applicable Data Protection Law and shall be independently and separately responsible for complying with the obligations applicable to it under Applicable Data Protection Law; and

(b) will individually determine the purposes and means of its processing of Customer Personal Data and Knowland Data.

2.2. Nothing in this Section 2 shall modify any restrictions applicable to either Party's rights to use or otherwise process Customer Personal Data or Knowland Data under the Agreement. Cendyn will

process Customer Personal Data solely and exclusively for the purposes specified in the Agreement. Customer will process Knowland Data solely and exclusively for the purposes specified in the Agreement.

3. PROTECTION OF PERSONAL DATA

3.1. To the extent not otherwise provided for in the Agreement:

(a) In accordance with Applicable Data Protection Laws, Cendyn shall implement and maintain appropriate security measures (including technical and organizational measures) to protect the security, confidentiality, and integrity of Customer Personal Data, as specified in **Exhibit A** below. The appropriate technical and organizational measures shall consider any applicable industry standards, the costs of implementation, the nature, scope, context, and purposes of the processing, and risks for the rights and freedoms of individuals;

(b) Cendyn shall ensure that its security measures cover all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones and other devices that process Customer Personal Data. Moreover, Cendyn shall ensure that its security measures include industry-standard password protections, firewalls and anti-virus and malware protections to protect Customer Personal Data handled or stored on Cendyn's computer systems;

(c) Cendyn shall review and, as appropriate, revise its security measures once a year or sooner if there a material change in Cendyn's business practices that may reasonably implicate the security, confidentiality, or integrity of Customer Personal Data;

(d) These security measures shall remain in place throughout the duration of Cendyn's processing of Customer Personal Data as specified in the Agreement or until Cendyn ceases to process Customer Personal Data (whichever is later);

(e) Cendyn will treat Customer Personal Data with strict confidence and take all reasonable steps to ensure that persons Cendyn employs and/or persons engaged at Cendyn's place(s) of business who will process Customer Personal Data are aware of and comply with this DSA and are under a duty of confidentiality with respect to Customer Personal Data no less restrictive than the duties set forth herein; and

3.2. To the extent not otherwise provided for in the Agreement:

(a) Customer shall implement appropriate organizational, technical and security measures to protect the security, confidentiality, and integrity of Knowland Data against the accidental, unlawful or unauthorized access to or use, transfer, destruction, loss, alteration, commingling, disclosure or processing of Knowland Data and ensure a level of security appropriate considering any applicable industry standards, the costs of implementation, the nature, scope, context, and purposes of the processing, and risks for the rights and freedoms of individuals;

(b) Customer shall ensure that its security measures cover all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones and other devices that process Knowland Data. Moreover, Customer shall ensure that its security measures include industry-standard password protections, firewalls and anti-virus and malware protections to protect Knowland Data handled or stored on Customer's computer systems;

(c) Customer shall review and, as appropriate, revise its security measures once a year or sooner if there a material change in Customer's business practices that may reasonably implicate the security, confidentiality, or integrity of Knowland Data;

(d) These measures shall remain in place throughout the duration of Customer's processing of Knowland Data as specified in the Agreement or until Customer ceases to process Knowland Data (whichever is later);

(e) Customer will treat Knowland Data with strict confidence and take all reasonable steps to ensure that persons Customer employs and/or persons engaged at Customer's place(s) of business who will process Knowland Data are aware of and comply with this DSA and are under a duty of confidentiality with respect to Knowland Data no less restrictive than the duties set forth herein;

(f) Customer will not transfer Knowland Data to third parties except to Authorized Users as specified in the Knowland Product Annex to Cendyn Master Service Agreement and will guarantee

Authorized Users maintain at least a level of data protection and information security as provided for herein. Customer will remain fully liable to Cendyn for any Authorized Party's failure to so comply; and

4. NOTICE AND COOPERATION

4.1. Cendyn will promptly give written notice to and fully cooperate with Customer regarding:

(a) any breach of security or unauthorized access to the Customer Personal Data that Cendyn detects or becomes aware of, and

(b) any complaint, inquiry, or request from an individual or government or regulatory agency regarding Customer Personal Data, unless such notice is prohibited by law.

(c) In such cases, without limiting the generality of the foregoing, Cendyn will refrain from notifying or responding to any data subject, government or regulatory agency, or other third party, for or on behalf of Customer, unless Customer specifically requests in writing that Cendyn do so, except as and when otherwise required by Applicable Data Protection Law.

4.2. Customer will promptly give written notice to and fully cooperate with Cendyn regarding:

(a) any breach of security or unauthorized access to the Knowland Data that Customer detects or becomes aware of, and

(b) any complaint, inquiry, or request from an individual or government or regulatory agency regarding Knowland Data, unless such notice is prohibited by law.

(c) In such cases, without limiting the generality of the foregoing, Customer will refrain from notifying or responding to any data subject, government or regulatory agency, or other third party, for or on behalf of Cendyn, unless Cendyn specifically requests in writing that Customer do so, except as and when otherwise required by Applicable Data Protection Law.

5. RESTRICTED TRANSFERS OF PERSONAL DATA

5.1. "**Restricted Transfer**" means any transfer of personal data protected by Applicable Data Protection Laws to a country outside of the country from which the data originates ("Third Country") or an international organization in a Third Country (including data storage on foreign servers).

5.2. Restricted Transfers of Customer Personal Data and Knowland Data within this DSA's scope shall be conducted in accordance with jurisdiction specific terms set forth in **Exhibit C** available here, and Applicable Data Protection Laws.

5.3. If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by Cendyn during the term of the Agreement (an "**Alternative Mechanism**"), and Cendyn notifies Customer that some or all Restricted Transfers can be conducted in compliance with Applicable Data Protection Laws pursuant to the Alternative Mechanism, the Parties will rely on the Alternative Mechanism instead of the transfer mechanisms in **Exhibit A** for Restricted Transfers of Customer Personal Data to which the Alternative Mechanism applies.

5.4. In addition, Cendyn is certified to the EU-U.S., UK Extension to the EU-U.S., and Swiss-U.S. Data Privacy Frameworks and the commitments entailed. Cendyn agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Frameworks.

6. GENERAL TERMS

6.1. **Governing Law.** This DSA is governed by and shall be construed in accordance with the laws of the state of Delaware. Each Party submits to the non-exclusive jurisdiction of the state and federal courts of Wilmington, Delaware.

6.2. Notice.

(a) Notice to Customer: Cendyn will send any notice made by Cendyn under this DSA to the data protection contact designated by the Customer.

(b) Notice to Cendyn: Any notice made by Customer will be provided in writing to the contact listed below.
Chief Legal Officer
301 Yamato Road, Suite 3194, Boca Raton, FL 33431, USA
Email: DPO@cendyn.com, with a copy to legal@cendyn.com

6.3. **Prior Existing Agreement.** This DSA supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations, and agreements, oral and written, with regard to this DSA's subject matter.

6.4. **Survival.** This DSA's termination or expiration shall not affect any rights or liabilities that accrued prior to such termination or expiry, or the coming into force, or continuance in force, of any term that is expressly or by implication intended to come into, or continue in force, on or after termination or expiry.

6.5. **No Waiver.** Delay in exercising, or failure to exercise, any right or remedy in connection with this DSA shall not operate as a waiver of that right or remedy.

6.6. **Severability.** If any part of this DSA is found to be legally invalid or unenforceable, it will be replaced with a valid provision that best reflects the original intent, and the rest of the DSA will remain in effect.

6.7. **Conflicts.** In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this DSA, the provisions of this DSA shall prevail. In case of any conflict or ambiguity between the jurisdiction specific terms in **Exhibit A** and any other terms of this DSA, the applicable jurisdiction specific terms in **Exhibit A** will prevail.

6.8. **Ambiguity.** Cendyn may amend this DSA without notice to or consent of Customer for the purposes of: (a) curing any ambiguity; (b) curing, correcting or supplementing any defective provision of the DSA; or (c) making any other provisions with respect to matters or questions arising under this DSA; provided that such action shall not materially alter the DSA.

6.9. **Online Hosting and Amendment.** Subject to this DSA, Cendyn may host the content of the DSA and its exhibits online and further update the DSA and exhibits in order to ensure that Parties comply with Applicable Data Protection Laws. The online DSA or exhibit is considered by the Parties as the latest version, and the Parties agree that the online version takes precedence over the relevant DSA or exhibit originally agreed to by the Parties.

6.10. **Disclosure to Supervisory Authorities.** The Parties acknowledge that either Party may disclose this DSA and any relevant privacy provisions in the Agreement to Supervisory Authorities, or any other judicial or regulatory body, upon their request.

7. EXHIBITS AND APPENDICES

A. Exhibit A - Jurisdiction Specific Terms;
B. Exhibit B – Supplementary Measures to the Standard Contractual Clauses; and
C. Exhibit C - Security Measures.

Exhibit A – Jurisdiction Specific Terms to the Controller to Controller Data Sharing Agreement

1. **Europe**

1.1. **Definitions**

(a) "**EEA**" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(b) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EU and the EEA countries applicable to transfer of personal data.

(c) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 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.

(d) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as may be amended from time to time.

(e) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

(f) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection.

(g) "**UK Data Protection Laws**" includes the Data Protection Act 2018 and the UK GDPR.

(h) "**UK GDPR**" means the United Kingdom General Data Protection Regulation, 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.

(i) "**UK ICO**" means the UK Information Commissioner's Office.

(j) "**UK Transfer Addendum**" means the International Data Transfer Addendum (version B1.0) to the European Union Commission's EU 2021 Standard Contractual Clauses issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

1.2. To the extent that the Parties transfers personal data subject to EEA Data Protection Laws, Swiss Data Protection Laws, or UK Data Protection Laws, outside the EEA, Switzerland, or the United Kingdom, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) Certification of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, or any successors thereto (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the relevant Data Privacy Framework), provided that the transfers are covered by the self-certification;

(b) A valid adequacy decision adopted by the European Commission, UK ICO, or FDPIC (as applicable);

(c) The appropriate SCCs adopted by the European Commission, UK ICO, or FDPIC from time to time; and

(d) Any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws, UK Data Protection Laws, or Swiss Data Protection Laws.

1.3. **European Economic Area - Standard Contractual Clauses**

(a) The DSA hereby incorporates by reference the EU 2021 SCCs.

(b) The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(c) The Parties agree that any references to clauses, annexures, modules and choices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated EU 2021 SCCs, as may be applicable from time to time pursuant to the DSA.

(d) For the purposes of the EU 2021 SCCs and any substantially similar SCCs which may be adopted by the relevant authorities in the future:

i. Each party sending personal data shall be deemed the "data exporter" and each party receiving personal data shall be the "data importer."

ii. The Parties agree to apply Module One with respect to Controller-to-Controller transfers.

iii. Clause 7: The Parties choose to include the optional docking clause.

iv. Clause 8: The technical and organizational measures are described in Section 3 of the DSA.
v. Clause 11: The Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.
vi. Clause 13 (Annex I.C): The competent Supervisory Authority shall be the competent Supervisory Authority in the jurisdiction where the data exporter is established. If the data exporter is not located in the EEA, the competent Supervisory Authority shall be the competent Supervisory Authority in the jurisdiction where data exporter's data protection representative in the EEA under Article 27 EU GDPR is established. If the data exporter is not established in an EEA country, its processing activities are subject to the EU GDPR by virtue of application of Article 3(2) EU GDPR, and the data exporter does not have a data protection representative under Article 27 EU GDPR, the data exporter chooses the Republic of Ireland as its competent Supervisory Authority for the purposes of Clause 13 and Annex I.C.
vii. Clause 17: The EU 2021 SCCs shall be governed by the laws of the Republic of Ireland.
viii. Clause 18: Any dispute arising from the EU 2021 SCCs shall be resolved by the courts of the Republic of Ireland.

(e) The terms contained in **Exhibit B** to the DSA supplement the SCCs.
(f) In cases where the EU 2021 SCCs apply and there is a conflict between the terms of the DSA and the terms of the EU 2021 SCCs, the terms of the EU 2021 SCCs shall prevail.

1.4. **Switzerland - Standard Contractual Clauses**

(a) The DSA hereby incorporates by reference the EU 2021 SCCs, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).
(b) The Parties incorporate and adopt the EU 2021 SCCs for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms, subject to the following:
i. Clause 13 (Annex I.C): The competent authority shall be the FDPIC.
ii. Clause 17: Under Option 1 of module one, the law of the Swiss Confederation.
iii. Clause 18: The Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland. The Parties choose the Swiss courts as an alternative place of jurisdiction for data subjects habitually resident in Switzerland.
iv. The Parties' selection of forum may not be construed as forbidding data subjects habitually resident in Switzerland from suing for their rights in Switzerland.
v. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there are any Restricted Transfers subject to Swiss Data Protection Laws.
(c) In cases where the EU 2021 SCCs apply and there is a conflict between the terms of the DSA and the terms of the EU 2021 SCCs, the terms of the EU 2021 SCCs shall prevail.

1.5. **United Kingdom - EU 2021 SCCs and UK Transfer Addendum**

(a) This DSA hereby incorporates by reference the EU 2021 SCCs which have been adopted for use by the UK ICO with certain modifications and the addition of the UK Transfer Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).
(b) For the purposes of the tables to the UK Transfer Addendum:
i. Table 1: The content of Table 1 is set out in the Agreement.
ii. Table 2: The content of Table 2 is incorporated and adopted as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms.
iii. Table 3: The content of Table 3 is set forth as follows:
i. Annex 1: The content of Annex 1 is set out in the Agreement.
ii. Annex II: The content of Annex II is set out in Section 3 of the DSA.
iv. Table 4: The Parties agree that neither party may terminate the UK Transfer Addendum.

(c) The Parties incorporate and adopt the EU 2021 SCCs as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be UK ICO.

ii. Clause 17: The EU 2021 SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.

iii. Clause 18: Any dispute arising from the EU 2021 SCCs, or the incorporated UK Transfer Addendum, shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The terms contained in **Exhibit B** to the DSA supplements the EU 2021 SCCs.

(e) In cases where the EU 2021 SCCs, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of the DSA and the terms of the EU 2021 SCCs or UK Transfer Addendum, the terms of the UK Transfer Addendum shall prevail.

2. United States of America

2.1. **Definitions**

(a) **"United States Data Protection Laws" include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the processing of personal data, as may be amended from time to time, and their implementing regulations. Such laws include, without limitation:**

i. The California Consumer Privacy Act (the "**CCPA**")
ii. The Colorado Privacy Act
iii. The Delaware Personal Data Privacy Act
iv. The Indiana Consumer Data Protection Act
v. The Iowa Consumer Data Protection Act
vi. The Montana Consumer Data Privacy Act
vii. The Oregon Consumer Privacy Act
viii. The Tennessee Information Protection Act
ix. The Texas Data Privacy and Security Act
x. The Utah Consumer Privacy Act
xi. The Virginia Consumer Data Protection
xii. The U.S. state data breach notification statutes

(b) "**Breach of Security**" and "**Breach of the Security of the System**" have the meaning set forth under applicable United States Data Protection Laws.

2.2. **Obligations Related to the Sales of Personal Data**. To the extent that a disclosure of personal data among Controllers qualifies as a sale under Applicable Data Protection Laws, each Party must comply with the obligations associated with the sale of personal data under such Applicable Data Protection Laws.

3. Transfers of Non-European and Non-U.S. Data

3.1. Where either Party intends to conduct a Restricted Transfer and Applicable Data Protection Law requires certain measures to be implemented prior to such transfer, the data exporter agrees to implement such measures to ensure compliance with Applicable Data Protection Law.

Exhibit B -Supplementary Measures to the Standard Contractual Clauses

By this Exhibit B the Parties provide additional safeguards and additional redress to the data subjects to whom Customer Personal Data and Knowland Data relates. This Exhibit B supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses set out in **Exhibit A** that may be applicable to the Restricted Transfer.

1. **Applicability of Exhibit B**
   This Exhibit B only applies with respect to Restricted Transfers where the terms of **Exhibit A** indicate it.
2. **Definitions.** For the purpose of interpreting this Exhibit B, the following terms shall have the meanings set out below:
   2.1. "**DSA"** means the Controller to Controller Data Sharing Agreement that incorporates this Exhibit B.
   2.2. "EO 12333" means the U.S. Executive Order 12333.
   2.3. "FISA" means the U.S. Foreign Intelligence Surveillance Act.
   2.4. "Schrems II Judgment" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.
3. **Applicability of Surveillance Laws**
   3.1. Data importer represents and warrants that, as of the DSA Effective Date, it has not received any national security orders of the type described in paragraphs 150-202 of the Schrems II Judgment.
   3.2. Data importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:
      (a) no court has found the data importer to be an entity eligible to receive legal process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4) or (ii) an entity belonging to any of the categories of entities described within that definition;
      (b) if data importer were to be found eligible for FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II Judgment; and
      (c) EO 12333 does not provide the U.S. government the ability to order or demand data importer to provide assistance for the bulk collection of information and data importer shall take no action pursuant to EO 12333.
4. **Backdoors**
   4.1. Data importer certifies that:
      (a) it has not purposefully created back doors or similar programming that could be used to access data importer's systems and/or data exporter's personal data subject to the applicable EU 2021 SCCs;
      (b) it has not purposefully created or changed its business processes in a manner that facilitates access to data exporter's personal data or systems; and
      (c) national law or government policy does not require data importer to create or maintain back doors or to facilitate access to data exporter's personal data or system.
   4.2. Data exporter will be entitled to terminate the Agreement on short notice in cases in which data importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform data exporter once their existence comes to its knowledge.
5. **Information about legal prohibitions.** Data importer will provide data exporter information about the legal prohibitions on data importer to provide information under this Exhibit B. Data importer may choose the means to provide this information.
6. **Obligations on Data Importer in the Event of Receiving a Disclosure Request.**
   6.1. In the event data importer receives an order from any third party for compelled disclosure of any personal data received from data exporter subject to the DSA that has been transferred under the

Standard Contractual Clauses, data importer shall comply with the following, unless prohibited under the law applicable to data importer:

(a) Promptly and, when possible, before granting access to the transferred personal data, notify data exporter, unless prohibited by law, or, if prohibited from notifying data exporter, data importer shall use all lawful efforts to obtain the right to waive the prohibition to communicate information relating to the order to data exporter as soon as possible. This includes, but is not limited to, informing the requesting public authority of the incompatibility of the order with the safeguards contained in the Standard Contractual Clauses and the resulting conflict of obligations for data importer and documenting this communication.

(b) Use every reasonable effort to redirect the third party requesting the disclosure of any personal data from the data exporter that has been transferred to data importer directly to data exporter.

(c) Use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable EEA Member State law or any other Applicable Data Protection Laws. For the purpose of this Exhibit B, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

(d) Seek interim measures with a view to suspend the effects of the order until the competent court has decided on the merits.

(e) Not disclose the requested personal data until required to do so under the applicable procedural rules.

(f) Provide the minimum amount of information permissible when responding to the request, based on a reasonable interpretation of the request.

(g) Document all the steps taken by data importer related to the disclosure request.

7. **Inability to Comply with this Exhibit B**. If data importer determines that is no longer able to comply with its contractual commitments under this Exhibit B, data importer must promptly inform data exporter and data exporter can swiftly suspend the transfer of data and/or terminate the DSA.
8. **Termination**. This Exhibit B shall automatically terminate with respect to the personal data transferred in reliance of the EU 2021 SCCs if the Supervisory Authority or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted Transfers covered by the EU 2021 SCCs (and if such mechanism applies only to some of the data transfers, this Exhibit B will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Exhibit B.

Exhibit C – Security Measures

A. Introduction and Objectives

Cendyn has implemented corporate information security practices and standards that are designed to safeguard Cendyn corporate environment and to address business objectives across information security, system and asset management, development, and governance.

These practices and standards are approved by Cendyn executive management and are periodically reviewed and updated where necessary. As such, this document and its objectives may change accordingly.

A-1 Technical Organization Measures

As stated in Article 32 of the GDPR under "Security of processing" it is required that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".

Cendyn has structured this overview of its technical and organizational measures into the following categories:

- Organizational control
- Physical access control
- System access control
- Data access control
- System security control

A-2 Structure of the Document

This document is divided into three sections, first the document structure topics, second the Management initiatives and third the TOM-structured categories outlined above.

B. Applicability

B-1 Scope

This document outlines the security policies, practices, and controls in place for Cendyn platforms and applications.

B-2 Target Groups and Audiences

This document is mandatory directed to all employees of Cendyn. Employees are bound to the requirements based on this document. External parties and partners must also apply with these requirements.

B-3 Trust Commitment

Cendyn is committed to protecting the data that our customers have entrusted us with. Safeguarding the private information of individuals is also paramount. Cendyn warrants that it has in place physical, administrative safeguards and procedures to protect the confidentiality of all personal and confidential information of a customer. Cendyn maintains an Information Security Management System (ISMS) that addresses:

- User access and identity management
- Vulnerability management
- Change management
- Business continuity
- Physical security
- Network management
- Cryptography
- Human resources
- Incident response

All Cendyn employees with access to personal data are subject to confidentiality obligations which extend beyond cessation of the employee's employment with Cendyn.

B-4 Implementation

Data privacy documents are reviewed in yearly iterations or with required changes, whatever applies first. All data privacy related documents are reviewed and accepted by our DPO.

C. General Security Management

C-1 Risk Management

The Cendyn Risk Management program is divided into four phases:

- Risk Program executive-level authorization
    - Authorization and Support for beginning the risk management process.
    - Determine risk context (external and internal threats, existing controls, risk acceptance criteria).
- Risk identification

    - Identify the criticality of each asset group and impact of loss.
    - Determine risk owners and identify the risks applicable to each asset group.
    - Select the mitigation controls for each risk and their maturity level.
- Risk analysis and evaluation
    - Determine the level of risk, depending on the asset impact and risk likelihood.
- Risk treatment
    - Select the risk treatment options considering the risk assessment results and the risk acceptance criteria.

C-2 Data Residency

Cendyn's platforms are hosted and running on servers and hardware that we own and/or cloud technology we fully manage. For hardware we own: we house our equipment in a Tier 5 facility owned and managed by 365 Data Centers located at 3500NW Boca Raton Blvd, Building 900, Boca Raton, FL 33431. For Cloud technology, we leverage Azure, AWS, or GCP in the USA, EU, and APAC regions.

C-3 Audits and Certifications

Cendyn requires that 365 Data Center maintain SOC 2 audit standards.

Facility information can be reviewed here https://www.365datacenters.com/boca-raton-data-center/

Azure Compliance offerings https://docs.microsoft.com/en-us/azure/compliance/offerings/

AWS Compliance offerings https://aws.amazon.com/blogs/security/new-soc-1-2-and-3-reports-available-including-a-new-region-and-service-in-scope/

C-4 Security Policies and Procedures

Cendyn adheres to a comprehensive security policy framework. This framework includes standards for access control, HR processes, environmental/physical security, communications and network security, cryptography, software development, incident management, business continuity, vulnerability management, and data privacy. Cendyn's security policy framework is reviewed on a regular basis.

C-5 HR Policies

A Cendyn HR Specialist conducts background investigation for all new hires as well as existing personnel in critical roles or those who have access to sensitive information. The background check includes employment verification, educational and license or credential verification, criminal history, reference checks, and other pertinent information.

Employees are required to sign an employee contract, Code of Conduct, Employee Handbook, and participate in security awareness training.

New employee (Onboarding)

Cendyn follows the principle of least privilege. As new employees are onboarded only the required set of system permissions are granted. Authorization badges and/or keys are handed over by HR and/or the responsible department.

Termination of employee (Offboarding)

All permissions granted are terminated and login access is inactivated on the last day of employment or when their contract ends – whatever comes first. Access badges, keys, IT equipment and any other company assets are returned to HR and IT.

Job role and responsibilities changes

All permissions required for the previous role are rejected as the job change takes place.

Received access badges and keys must be authorized by HR on necessity for the new role. All permissions required for the new role and responsibility are granted by the time the previous permissions are taken.

C-6 Secure Supplier Evaluation

Cendyn conducts a review of service providers periodically. This review evaluates the security, privacy, service levels, and IT controls.

D. System Security Management

D-1 Data Classification and Handling

Cendyn's Asset Management policy defines a set of rules that help protect the confidentiality of information Cendyn processes. The rules set out in the policy describe several methods to protect data, such as controlling the access to sensitive and confidential information and protecting sensitive or confidential information. It is the responsibility of all Cendyn employees to classify their information and ensure appropriate measures to handle and protect data. The information lifecycle consists of:

- Labeling: Categorization of private, sensitive, public or unclassified
- Usage scope: Cendyn Internal or Client Data by application use
- Method of Transfer and encryption requirements
- Disposal

D-2 Change Management

Cendyn leverages documented processes and system-based Microsoft Operations Framework to ensure that all environmental changes are documented, tested, reviewed, and approved. A defined maintenance window is used for applying changes to systems in the environment, along with a communication plan informing all stakeholders of pending changes. System rollback procedures include backups before making any changes in addition to the regular nightly backups. The Change Management process involves four phases to deploy updates or fixes to the production environment.

- Communication
  - The technical owner proposing changes documents the change, including the requested change date, deployment owner and deployment manager.
- Deployment
  - The deployment steps are outlined with detailed steps to deploy changes to the application or environment.
- Test
  - The test plan describes the steps to take to confirm that the changes have been completed successfully. If the test plan fails, the technical owner determines whether to roll back the changes or continue troubleshooting.
- Rollback
  - The rollback plan describes the steps to revert the changes using a backup or snapshot created in the deployment phase.

Cendyn only makes changes to Cendyn Applications during scheduled maintenance windows.

D-3 Software Development Lifecycle

The Cendyn Software Development Lifecycle (SDLC) describes the processes in place to develop software in a secure manner. The SDLC model consists of several distinct stages including planning, design, building, testing, and deployment with security throughout the development process. Below is an outline of how we handle updates to Cendyn products.

- Planning and Requirements Analysis
  - Requirement analysis is performed by the senior members of the team with inputs from the customer and product subject matter expert. This information is then used to plan the basic project approach.
  - Planning for the quality assurance requirements and identification of the risks associated with the project is also done in the planning stage.
- Defining Requirements
  - Once the requirement analysis is done the next step is to clearly define and document the product requirements and get them approved from the Customer and/or the product manager. This is done through a BRD (Business Requirements Document) or other agile artifacts which consists of all the product requirements to be designed and developed during the project life cycle.
- Designing the change to product architecture (if required)
  - BRD is the reference for product architects to come out with the best architecture updates, if required. The design approach for the updated architecture is proposed and documented in a DDS – Design Document Specification.
  - This DDS is reviewed by all the important stakeholders and based on various parameters such as risk assessment, product robustness, design modularity, budget and time constraints, the best design approach is selected for the product.
  - A design approach clearly defines all the architectural modules of the product along with its communication and data flow representation with the external and third-party modules (if any). The internal design of all the modules of the proposed architecture should be clearly defined with the minutest of the details in DDS.

- Building or Developing the Product
    - In this stage of SDLC the actual development starts utilizing the Agile Model and product changes commence. The programming code is generated as per DDS during this stage.
    - Developers will follow Cendyn development guidelines.
- Testing the Product
    - While all stages have testing, this stage refers to the testing only stage of the product where product defects are reported, tracked, fixed and retested, until the product reaches the quality standards defined in the BRD.
- Deployment and Maintenance
    - Once the update is tested and ready to be deployed it is released formally in production with communication sent to clients.

D-4 Patch Management

Cendyn patch policy utilizes three tools to automate our patch management program. Each server is updated monthly.

- VMware provides scheduled snapshots of the server before a patch.
- Kaseya automates the approved patch utilizing a Patch Policy Membership that each server is assigned.
- PDQ is used to confirm that new patches have been installed.
- Cloud based systems provide for automated regular patching cycles.

D-5 Vulnerability Management

Cendyn corporate policy outlines the process and procedures to be followed when implementing a vulnerability management program. The policy is documented and divided into sections that identify, classify, remediate and mitigate vulnerabilities.

The core vulnerability management requirements:

- Documenting the roles and responsibilities associated with technical vulnerability management, including asset inventory, vulnerability monitoring, vulnerability risk assessment, remediation and mitigation, and any coordination responsibilities required.
- Performing vulnerability scanning to detect vulnerabilities.
- Classifying, remediating and mitigating the identified technical vulnerabilities.
- Implementing vulnerability management prior to enabling internet facing infrastructure or web applications.
- Implementing vulnerability management for major changes to the environment.
- Reporting status to management.
- Ensuring the vulnerability management procedure is an auditable process.

Vulnerability Scans are run monthly.

D-7 Penetration Test Management

Cendyn will perform penetration testing annually utilizing a trusted third-party vendor. Identified vulnerabilities will be addressed following the Cendyn vulnerability management program to identify, classify, remediate and mitigate vulnerabilities. Patch management is a component of the remediation plan within the vulnerability management policies. Patches are deployed to systems with the highest level of exposure and potential impact. All patches are deployed to development, QA, staging and finally production once all testing has been completed.

Targeted Vulnerability Scan and Penetration Testing Remediation Timeframes:

Critical	Fix or find remediation within two to four weeks from the date it was found
High	Fix or find remediation within two months from the date it was found
Medium	Fix or find remediation within 3 to 6 months from the date it was found
Low	At the discretion of the representative: no action, fix or find remediation within 6 to 12 months from the date it was found
Info	No action unless representative has a different reason/opinion

D-8 Incident Management

The Cendyn Incident Response Plan provides guidance for handling and communicating computer security incident responses at Cendyn. The Cendyn Incident Response Plan will be activated whenever a security incident occurs and guides the responses to all incidents whose severity is such that they could affect Cendyn's ability to

do business, undermine its reputation or result in a financial impact to the company. It is the responsibility of every employee and contractor of Cendyn to immediately report any security incident to the Support Team. Cendyn Support will work to resolve issues with malicious or unintentional alteration of data.

Intrusion Detection System

- Cendyn has implemented the Cisco FireSIGHT module at the ASA Firewalls which record all permitted and denied Intrusion Detection/Prevention events as determined by the Cisco Sourcefire IDS/IPS ruleset. The Cisco FireSIGHT module also does Application Firewall protections (i.e., SQL Injection, cross site scripting, etc.) for known and unknown vulnerabilities.
- Cendyn has also enabled the threat detection & protection to feature at the Cisco ASA perimeter firewalls to help mitigate DoS and other mass bot-net attacks. If the scanning threat rate is exceeded, then the ASA sends a system message, and shuns (blocks) the attacker for 30 minutes.
- We have a centralized log correlation via TrustedMetrics Services; alerts go out for suspicious activity at the network level and proper personnel take proper action and/or follow up. We also block IPs by monitoring load balancer logs to determine suspicious activity and if a pattern for non-trusted IPs is triggered; initiate the auto-shun (block) of such IPs at the Firewall.
- URl Filtering / URL Blocking: Cendyn has enabled the Cisco URL filtering feature at the firewall level to identify and control access to web (HTTP and HTTPS) traffic.
- FIM Alerts: changes to specific directories/shares, including new files, deleted files and modified files.

Response Team

Name/Team	Role/Title	Role and Responsibility of the Incident Response Team
Trusted Metrics	Cendyn Partner	Review of Logs (Security & Others). Always watching for anomalous behavior, so when things seem out of the ordinary, alerts go out.
Cendyn Support Team	Support Team	Responsible to audit alerts from multiple monitoring systems to analyze and validate a threat, error, etc. Once an issue is validated; escalate, triage & follow up until proper resolution is found.
IT Management	Senior Director, IT	Ensure Incident Response Plan is executed correctly. If there are any incidents, communicate with VP and executive teams.
IT Department	IT Team	Assist with investigation/ remediation of incident.
DEV Department	DEV Team per Product	Assist with investigation/ remediation of incident.
VPs	Company VPs	Correspond with clients as necessary and provide Support to VP of IT as needed.

The following documented response mechanisms serve as the Standard Operating Procedures for responding to any incident within the organization:

1. For any incident that has been detected, the Incident Response Team is to be immediately notified via Text Service and Communication Bridge opened.
2. The Incident Response Team is to formally assume control and to identify the threat and its severity to the organization's information systems.
3. In identifying the threat, the Incident Response Team is to specifically identify which resources, both internal and external, are at risk and which harmful processes are currently running on resources that have been identified as at risk.
4. The Incident Response Team is to determine whether the resources at risk (hardware, software, etc.) require physical or logical removal. Resources posing a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically. Resources that may require physical or logical removal or isolation may include, but are not limited to, the following:
    - All IP addresses in use

- Firewalls
- Routers and switches
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Any enterprise-wide applications (CRM systems, etc.)
- Remote access
- Point-to-point secure data transmission methods used for data traversing back and forth on the network
- Wireless networking or networks
- Authentication servers (RADIUS)
- Web servers
- Proxy servers
- File servers
- Email servers
- DNS servers
- Operating systems
- Databases
- Applications

5. If the incident is identified as a DDoS attack, Cendyn should first contact R2 and then the ISP per the incident response plan.
6. If the incident has affected the PCI environment in any way, and has impacted the system components within this environment, Cendyn must immediately report the incident, its severity and other essential information to the major credit card payment brands (Ovations only).
7. Notify affected client contacts immediately after discovery of a breach, serious attempt to breach, unauthorized disclosure, or security incident which would compromise personally identifying information or other sensitive information such as payment card data. Do not notify or contact any customers directly without the authorization of the client.
8. If the incident has in any way resulted in a criminal matter that may be readily identified, Cendyn must immediately report it to law enforcement officials, such as the following:
    - Local law enforcement
    - The United States Secret Service (for credit card fraud)
    - The Federal Bureau of Investigation (FBI)
9. Investigating the incident is also a critical process within the Incident Response Plan. Proper investigative techniques are to include, but are not limited to, the following:
    - Understanding how the incident occurred and what led to the compromise.
    - Reviewing all necessary system documentation such as logs, audit trails, rule sets, configuration and hardening standards and all other supporting documentation.
    - Interviewing personnel as needed.
    - Examining any third-party providers and their respective products and services that are utilized within Cendyn's network architecture.
    - If warranted, a third-party resource for assisting in the investigation of the incident may be utilized (this will be done at the management's discretion).

Recovery from an Incident

Recovery procedures will include but are not limited to the following:

- Restoring systems from clean backups (a trusted source only).
- Completely rebuilding systems as needed and warranted.
- Replacing systems as needed (this includes all system components within the personally identifying information or cardholder data environment and any other IT resources deemed critical by Cendyn).
- Reconfiguring network security (stronger, more adaptive configuration and hardening rules) for all system components within the personally identifying information or cardholder data environment and any other IT resources deemed critical by Cendyn.

The recovery procedures will be commensurate with the incident that has occurred. This will be conducted on a case-by-case basis with all aspects of the recovery process fully documented.

Post-Incident Activities and Awareness

A formal and documented Root Cause Analysis (RCA) is to be compiled and given to management of Cendyn within an acceptable timeframe following the incident. The RCA must contain the following elements:

- What happened: a detailed description of the incident.
- Root cause: a description of the root cause.
- Resolution: steps taken for restoring affected systems.
- Timeline: timestamps from start to finish, including all important times from the incident.
- Impact: specific systems, accounts, and users affected by the challenge.
- Communication: reporting of the incident for all relevant third parties as needed.
- Lessons to Learn: A list of items, positive or learning touch points, from which Cendyn can take to improve systems and processes and hopefully eliminate the likelihood of future incidents.

All RCA documents will be stored in Salesforce and reviewed monthly by the INFOSEC Committee.

D-9 Disaster Recovery and Business Continuity

Cendyn participates in a corporate-wide program for business continuity planning. Critical business processes and the resources required to support those processes are inventoried. For each process and resource, an alternative is identified, such as a corresponding team at another site that can provide Support in the case of a business interruption until service is restored. Gaps are identified and addressed according to the documented process.

1. Organizational Controls

1-1 Contractual Base

Contract

Cendyn offers services on the basis of standardized contracts which fits our service design and the legal requirements.

The contracts are updated to incorporate any changes in the applicable law or in the general service design / technical functions. Changes are communicated transparently with the customer.

Terms & Conditions

The general Terms & Conditions define more specifically how the SaaS service is delivered, and which arrangements apply. Changes are communicated transparently with the customer.

Service Level Agreements

The SLAs define in a specific form the reaction and support levels on the basis of the severity of requests and escalation. Changes are communicated transparently with the customer.

Data Processing Addendum

The Cendyn DPA (available at https://www.cendyn.com/cendyn_customer_dpa/) defines in a standardized form the processing of customer personal data. Changes are communicated transparently to customers.

1-2 General Data Usage

Cendyn does not process PII without prior written consent of the owner. Cendyn requires customers to gain the consent for the submitted data which is specified in the contracts. Customers and or partners utilizing Cendyn services are required to obtain consent for the data to be processed.

1-3 Defined Overview of Sub-processors

Active service providing partners processing personal data on behalf of Cendyn, when Cendyn processes personal data on behalf of its customers, are added to a sub-processors list: https://www.cendyn.com/subprocessors_list/.

1-4 Security Awareness Training

All Cendyn employees are required to attend annual mandatory security awareness training. Training includes awareness of data privacy policies and issues, safe email and browsing habits, phishing and social engineering, and proper procedures for reporting security issues. Additionally, development staff are required to attend annual mandatory Secure Code Training

In addition to mandatory training, Cendyn employees receive weekly security notices outlining recent known threats on the internet and receive test phishing emails biweekly. Failure of the phishing test requires additional training.

2. Physical Controls

Cendyn has defined appropriate organizational (accompanying externals) and technical measures (key card token system) to protect against unauthorized physical access.

2-1 Definition of Security Areas

General

General areas can be accessed by all employees with their authorization badge.

The access is always bound to the exact location of employment.

Cendyn's sites are protected with electronic security, intrusion alarms, and fire detection equipment. Cendyn's data centers provide state-of-the-art innovative architectural and engineering methodologies and are housed in nondescript facilities as an added security measure.

Restricted

Restricted areas can only be accessed by authorized employees with separated access mechanisms (e.g., different authorization badges, keys).

365 Data Center physical access to the facility by requiring ID badges that are scanned for entry. Visitors require advance notice and proper ID and must enter through a reception area. They are required to sign in, and ID is matched to the advance reservation.

Additionally, physical access to the data centers is strictly controlled at building ingress points by professional security staff utilizing video surveillance and other electronic means like ID reader, magnetic or chip cards and door locking mechanisms. Once within the data center, access is further restricted as Cendyn's equipment is contained within locked cabinets. Without the required key, nobody can access Cendyn's locked cabinets. All physical access to the premises is logged and audited routinely. Physical locations of Cendyn's data centers are carefully selected with co-location partners that meet or exceed the following standards:

- SSAE16 SOC1/2 – Type 2;
- PCI DSS Level 1; and
- Uptime Institute – Tier III.

In addition to requiring badges, all data centers require biometrics to gain physical access to the data center. The parking and surrounding areas of the data centers are inaccessible without a badge. All data centers have CCTV as well as fully auditable access logs. The data center racks themselves are also protected with locking front and rear doors. All cross connects and intra-cabinet cabling is completely shielded and secured.

3. System / Data Access Control

Cendyn has defined appropriate technical (e.g., login credentials) and organizational measures (e.g., access permissions through group policy based on AD groups) to protect against unauthorized system access.

3-1 Operational Measures

The following operational measures are in place to ensure technical and organizational security for user identification and authentication:

- Physical locations housing employees do not have direct network, VPN, etc. access to the server/data centers;
- Access to servers is controlled with client VPN, as well as maintenance of local workstation compliance leveraging Cendyn's configuration management tools;
- Client VPN is protected with MFA, UserID/Password and Duo;
- Server access once past all VPN controls, is then maintained with SSH keys; and
- Once in Cendyn's network, to access servers, a second VPN tunnel is established, to access production data. This is also protected with MFA but leverages a different UserID/Password combination.

3-2 Architecture and Data Segregation

Cendyn production and non-production environments are separated as required by policy. The systems exposed to the internet are kept isolated from internal systems that process and store data. The internal systems have several layers of protection including multiple firewall devices, access control lists, and intrusion detection systems. Access to network devices for management purposes are only provided through a logical and separate administration network.

Cendyn separates development, QA, staging, and production networks to reduce the risk of unauthorized access to, or changes in production. Segregation of duties is implemented to minimize the risk of negligence and to prevent intentional abuse of systems.

Cendyn customer data is separated by server and logical controls within the application.

Client data is retained per client request. All client data is routinely saved until the client is no longer contracted with Cendyn when it is purged and deleted. Some clients prefer a systematic purge and delete which can be set up and run to the client specifications.

3-3 Access Management

Cendyn corporate policies provide guidelines for managing access management, privileged access, and handling initial passwords.

Cendyn corporate policies provide guidelines to manage the identity lifecycle, access management, privileged access, handling of initial passwords, and identity de-registration:

Access Management

Formal access management processes and procedures are required to allocate the lowest level of system access rights required to allow the user to fulfill the assigned duties.

Privileged Access

Formal processes and procedures are required for the secure usage of privileged access. Management is responsible for the setup and operation of every user account with privileged access rights. The approval and usage of privileged accounts is based on need-to-use, need-to-handle, and least privilege principles. Users with privileged accounts are kept to a minimum. Multifactor authentication is enabled and implemented to get access to more critical infrastructure and/or secure environments.

Product Access – Hotel Users

Admin Role has single property access to all functionality plus access to add/remove users and to view all users and proposals.

Non-Admin Role has access to all functionality for themselves only.

Handling of Initial Passwords

A formal password provisioning procedure is required to securely allocate initial passwords to users. Every Cendyn user account must have a unique initial password assigned to the user and must be communicated to the user in a secure manner. The initial password is only temporary and must be changed by the user upon first logon.

Admin user password security

Password requirements:

- Cannot be all digits.
- Cannot be all lowercase letters.
- Cannot be all Uppercase letters.
- Cannot be all Mix letters.
- Cannot be all Uppercase letters (this includes numbers).
- Cannot be all lowercase letters (this includes numbers).
- Must be more than 6 characters.
- Must be less than 15 characters.
- Cannot contain ‘password’, including leet variants.
- Cannot contain ‘qwerty’, including leet variants.
- Cannot be simple word with 123…
- Cannot be simple word with 123 or 1234… prepended.
- Cannot be simple word with 1’s appended.
- Cannot be simple word with 1’s prepended.
- User is locked out after five incorrect attempts.

Cendyn corporate policies define security mechanism requirements for accessing Cendyn systems and applications to avoid or impede unauthorized access. The policy outlines the controls in place including secure log-on procedures, password management systems, use of privileged utility programs, and access control to program source code.

All usernames and passwords are created and altered from generally recognized principles and no username is reused within a period of at least 4 months since the username was last in use. If at any time an employee has not used their username within a period of 3 months, the username will automatically be suspended. Cendyn employees with access to the IT solution are covered by a strict password policy. All system access passwords must be unique from the user's last 24 passwords and must be changed at least every 3 months.

Secure log-on procedures

Systems and technical owners implement and manage secure log-on procedures/measures to support control and minimize access to Cendyn systems. Examples would include:

- The number of unsuccessful log-on attempts is limited to a maximum of five attempts.

- The passwords are not transmitted in plain text over any network.

Password Management Systems

- The password procedure enforces complex passwords.

Access control to program source code

- Technical owners implement and manage procedures for access to the source code to prevent the introduction of unauthorized functionality and to avoid unintentional changes, access to the program source code.
- All changes to the application are strictly controlled and follow the appropriate change process.
- Access to the source code and associated items (e.g., designs, specifications, verification plans, validation plans, etc.), are granted on a need-to-know basis and strictly controlled.

The source code is centrally managed, and access is logged.

Disclosure Control

Data transfers occur via a secure VPN or over a company-owned network. When Cendyn employees access Cendyn systems, connections are secured through encryption. Any access to Cendyn's IT systems requires that the employees register a username and a password. All data transfers are audited and must be business justified and limited to the minimum necessary data.

Input Control

Cendyn employs measures to log the username, time, type of application, and the person that data is concerning, to ensure all access to personal data is kept on record. Cendyn maintains logs for a minimum of 6 months, which are deleted after a maximum of 7 months. All system, security, network, and application logs are streamed in real time to an outsourced SIEM. This SIEM alerts on all predefined incidents/patterns with an SLA of 15 minutes.

Availability Control

Cendyn secures stored data through the regularly scheduled backup of stored data. The backup is conducted as a mix of full backup and incremental backup. Cendyn regularly conducts tests of previously completed backups to ensure that the backup routines function as intended. For safety reasons, critical backups are also duplicated and stored in another data center from the same provider in the same country and region. For systems that are hosted in the cloud, backups are taken and stored by the cloud provider automatically.

Cendyn's data centers electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Pegasus ´s business continuity procedures include backup copies at alternate data centers, with pre-configured servers available if operations need to be shifted between data centers.

Climate control is required to maintain a constant operating temperature for the servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. Electrical, mechanical, and life support systems and equipment are monitored so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

4. System Security Controls

4-1 Cryptography

Cendyn corporate policies define the requirements for cryptographic algorithms, protocols, and handling the underlying cryptographic keys (generation, use, protection, selection, and lifetime). The requirements are based on industry best practices. Various methods are being utilized to secure data at rest and in transit.

Cendyn products provide a minimum of TLS 1.2 to encrypt data in motion and industry-standard AES 256 or higher for data at rest. Regarding data backup, we use Dell/EMC SAN devices in our 100% Virtual Infrastructure where data is stored, and these devices natively run (AES-XTS) 256 encryption.

4-2 Anti Malware

The Cendyn corporate policy framework defines procedures and controls for handling the protection of systems from malware. Cendyn systems are protected to prevent, detect and remove malware and ensure that users are aware of the risks that might arise.

Preventive Measures

Cendyn employees are made aware of the risks that malware might cause and which preventive measures they can take via annual training and weekly security updates. Examples of potential risks include:

- Installing software on Cendyn managed software.
- Downloading files.
- Attachments to suspicious emails.
- Use of removable media.
- Reporting suspicious or possible malware infection.
- USB Drop Tests.

Detective Measures

Cendyn systems are automatically and regularly inspected for malware. At least the following elements are inspected:

- Emails and attachments transferred via Cendyn email systems before use.
- Files received by any medium, before use.
- Content published on the Intranet and Internet.
- Access to websites.
- All data, software, and other files from removable storage.

Logging and Monitoring

Cendyn uses a combination of tools to monitor our Applications, Availability, Logs and Performance. We have procedures and tools for the following activities:

- Infrastructure performance and monitoring.
- Application code and errors monitoring.
- Site monitoring and availability metrics.
- Security events correlation using a SIEM tool.