

# **Standard Student Data Privacy Agreement**

**IL-NDPA v1.0a**

School District or LEA

Warren Township High School District 121

**and**

Provider

Community Funded Enterprises, Inc

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between: 34090 Almond Rd  
[Warren Township High School District], located at [ Gurnee, IL 60031 ] (the "Local Education Agency" or "LEA") and  
[Community Funded Enterprises, Inc], located at [ Fort Collins, CO ] (the "Provider").

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
  - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**
  - If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "Services").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

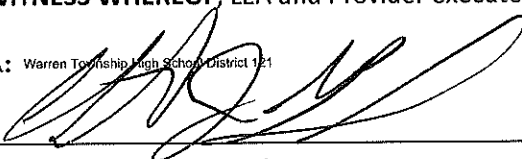
Name: Chris Geocaris Title: Assistant Superintendent  
Address: 34090 N. Almond Rd, Gurnee, IL 60031  
Phone: (847)548-7103 Email: cgeocaris@wths.net

The designated representative for the Provider for this DPA is:


Name: Carrie Spiegelhoff Title: Vice President, Fundraising Solutions  
Address: 1001-A East Harmony Rd #436, Fort Collins, CO, 80525  
Phone: 857-472-0217 Email: carrie@communityfunded.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Warren Township High School District 121

By:  Date: 3/9/2022  
Printed Name: Christopher Geocaris Title/Position: Asst. Superintendent

Provider: Community Funded Enterprises, Inc

By:  Digitally signed by Carrie Spiegelhoff  
Date: 2022.03.08 22:35:12 -06'00' Date: 03/04/2022  
Printed Name: Carrie Spiegelhoff Title/Position: VP, Fundraising Solutions

## **STANDARD CLAUSES**

Version 1.0

### **ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.



5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
  
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
  
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
  
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
  
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>

Category of Data	Elements	Check If Used by Your System
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:	<input type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input checked="" type="checkbox"/>

## EXHIBIT "C" DEFINITIONS

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Student Generated Content:** The term "Student-Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and redisclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[ ]

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[ ]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By [ ]

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date



**EXHIBIT "E"**  
**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Warren Township High School District 121 ("Originating LEA") which is dated \_\_\_\_\_, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: carrie@communityfunded.com.

**PROVIDER:** Community Funded Enterprises, Inc

BY: \_\_\_\_\_ Date: 03/04/2022

Printed Name: Carrie Spiegelhoff Title/Position: Vice President, Fundraising Solutions

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Warren Township High School District 121 and Community Funded Enterprises, Inc

**\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA:**

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

**DESIGNATED REPRESENTATIVE OF LEA:**

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_

Email: \_\_\_\_\_

**EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider .

**Cybersecurity Frameworks**

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G" - Supplemental SDPC (Student Data Privacy Consortium) State Terms for Illinois**

Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit G**, Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between Warren Township High School District 121

\_\_\_\_\_ (the "Local Education Agency" or "LEA") and \_\_\_\_\_ Community Funded Enterprises, Inc \_\_\_\_\_ (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C**, Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or

copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

**7. Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

**8. Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this Exhibit G, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

**9. Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

- a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
- b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

**10. Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

- a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
- b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

- d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

**11. Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

**12. Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this Exhibit G.

**13. Subcontractors.** By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

**14. DPA Term.**

- a. **Original DPA.** Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."
- b. **General Offer DPA.** The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: "The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."

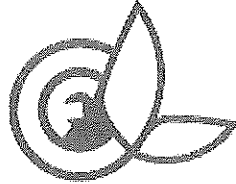
15. **Termination.** Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."
16. **Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
17. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
18. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
19. **Data Storage.** Provider shall store all Student Data shared under the DPA within the United States.
20. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

**EXHIBIT "H"**  
**Additional Terms or Modifications**  
Version \_\_\_\_\_

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

See Community Funded SOC-2 Document



CommunityFunded™

COMMUNITY FUNDED INC.  
REPORT ON SYSTEM & ORGANIZATION  
CONTROL (SOC)  
SOC 2 TYPE I REPORT RELEVANT TO SECURITY TRUST SERVICE  
CRITERIA AS ON APRIL 15, 2021

MAYANK KUSHWAHA  
COMMUNITY FUNDED  
[www.Communityfunded.com](http://www.Communityfunded.com)



Table of Contents

1.	Independent Service Auditors' Report .....	5
2.	Assertion by Management of Community Funded Inc. ....	9
3.	System Description Provided by Service Organization .....	11
3.1	Scope and Purpose of the Report.....	11
3.2	Community Funded Overview.....	11
3.3	Description of Company's Controls.....	11
3.3.1	Control Environment .....	11
(i)	Integrity and Ethical Values.....	11
(ii)	Policies and Procedures .....	12
3.3.2	Risk Assessment.....	13
3.3.2.1	Risk Mitigation.....	13
3.3.3	Information and Communication Systems .....	14
3.3.4	Description of the System .....	14
3.3.4.1	Information Security .....	14
3.3.5	Monitoring.....	16
3.4	Subservice Organization .....	16
3.5	Complementary User Entity Control (CUEC).....	17
3.6	Principal Service Commitments and System Requirements .....	17
3.7	Applicable Trust Service Criteria and Related Controls.....	19
4.	Information Provided by Service Auditor for Applicable Trust Service Criteria and Controls.....	39
4.1	Objective of Our Examination .....	39
4.2	Control Environment Elements .....	39
4.3	Reporting on Results of Testing.....	39
4.4	Results of Testing performed by Independent Service Auditor .....	40

**SECTION 1**  
**INDEPENDENT**  
**SERVICE**  
**AUDITOR'S REPORT**

## **1. Independent Service Auditors' Report**

### **Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the design of Controls relevant to Security Trust service principle.**

#### **Scope**

We have examined the description of Community Funded Inc.'s ('Community Funded', the 'Service Organization', or the 'Company') related to Community Funded crowdfunding platform relevant to the Security ('in-scope Trust Principles') as on 15 April, 2021 based on criteria for a description of a service organization's system in DC Section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Community Funded's system, particularly information about system controls that Community Funded has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("Applicable Trust Services Criteria") set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, Trust Services Criteria").

The description indicates that certain applicable trust services criteria specified in the Description can be achieved only if complementary user-entity controls contemplated in the design of the Service Organization's controls are suitably designed, along with the related controls at the service organization. We have not evaluated the suitability of the design of such complementary user-entity controls.

#### **Service Organization's Responsibilities**

In Section 2 of this report, Community Funded has provided an assertion letter about the fairness of the presentation of the description based on the description criteria and suitability of the design of the controls described therein to meet the applicable trust services criteria.

Community Funded is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; identifying the risks that would prevent the applicable trust services criteria from being met designing, implementing, and documenting controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the Description.

#### **Service Auditor's Responsibilities**

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented based on the description criteria, and the controls are suitably designed to meet the applicable trust services criteria stated in the description as on 15 April, 2021.

An examination of a Description of a service organization's system and the suitability of the design of those controls to meet the applicable trust services criteria involves:

- Performing procedures to obtain evidence about whether the description is fairly presented based on the Description criteria and controls were suitably designed to meet the applicable trust services criteria as on 15 April, 2021.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria.
- Evaluating the overall presentation of the description.

### **Limitations of Controls at a Service Organization**

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

### **Opinion**

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects:

- a) The description fairly presents the system that was designed and implemented as on 15 April, 2021.
- b) The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls implemented as on 15 April, 2021 and user entities applied the controls contemplated in the design of the Service Organization's controls as on 15 April, 2021.
- c) During the examination following controls have not sufficiently implemented to meet the applicable trust services criteria:
  - CA 7: A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.
  - CA 15: Community Funded performs an annual vendor assessment based on its Vendor Management Policy.
  - CA 23: The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.
  - CA 31: Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.
  - CA 34: Change requests are logged in Jira tool and change request tickets are approved by Product/Application Manager.

### **Description of Test of Controls**

The specific controls we tested, the nature, timing, and results of our tests are presented in the section 4 of this report.

### **Restricted Use**

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Community Funded, user entities of the system related to crowdfunding Platform Services of Community Funded provided to its customers relevant to the Security and system of Community Funded as on 15 April 2021; and those prospective user entities, independent auditors and

**Jay Maru, Certified Public Accountant**

Off: 280, Moon Clinton Rd, Moon Twp, PA 15108, USA

Tel: +412-269-0499

Email: [support@accorppartners.com](mailto:support@accorppartners.com)

[www.accorppartners.com](http://www.accorppartners.com)

---

practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations or other parties.
- Internal control and its limitations.
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.



LICENSE NO.41401  
ACTIVE 06/30/2024  
STATE OF WASHINGTON  
JAY MARU

**Jay Maru, Certified Public Accountant**

Date: 18th June 2021

**SECTION 2**  
**MANAGEMENT**  
**ASSERTION**  
**PROVIDED BY**  
**SERVICE**  
**ORGANIZATION**

## 2. Assertion by Management of Community Funded Inc.

We have prepared the accompanying Description of the system in Section 3 of Community Funded Inc. ("Service Organization" or "Community Funded") related to Community Funded crowdfunding platform relevant to the Security ('in-scope Trust Principles') as on 15 April, 2021 in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Community Funded services that may be useful when assessing the risks from interactions with the System as on 15 April, 2021, particularly information about system controls that Community Funded has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("AICPA, Trust Services Criteria).

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Community Funded's controls are suitably designed along with related controls at the Service Organization. The Description does not extend to controls of user entities.

Community Funded uses Amazon Web Services (AWS), Inc. for cloud server hosting of Community Funded platform. The Description includes only the controls of Community Funded and excludes controls of AWS. The Description also indicates that certain trust services criteria specified therein can be met only if AWS controls assumed in the design of Community Funded's controls are suitably designed along with the related controls at the Service Organization. The Description does not extend to controls of AWS.

We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the Community Funded's system that was designed as on 15 April, 2021 based in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed and implemented to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Community Funded's controls as on 15 April, 2021.

**For Community Funded Inc.**



Name: **Charlie Lambropoulos**  
Title: **CEO**  
Date: **6/18/2021**

**SECTION 3**  
**DESCRIPTION OF**  
**THE SYSTEM**



### **3. System Description Provided by Service Organization**

#### **3.1 Scope and Purpose of the Report**

This report is a description of Community Funded Inc. (hereinafter referred to as "Service Organization" or "Community Funded") related to Community Funded crowdfunding platform relevant to the Security ("in-scope Trust Principles") as on 15 April, 2021 based on criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Community Funded's system, particularly information about system controls that Community Funded has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("Applicable Trust Services Criteria") set forth in TSP Section 100A, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("AICPA, Trust Services Criteria").

#### **3.2 Community Funded Overview**

Community Funded is a crowdfunding platform based in Fort Collins, Colorado allowing project creators to create one or more fundraising projects on the site with the goal of helping people and organizations with projects find the ideas, funding, and resources they need to be successful. The company Create branded, mobile-optimized fundraising pages and easily manage initiatives like crowdfunding and giving days across multiple campuses and departments. Their platform integrates directly with the user entities brand, their website, and their existing payment processor. Tie everything together with one seamless solution.

Community Funded focuses on systemic integration of crowdfunding platforms, allowing for Universities and other organizations to integrate the Community Funded crowdfunding tools into their own website. Community Funded also offers the one-off project funding concept common to many crowdfunding sites. Projects can be submitted by any individual or organization. Community Funded requires all projects have a positive community impact regardless of if the project is a "Keep-it-All" or "All-or-Nothing" style project. Businesses can also support fundraising projects by providing in-kind donations of products or services in exchange for promotion on the project page.

#### **3.3 Description of Company's Controls**

Community Funded's internal control environment demonstrates a comprehensive, proactive attitude that is exhibited by the entire organization as it relates to technology trends that may impact the products and services offered to user entities. This includes a high regard for the value of controls and the emphasis given to these controls that are reflected in the company's policies, procedures, methods, and organizational structure.

##### **3.3.1 Control Environment**

Community Funded has established an internal control framework that reflects the overall control environment within the organization and its various processes, risk assessment procedures, control activities (that help in meeting the overall control objectives), information and communication, and monitoring components of internal control. The leadership team of Community Funded is committed to the Information Security Management System which ensures that IT policies are communicated, understood, implemented and maintained at all levels of the organization and regularly reviewed for continual suitability.

##### **(i) Integrity and Ethical Values**

Community Funded expects a high bar for the integrity and ethical values of its people. These values are interwoven into every aspect of the organization and exemplified by management at every level.

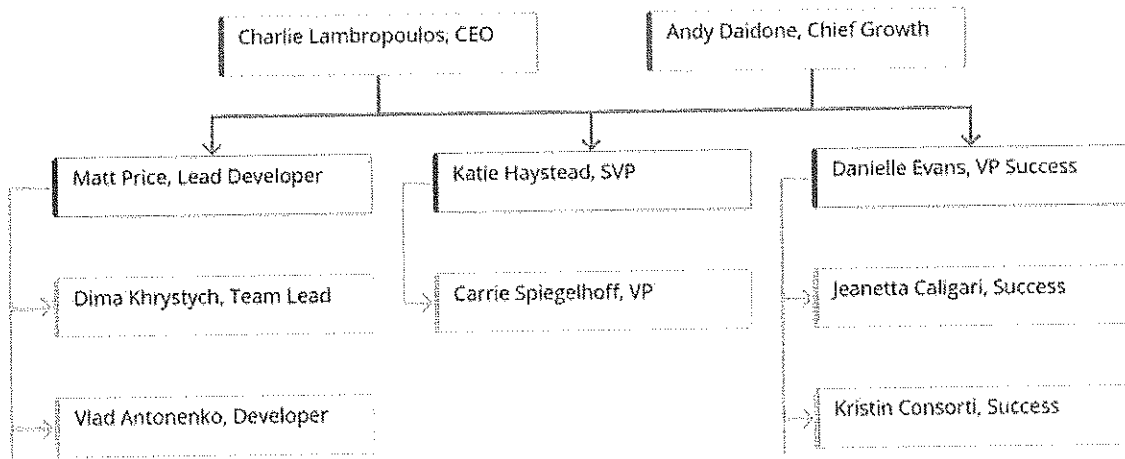
## Information provided by the Service Organization

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policy statements communicate values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee handbook and understand their responsibility for adhering to the policies and procedures contained within.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.

### (ii) Policies and Procedures

Community Funded has designed its organizational structure to provide quality service and accountability in support of Community Funded's mission. The organizational structure of Community Funded provides the overall framework for planning, directing, and controlling operations. Reporting relationships and organizational structures are reviewed periodically by Community Funded management as part of organizational planning and adjusted as needed based on company requirements. Major changes implemented in roles and responsibilities and changes in the position of key personnel are communicated to internal and external users via e-mail.



### (iii) Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, change control, and Incident management. All teams are expected to adhere to the Community Funded's policies and procedures that define how services should be delivered. These are located on the Company's shared drive and can be accessed by any Community Funded team member. Community Funded IT policies are as follows:

- Acceptable usage Policy:  
The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.
- Remote Access Policy:

## Information provided by the Service Organization

---

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with company-provided or non-company-provided equipment.

- **Incident Response Policy:**  
The scope of this policy covers all information assets owned or provided by the company, whether they reside on the corporate network or elsewhere.
- **E-mail Policy**  
The scope of this policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network.
- **Network Security Policy:**  
This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.
- **Change Management Policy:**  
Documenting changes to network devices is a best practices and can help speed resolution in the event of an incident. The company encourages documentation of changes to network devices but does not require it.
- **Risk Management Policy:**  
This policy outlines the Risk Management process for activities within Community Funded and all its operations.

### 3.3.2 Risk Assessment

Community Funded employs a risk management framework to identify and manage risks that could potentially impact the ability to deliver reliable services to customers. Community Funded identifies the underlying sources of risk, measures the impact to organization and implements appropriate measures to monitor and manage the risks.

The primary aims of the risk management framework and risk assessment process are:

- Identifying and managing risks potentially impacting Business Activities
- Determining risks and opportunities that need to be addressed to ensure:
  - Business objectives and goals may be met
  - Prevention, management, or reduction of undesirable effects
- Planning actions to address identified risks and opportunities
- Integrating and implementing actions into relevant processes
- Utilizing a risk assessment methodology suited to the identified business and information security opportunities.

#### 3.3.2.1 Risk Mitigation

The Information security related risks are identified and documented in the risk register along with the mitigation steps by respective functions and the Risk register are reviewed by management on an annual basis during the Management meeting or as and when any change. A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. The IT team performs the risk assessment and plans appropriate mitigating action plans. Risk assessment at minimum address the following:

- Unauthorized access
- Malicious or unintended use of access controls credentials

## Information provided by the Service Organization

---

- Unauthorized disclosure
- Modification or disruption of the information system.

### 3.3.3 Information and Communication Systems

Information and Communication is an integral component of Community Funded's internal control system. Electronic messaging has been incorporated in Community Funded's processes to provide timely information to employees regarding daily operating activities and to communicate management's expectations with Community Funded employees. Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization.

Community Funded employees and contractors use their own personal laptops to perform their work. Most of the employees use MacBook and some use the Windows system and work remotely. Employee ID, Community Funded e-mail box and Slack channel are provided to every employee and contractor during the joining for day-to-day communication and meetings. Important corporate events, employee news, and cultural updates are some of the messages communicated using email. Community Funded policies and procedures are accessible by all employees via shared folder. System networks and hosts are protected by AWS security policies. External points of connection to the system are protected by AWS security group rules that allow permissible connections to incoming traffic.

### 3.3.4 Description of the System

#### 3.3.4.1 Information Security

Community Funded has an Information security policy which is associated with various IT policies to ensure that employees understand their individuals' roles and responsibilities concerning to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of emails to communicate time sensitive information and processes for security purpose to notify key personnel in the event of any potential security issues or system outages.

#### Human Resources Policies and Practices

The HR policies and procedures describe Community Funded practices related to hiring, training and termination. Formal HR policies and procedures are communicated to the employees at the time of joining as part of the induction training program along with the Roles and responsibilities that are defined in employee's job descriptions. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behavior and company's Information security policy.

Specific control activities that the service organization has implemented in this area are described below:

- New employees and contractors are required to sign Mutual Non-Disclosure agreement form while joining which includes the confidentiality clause.
- All Employees are required to attend annual security training to the adherence of the IT policies.
- New employees are required to read and acknowledge the Employee Handbook stating that they have read and understand it and other applicable policies during their first day of employment.
- Employee termination procedures are in place to guide the termination process.
- The information security awareness training is provided to all employees on an annual basis by the IT team.

#### Logical Access

All identity and access management within the Community Funded production environment adheres to the following tenets:

- Access is provisioned according to access control policy

## Information provided by the Service Organization

---

- System access is reviewed annually at a minimum
- Account IDs must be unique for all users

Systems access is provisioned based on role or specific authorized need. New access is requested by HR as part of on-boarding process, or as an explicit request which requires system owner approval. Access to production infrastructure requires two forms of authentication which are Password requirements and multi factor authentication.

### Incident Management:

Community Funded maintains Incident Management policy to guide staff in reporting and responding to both potential security and information technology incidents. Any Security incidents are reported to IT team and registered on Incident Register document which is monitored to resolution as per defined security incident policy. Community Funded has defined security Incident Response plan which demonstrates the responsibilities and actions to be performed in the event of a breach of security and resolved in a timely manner. After making the appropriate corrective action, the IT team document a detailed root cause and corrective action in an Incident Reporting form.

### Change Management:

Community Funded has documented a Change management policy to guide staff in documenting and implementing software and infrastructure changes. Procedures include change declaration, required documentation, development standards, and testing and approval requirements. Community Funded's codebase is tracked in a revision control system, git, and is hosted by Github. The development, test and production environments are segregated for the in-scope application.

Before making changes to the project, the analysis of the task required for implementation is carried out. Its discussion takes place at a general meeting with all team members to find the best way to implement and eliminate possible conflicts with the existing functionality. At the meeting, the task is assigned a number, the complexity of the tasks and design stages, the approximate time for its implementation, and the most suitable team members are selected for its implementation on the project. On Jira, a ticket is created with a list of all the necessary changes, taking into account the comments drawn up on the basis of a general discussion of this problem with the team.

During the designing stage the key aspects of new Feature/ Improvement/BugFix are discussed and documented. All the necessary Requirement documents are created/updated accordingly. Tasks prioritization and Jira tickets creation (that are necessary for Dev and QA teams) are performed. Investigations and collaboration with the customers are performed if necessity arises. Basis on the requirements a developer or a group of developers creates a separate branch with a task number in its name. This branch is created from the current 'develop' branch from the repository on GitHub which contains the latest relevant changes. In the process of work, each implemented item from the task is drawn up in the form of a commit with a corresponding description and added to the current branch for this task. The code, files, and general structure are compiled in such a way as to be as readable and understandable as possible for the rest of the team.

After the developer has completed the task, he sends it to the first stage of the review. To pass the first stage, at least two other team members are required, checked the new changes for errors. If errors are found, the author is sent feedback with a list of those problems that he must fix in order to successfully pass the code review. When all bugs are fixed, the developers confirm the changes, merge the branch with the issue number into the 'develop' branch for testing, after which they are automatically deployed to the test server to start testing. After passing all stages of testing, the final version of the changes is merged into production with a corresponding note of the releases.

## Information provided by the Service Organization

### Data Backup and Restoration:

Community Funded has developed formal policies and procedures related to back up and recovery. The backup procedure defines the type of information to be backed-up, backup cycles and the methods used for performing the backup. The application production data and client data are backed-up in a server hosted at AWS. Backup are managed by IT team which keeps the backup in an encrypted S3 bucket in the US region. The backup data-restoration testing is performed on requirement basis and at least once in a year to check the usability of the stored data.

### 3.3.5 Monitoring

Community Funded leadership monitors controls to ensure they are operating in alignment with policies, standards, and operational baselines. Monitoring encompasses technical and business operations, security events and compliance changes. Community Funded management performs monitoring activities in order to access the quality of internal control and monitors activities throughout the year and take corrective actions to address deviation from company policy and procedures. The Management holds regular meetings with the respective business process and team managers to maintain oversight of team activities and client's requirements.

Third party vendor performs annually vulnerability scanning and penetration testing in order to identify potential threats to the Network Infrastructure and assesses the likelihood and severity of those threats and recommend corrective actions (as necessary). The results are reviewed by IT head and any required follow-up actions are taken from respective IT team.

### 3.4 Subservice Organization

AWS provides cloud hosting services, which includes implementing physical security controls for the housed in-scope systems. Community Funded's application is hosted and managed within Amazon's secure data centre service platform.

#### Complementary Sub-service organization controls (CSOC)

Community Funded's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Community Funded. The following subservice organization controls should be implemented by AWS provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization Controls		
Category	TSC Criteria	Control
Common Criteria/ Security	CC6.4 CC6.5 CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.

**Information provided by the Service Organization**

Subservice Organization Controls		
		Physical access points to server locations are managed by electronic access control devices.
		Data Center is protected by fire detection and suppression systems.

**3.5 Complementary User Entity Control (CUEC)**

Community Funded's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Community Funded's services to be solely achieved by Community Funded control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Community Funded.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. Some of the controls that user entities are responsible for include, but are not limited to, the following:

CUEC #	User Entity Control	Associated TSC
1	User entities are responsible for communicating relevant security issues and incidents to Community Funded via e-mail.	CC2.2 CC7.3
2	User entities are responsible for ensuring that authorized users are appointed as administrator for granting access to the Community Funded platform.	CC6.2 CC6.3
3	User entities are responsible for informing their Community Funded Account/Project Manager when user accounts that are delegated administrative access rights within the Community Funded platform are to be removed or reassigned.	CC6.2 CC6.3

**3.6 Principal Service Commitments and System Requirements**

Service commitments are mentioned and communicated as a Terms of Service which is published on Community Funded website for user entities. Community Funded makes service commitments to its user entities and has established system requirements as a part of its services.

Community Funded is responsible for its service commitments and system requirements for designing and implementing controls to provide reasonable assurance that Community Funded's service commitments and system requirements are achieved.

CUEC #	Principal Commitments and Requirements	Related Controls
1	Community Funded has made commitment to communicate the security incident or data breach in a timely manner.	Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident.

**Information provided by the Service Organization**

CUEC #	Principal Commitments and Requirements	Related Controls
		The policy is reviewed and approved on an annual basis. [CA 11]
2	Community Funded has made commitment that authorized users should be given access to the customer data.	Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities. [CA 22]
3	Community Funded has made commitment to comply with applicable Law concerning the collection, receipt, transmission, storage, disposal, use, and disclosure of Client Data.	Community Funded maintains a Data retention policy that provides guidance on retention & deletion of customer data. [CA 39]

[Space Left Blank Intentionally]



## Information provided by the Service Organization

---

### 3.7 Applicable Trust Service Criteria and Related Controls

The security trusts service category and Community Funded related controls is included in section 4 of this report, "Information Provided by the Service Auditor: Tests of Controls".

#### Control Criteria and Related Controls:

**CC 1.1: *The entity demonstrates a commitment to integrity and ethical values.***

#### Community Funded Control Activities

CA 1 All employees are required to read and accept the code of conduct (Employee Handbook) over e-mail and the statement of confidentiality & privacy at the time of joining.

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 7 A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.

CA 14 Community Funded has a documented Terms of Service and Privacy policy, which is mentioned on its website and Community Funded clients, agrees the Terms of Service before using the service.

CA 26 Community Funded has a documented Acceptable Usage Policy that is accepted by all employees and contractors. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets in order that Community Funded's commitments and objectives are met.

**CC 1.2: *The Board of Directors demonstrates independence from management and oversees the development and performance of internal controls.***

#### Community Funded Control Activities

CA 1 All employees are required to read and accept the code of conduct (Employee Handbook) over e-mail and the statement of confidentiality & privacy at the time of joining.

CA 4 A documented organization chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to Community Funded staff.

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 7 A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.

CA 8 Community Funded has documented HR Policies and procedures including recruitment, training and exit procedures. The policy is reviewed on an annual basis.

CA 14 Community Funded has a documented Terms of Service and Privacy policy, which is mentioned on its website and Community Funded clients, agrees the Terms of Service before using the service.

## Information provided by the Service Organization

---

### Community Funded Control Activities

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in the risk register is reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks.

***CC 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.***

### Community Funded Control Activities

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 4 A documented organization chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to Community Funded staff.

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 8 Community Funded has documented HR Policies and procedures including recruitment, training and exit procedures. The policy is reviewed on an annual basis.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

[Space Left Blank Intentionally]

**Information provided by the Service Organization**

---

**CC 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with the objectives.**

**Community Funded Control Activities**

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 7 A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.

CA 8 Community Funded has documented HR Policies and procedures including recruitment, training and exit procedures. The policy is reviewed on an annual basis.

CA 26 Community Funded has a documented Acceptable Usage Policy that is accepted by all employees and contractors. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets in order that Community Funded's commitments and objectives are met.

**CC 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of the entity's objectives.**

**Community Funded Control Activities**

CA 1 All employees are required to read and accept the code of conduct (Employee Handbook) over e-mail and the statement of confidentiality & privacy at the time of joining.

CA 4 A documented organization chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to Community Funded staff.

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 7 A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.

CA 11 Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident. The policy is reviewed and approved on an annual basis.

CA 12 All policies, procedure documents are available in a Google drive folder accessible to all Community Funded employees for ready access.

CA 32 AWS security rules is configured to log security events that are reviewed on a periodic basis.

CA 33 A documented policy/ process for incident management exists which covers all security incidents related to IT and is approved/reviewed by Management on an annual basis.

[Space Left Blank Intentionally]

**Information provided by the Service Organization**

---

**CC 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**

**Community Funded Control Activities**

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 8 Community Funded has documented HR Policies and procedures including recruitment, training and exit procedures. The policy is reviewed on an annual basis.

**CC 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**

**Community Funded Control Activities**

CA 1 All employees are required to read and accept the code of conduct (Employee Handbook) over e-mail and the statement of confidentiality & privacy at the time of joining.

CA 13 Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users as applicable through Google drive folder.

**CC 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.**

**Community Funded Control Activities**

CA 4 A documented organization chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to Community Funded staff.

CA 13 Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users as applicable through Google drive folder.

CA 14 Community Funded has a documented Terms of Service and Privacy policy which is mentioned on its website and Community Funded clients agrees the Terms of Service before using the service.

**CC 3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**

**Community Funded Control Activities**

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

## Information provided by the Service Organization

### Community Funded Control Activities

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks.

CA 19 Community Funded has a documented Change Management Policy that guides personnel in the handling system changes with regards to (a) software changes, and (b) Infrastructure changes. The policy is reviewed and approved during the management meeting on an annual basis.

CA 20 Community Funded uses GitHub source'-code'-repository to document and track all software changes.

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

CA 34 Change requests are logged in Jira tool and change request tickets are approved by Product/Application Manager.

CA 35 Separate environments are used for development, testing, production. Developers do not have the ability to make changes to software in testing or production environment.

***CC 3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.***

### Community Funded Control Activities

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks.

**Information provided by the Service Organization**

---

**Community Funded Control Activities**

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

CA 36 The management and IT team reviews SOC 2 reports or other such relevant information of Sub service organizations and evaluates the suitability of internal control at the sub service organization in achieving its organization objectives.

**CC 3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**

**Community Funded Control Activities**

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

**Information provided by the Service Organization**

---

**CC 3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.**

**Community Funded Control Activities**

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 13 Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users as applicable through Google drive folder.

CA 14 Community Funded has a documented Terms of Service and Privacy policy which is mentioned on its website and Community Funded clients agrees the Terms of Service before using the service.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

[Space Left Blank Intentionally]

**Information provided by the Service Organization**

---

**CC 4.1: The entity selects, develops, and performs ongoing and/ or separate evaluations to ascertain whether the components of internal control are present and functioning.**

**Community Funded Control Activities**

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 6 IT head is responsible for maintaining the Security of Community Funded systems and performs the review of all the security incidents and events on quarterly basis.

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 12 All policies, procedure documents are available in a Google drive folder accessible to all Community Funded employees for ready access.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

**CC 4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**

**Community Funded Control Activities**

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks



## Information provided by the Service Organization

---

**CC 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**

### Community Funded Control Activities

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

CA 22 Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities.

CA 35 Separate environments are used for development, testing, production. Developers do not have the ability to make changes to software in testing or production environment.

[Space Left Blank Intentionally]

**CC 5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.**

**Community Funded Control Activities**

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

CA 22 Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities.

CA 23 The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.

CA 25 The Privileged access to Community Funded's system and application is restricted to authorized employees.

CA 28 AWS user access review is performed at least on an annual basis to ensure that only personnel with appropriate and commensurate job responsibilities have necessary access.

CA 29 E-mail requests for disabling of user id of separated employee is approved by CEO/CTO and access is revoked within 24 hours or staff's last working day as a part of the off boarding process.

CA 30 Administrative access to the network and group policy is restricted to authorized individuals in line with their roles and responsibilities.

## Information provided by the Service Organization

---

**CC 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**

### Community Funded Control Activities

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 17 Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.

CA 18 Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

**CC 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**

### Community Funded Control Activities

CA 9 Processing capacity for cloud infrastructure for AWS is monitored by AWS Cloud watch on an ongoing basis. The cloud system is continuously monitored for availability, capacity, resource utilization (CPU, memory etc.).

CA 22 Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities.

CA 23 The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.

CA 24 The Community Funded has established multi factor authentication for accessing cloud system.

CA 25 The Privileged access to Community Funded's system and application is restricted to authorized employees.

CA 27 Access to the Community Funded system is secured through secure browser session using HTTPS/TLS and industry standard transmission encryption.

CA 28 AWS user access review is performed at least on an annual basis to ensure that only personnel with appropriate and commensurate job responsibilities have necessary access.

## Information provided by the Service Organization

---

CA 29 E-mail requests for disabling of user id of separated employee is approved by CEO/CTO and access is revoked within 24 hours or staff's last working day as a part of the off boarding process.

CA 30 Administrative access to the network and group policy is restricted to authorized individuals in line with their roles and responsibilities.

CA 31 Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.

**CC 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For the users whose access is administered by the entity, user system credentials are removed when the user access is no longer authorized.**

### Community Funded Control Activities

CA 22 Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities.

CA 23 The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.

CA 28 AWS user access review is performed at least on an annual basis to ensure that only personnel with appropriate and commensurate job responsibilities have necessary access.

CA 29 E-mail requests for disabling of user id of separated employee is approved by CEO/CTO and access is revoked within 24 hours or staff's last working day as a part of the off boarding process.

**CC 6.3: The entity authorizes, modifies, or removes access to data, software, functions and other protected information assets based on roles, responsibilities or system design and changes, giving consideration to the concepts of least privilege.**

### Community Funded Control Activities

CA 15 Community Funded performs an annual vendor assessment based on its Vendor Management Policy.

CA 23 The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.

CA 29 E-mail requests for disabling of user id of separated employee is approved by CEO/CTO and access is revoked within 24 hours or staff's last working day as a part of the off boarding process.

**CC 6.4: The entity restricts physical access to facilities and protected information assets (e.g. data centre facilities, back-up media storage, and other sensitive locations) to authorize personnel to meet the entity's objectives.**

Information provided by the Service Organization

---

**Community Funded Control Activities**

CA 37 Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis.

CA 38 Backup restoration testing is performed on an annual basis by the IT Team.

***CC 6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***

**Community Funded Control Activities**

CA 26 Community Funded has a documented Acceptable Usage Policy that is accepted by all employees and contractors. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets in order that Community Funded's commitments and objectives are met.

***CC 6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***

**Community Funded Control Activities**

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 9 Processing capacity for cloud infrastructure for AWS is monitored by AWS Cloud watch on an ongoing basis. The cloud system is continuously monitored for availability, capacity, resource utilization (CPU, memory etc.).

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 24 The Community Funded has established multi factor authentication for accessing cloud system.

CA 27 Access to the Community Funded system is secured through secure browser session using HTTPS/TLS and industry standard transmission encryption.

CA 31 Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.

***CC 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes and protects it during transmission, movement, or removal to meet the entity's objectives.***

**Information provided by the Service Organization**

---

**Community Funded Control Activities**

CA 9 Processing capacity for cloud infrastructure for AWS is monitored by AWS Cloud watch on an ongoing basis. The cloud system is continuously monitored for availability, capacity, resource utilization (CPU, memory etc.).

CA 24 The Community Funded has established multi factor authentication for accessing cloud system.

CA 26 Community Funded has a documented Acceptable Usage Policy that is accepted by all employees and contractors. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets in order that Community Funded's commitments and objectives are met.

CA 27 Access to the Community Funded system is secured through secure browser session using HTTPS/TLS and industry standard transmission encryption.

CA 31 Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.

CA 37 Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis.

***CC 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***

**Community Funded Control Activities**

CA 19 Community Funded has a documented Change Management Policy that guides personnel in the handling system changes with regards to (a) software changes, and (b) Infrastructure changes. The policy is reviewed and approved during the management meeting on an annual basis.

CA 20 Community Funded uses GitHub source-code-repository to document and track all software changes.

CA 34 Change requests are logged in Jira tool and change request tickets are approved by Product/Application Manager.

CA 35 Separate environments are used for development, testing, production. Developers do not have the ability to make changes to software in testing or production environment.

***CC 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.***

**Community Funded Control Activities**

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 9 Processing capacity for cloud infrastructure for AWS is monitored by AWS Cloud watch on an ongoing basis. The cloud system is continuously monitored for availability, capacity, resource utilization (CPU, memory etc.).

Information provided by the Service Organization

**Community Funded Control Activities**

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 24 The Community Funded has established multi factor authentication for accessing cloud system.

CA 27 Access to the Community Funded system is secured through secure browser session using HTTPS/TLS and industry standard transmission encryption.

CA 31 Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.

CA 37 Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis.

**CC 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters and errors affecting the entity's ability to meet its objectives. Anomalies are analysed to determine whether they represent security events.**

**Community Funded Control Activities**

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 37 Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis

CA 38 Backup restoration testing is performed on an annual basis by the IT Team.

**CC 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**

**Community Funded Control Activities**

CA 6 IT head is responsible for maintaining the Security of Community Funded systems and performs the review of all the security incidents and events on quarterly basis.

CA 11 Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident. The policy is reviewed and approved on an annual basis.

CA 32 AWS security rules is configured to log security events that are reviewed on a periodic basis.

**Information provided by the Service Organization**

---

CA 33 A documented policy/ process for incident management exists which covers all security incidents related to IT and is approved/reviewed by Management on an annual basis.

[Space Left Blank Intentionally]

**CC 7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents as appropriate.**

**Community Funded Control Activities**

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 6 IT head is responsible for maintaining the Security of Community Funded systems and performs the review of all the security incidents and events on quarterly basis.

CA 11 Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident. The policy is reviewed and approved on an annual basis.

CA 32 AWS security rules is configured to log security events that are reviewed on a periodic basis.

CA 33 A documented policy/ process for incident management exists which covers all security incidents related to IT and is approved/reviewed by Management on an annual basis.

**CC 7.5: The entity identifies, develops and implements activities to recover from identified security incidents.**

**Community Funded Control Activities**

CA 5 Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.

CA 6 IT head is responsible for maintaining the Security of Community Funded systems and performs the review of all the security incidents and events on quarterly basis.

CA 11 Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident. The policy is reviewed and approved on an annual basis.

CA 32 AWS security rules is configured to log security events that are reviewed on a periodic basis.

CA 33 A documented policy/ process for incident management exists which covers all security incidents related to IT and is approved/reviewed by Management on an annual basis.

**CC 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**



## Information provided by the Service Organization

### Community Funded Control Activities

CA 3 External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.

CA 10 Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).

CA 19 Community Funded has a documented Change Management Policy that guides personnel in the handling system changes with regards to (a) software changes, and (b) Infrastructure changes. The policy is reviewed and approved during the management meeting on an annual basis.

CA 20 Community Funded uses GitHub source'-code'-repository to document and track all software changes.

CA 34 Change requests are logged in Jira tool and change request tickets are approved by Product/Application Manager.

CA 35 Separate environments are used for development, testing, production. Developers do not have the ability to make changes to software in testing or production environment.

**CC 9.1: The entity identifies, selects, and develops risk-mitigation activities for risks arising from potential business disruptions.**

### Community Funded Control Activities

CA 2 Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.

CA 14 Community Funded has a documented Terms of Service and Privacy policy which is mentioned on its website and Community Funded clients agrees the Terms of Service before using the service.

CA 15 Community Funded performs an annual vendor assessment based on its Vendor Management Policy.

CA 16 Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.

CA 21 The Senior Management of Community Funded meets annually to review and approve the following documents:

- 1) Annual Risk Assessment and Risk Register
- 2) Org structure and reporting lines
- 3) Job descriptions of employees
- 4) Code of Conduct
- 5) Policies and Procedures
- 6) Vendor Risk assessment

CA 36 The management and IT team reviews SOC 2 reports or other such relevant information of Sub service organizations and evaluates the suitability of internal control at the sub service organization in achieving its organization objectives.

**Information provided by the Service Organization**

---

**Community Funded Control Activities**

CA 37 Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis.

CA 38 Backup restoration testing is performed on an annual basis by the IT Team.

CA 39 Community Funded maintains a Data retention policy that provides guidance on retention & deletion of customer data.

**CC 9.2: The entity assesses and manages risks associated with vendors and business partners.**

**Community Funded Control Activities**

CA 14 Community Funded has a documented Terms of Service and Privacy policy which is mentioned on its website and Community Funded clients agrees the Terms of Service before using the service.

CA 15 Community Funded performs an annual vendor assessment based on its Vendor Management Policy.

CA 36 The management and IT team reviews SOC 2 reports or other such relevant information of Sub service organizations and evaluates the suitability of internal control at the sub service organization in achieving its organization objectives.

CA 39 Community Funded maintains a Data retention policy that provides guidance on retention & deletion of customer data.

[Space Left Blank Intentionally]

**Information provided by the Service Organization**

---

---

**SECTION 4**  
**INFORMATION**  
**PROVIDED BY**  
**THE SERVICE**  
**AUDITOR: TEST**  
**OF CONTROLS**

#### **4. Information Provided by Service Auditor for Applicable Trust Service Criteria and Controls**

##### **4.1 Objective of Our Examination**

This report is intended to provide interested parties with information about the controls at Community Funded that may affect the processing of user organizations' transactions and also to provide users with information about design of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and in (2) assessing control risk for assertions in user organizations' financial statements that may be affected by controls at Community Funded.

Our testing of Community Funded's controls were restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, Community Funded's controls may not compensate for such weaknesses.

##### **4.2 Control Environment Elements**

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design and implementation of controls identified by Community Funded procedures include test of the following relevant elements of the Community Funded's control environment

1. Control Environment
2. Internal Risk Assessment
3. Information and Communication
4. Monitoring

##### **4.3 Reporting on Results of Testing**

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because auditors does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, auditor reports all deviations.

[Space Left Blank Intentionally]

**Information provided by the Service Auditor**

**4.4 Results of Testing performed by Independent Service Auditor**

Each controls listed below as specified by Community Funded, ascertained through inquiry with management and the control owner that each control activity listed below implemented as described during the Audit.

TSP Ref #	Control Activity #	Controls	Result of Tests
CC1.1 CC1.2 CC1.5 CC2.2	CA 1	All employees are required to read and accept the code of conduct (Employee Handbook) over e-mail and the statement of confidentiality & privacy at the time of joining.	No Exception Noted
CC1.1 CC1.3 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC9.1	CA 2	Community Funded has a documented Information security policy which defines the key aspects related to information security, organizational roles and responsibilities, physical & logical security and incident management and it is communicated to employees during security awareness training program and readily available on shared folder. The policy is reviewed and approved on an annual basis.	No Exception Noted
CC2.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC5.2 CC6.6 CC7.1 CC7.2 CC8.1	CA 3	External Third Party vendor performs annual Vulnerability assessment and penetration testing on the Company network. The results are reviewed by IT head and any required follow-up actions are taken from the IT team.	No Exception Noted
CC1.2 CC1.3 CC1.5 CC2.3	CA 4	A documented organization chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to Community Funded staff.	No Exception Noted
CC1.2 CC1.3 CC1.4 CC1.5 CC7.4 CC7.5	CA 5	Community Funded has job requirements documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	No Exception Noted
CC4.1 CC7.3 CC7.4 CC7.5	CA 6	IT head is responsible for maintaining the Security of Community Funded systems and performs the review of all the security incidents and events on quarterly basis.	No Exception Noted
CC1.1 CC1.4 CC1.5	CA 7	A security awareness program is conducted annually to apprise the employees about their job roles and responsibilities and Company's Information security policy.	Exception Noted. During the walkthrough, it was noted that security awareness training program was not conducted.

Information provided by the Service Auditor

TSP Ref #	Control Activity #	Controls	Result of Tests
CC1.2 CC1.3 CC1.4 CC2.1	CA 8	Community Funded has documented HR Policies and procedures including recruitment, training and exit procedures. The policy is reviewed on an annual basis.	No Exception Noted
CC6.1 CC6.6 CC6.7 CC7.1	CA 9	Processing capacity for cloud infrastructure for AWS is monitored by AWS Cloud watch on an ongoing basis. The cloud system is continuously monitored for availability, capacity, resource utilization (CPU, memory etc.).	No Exception Noted
CC3.4 CC4.1 CC5.1 CC6.6 CC7.1 CC7.2 CC8.1	CA 10	Internal Vulnerability scans are performed on an annual basis by the community funded IT team and Management takes appropriate action based on the results of scans for closure of findings (if any).	No Exception Noted
CC1.5 CC7.3 CC7.4 CC7.5	CA 11	Community Funded has a documented incident handling policy that requires the proper communication of events to the appropriate personnel responsible for resolving the incident. The policy is reviewed and approved on an annual basis.	No Exception Noted
CC1.5 CC4.1	CA 12	All policies, procedure documents are available in a Google drive folder accessible to all Community Funded employees for ready access.	No Exception Noted
CC2.2 CC2.3 CC3.4	CA 13	Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users as applicable through Google drive folder.	No Exception Noted
CC1.1 CC1.2 CC2.3 CC3.4 CC9.1 CC9.2	CA 14	Community Funded has a documented Terms of Service and Privacy policy which is mentioned on its website and Community Funded clients agrees the Terms of Service before using the service.	No Exception Noted
CC6.3 CC9.1 CC9.2	CA 15	Community Funded performs an annual vendor assessment based on its Vendor Management Policy.	Exception Noted. During the walkthrough, it was observed that Vendor assessment not performed.
CC1.3 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC5.2 CC5.3 CC9.1	CA 16	Community Funded has a documented Risk Assessment Policy that describes the processes which should be in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Community Funded's service commitments and system requirements.	No Exception Noted

Information provided by the Service Auditor

TSP Ref #	Control Activity #	Controls	Result of Tests
CC1.2 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3	CA 17	Risks are identified and documented in the risk register along with the mitigation steps by respective functions. Risk identified in in the risk register are reviewed by management on an annual basis or as and when any change.	No Exception Noted
CC1.2 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3	CA 18	Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks.	No Exception Noted
CC3.1 CC6.8 CC8.1	CA 19	Community Funded has a documented Change Management Policy that guides personnel in the handling system changes with regards to (a) software changes, and (b) Infrastructure changes. The policy is reviewed and approved during the management meeting on an annual basis.	No Exception Noted
CC3.1 CC6.8 CC8.1	CA 20	Community Funded uses GitHub source'-code'-repository to document and track all software changes.	No Exception Noted
CC1.3 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC5.2 CC5.3 CC9.1	CA 21	The Senior Management of Community Funded meets annually to review and approve the following documents: 1) Annual Risk Assessment and Risk Register 2) Org structure and reporting lines 3) Job descriptions of employees 4) Code of Conduct 5) Policies and Procedures 6) Vendor Risk assessment	No Exception Noted
CC5.1 CC5.2 CC6.1 CC6.2	CA 22	Community Funded has documented an Access Control Policy and develops controls in accordance to this policy to restrict system access rights to authorized personnel only, in a manner commensurate with their job responsibilities.	No Exception Noted
CC5.2 CC6.1 CC6.2 CC6.3	CA 23	The system access for new employees are provisioned, once e-mail requests for creation of new user id is created by the CTO.	Exception Noted. For sampled new user, ID creation approval evidence were not available.



Information provided by the Service Auditor

TSP Ref #	Control Activity #	Controls	Result of Tests
CC6.1 CC6.6 CC6.7 CC7.1	CA 24	The Community Funded has established multi factor authentication for accessing cloud system.	No Exception Noted
CC5.2 CC6.1	CA 25	The Privileged access to Community Funded's system and application is restricted to authorized employees.	No Exception Noted
CC1.1 CC1.4 CC6.5 CC6.7	CA 26	Community Funded has a documented Acceptable Usage Policy that is accepted by all employees and contractors. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets in order that Community Funded's commitments and objectives are met.	No Exception Noted
CC6.1 CC6.6 CC6.7 CC7.1	CA 27	Access to the Community Funded system is secured through secure browser session using HTTPS/TLS and industry standard transmission encryption.	No Exception Noted
CC5.2 CC6.1 CC6.2	CA 28	AWS user access review is performed at least on an annual basis to ensure that only personnel with appropriate and commensurate job responsibilities have necessary access.	No Exception Noted
CC5.2 CC6.1 CC6.2 CC6.3	CA 29	E-mail requests for disabling of user id of separated employee is approved by CEO/CTO and access is revoked within 24 hours or staff's last working day as a part of the off boarding process.	No Exception Noted
CC5.2 CC6.1	CA 30	Administrative access to the network and group policy is restricted to authorized individuals in line with their roles and responsibilities.	No Exception Noted
CC6.1 CC6.6 CC6.7 CC7.1	CA 31	Community Funded IT team can access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system and AWS is secured by restricting the access from 0.0.0.0/0 to port 22.	Exception Noted. During the walkthrough, it was noted that VPN configuration was not available.
CC1.5 CC7.3 CC7.4 CC7.5	CA 32	AWS security rules is configured to log security events that are reviewed on a periodic basis.	No Exception Noted
CC1.5 CC7.3 CC7.4 CC7.5	CA 33	A documented policy/ process for incident management exists which covers all security incidents related to IT and is approved/reviewed by Management on an annual basis.	No Exception Noted
CC3.1 CC6.8 CC8.1	CA 34	Change requests are logged in Jira tool and change request tickets are approved by Product/Application Manager.	Exception Noted. During the walkthrough, it was noted that Change approval for sampled changes were not available.

Information provided by the Service Auditor

TSP Ref #	Control Activity #	Controls	Result of Tests
CC3.1 CC5.1 CC6.8 CC8.1	CA 35	Separate environments are used for development, testing, production. Developers do not have the ability to make changes to software in testing or production environment.	No Exception Noted
CC3.2 CC9.1 CC9.2	CA 36	The management and IT team reviews SOC 2 reports or other such relevant information of Sub service organizations and evaluates the suitability of internal control at the sub service organization in achieving its organization objectives.	No Exception Noted
CC6.4 CC6.7 CC7.1 CC7.2 CC9.1	CA 37	Community Funded has a documented backup policy and procedures. The application and Database backups are taken by respective function as per backup schedule and any event of backup failure are investigated until resolution. The policy is reviewed and approved on an annual basis.	No Exception Noted
CC6.4 CC6.7 CC7.1 CC7.2 CC9.1	CA 38	Backup restoration testing is performed on an annual basis by the IT Team.	No Exception Noted
CC9.1 CC9.2	CA 39	Community Funded maintains a Data retention policy that provides guidance on retention & deletion of customer data.	No Exception Noted