Benevity Information Security Addendum

1. Information Security Program

1.1. Benevity has developed and implemented and will maintain and monitor a comprehensive, written information security program ("**Program**") that includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures to protect against known or reasonably anticipated threats or hazards to the confidentiality, integrity and/or security of Client Data and that complies with applicable data protection laws at each location from which Benevity provides the Services, covering all Benevity Systems.

1.2. Benevity employs and will continue to employ personnel to monitor ongoing compliance with the Program. Benevity will review and, as appropriate, revise the Program at least annually or whenever there is a material change in Benevity's business practices or IT environment that may reasonably affect the security or integrity of Client Data.

2. Data Protection and Personal Information

2.1. Personal Information: Benevity will act solely as a "data processor" (or equivalent term under applicable data protection laws), such that it will carry out the instructions of Client (the "data controller") with respect to its use, disclosure, and other handling of such Personal Information. Benevity will be permitted to utilize Personal Information of users as necessary to provide our Services and as may be authorized by the notification and privacy settings of such user in their respective personal profiles (if applicable). Benevity will not claim ownership of the user's Personal Information. Benevity will not use Personal Information other than to perform the services in accordance with the Agreement, and will not share, store, sell, remarket, transfer (except in a corporate merger or acquisition) or otherwise disclose Personal Information for any purpose other than in accordance with Benevity's Privacy Policy (https://benevity.com/privacy-policy).

2.2. Benevity will use such reasonable degree of care as is appropriate to avoid unauthorized use or disclosure of Personal Information, including following Benevity's own security and privacy policies and procedures, which Benevity represents as complying with applicable data protection laws and being no less rigorous than accepted practices in the industry and in accordance with the Program as detailed in this Information Security Addendum.

3. Cloud Hosting Locations

3.1. Benevity's Platform, Employee Engagement, and Community Investment solutions, are hosted with cloud service providers located in the United States. This includes infrastructure and Client Data including Personal Information

3.2. Alaya's platform, infrastructure, Client Data including Personal Information with cloud service providers located in the EU.

4. Physical Security

4.1. Benevity's office locations from which Client Data is accessed will conform to the following baseline of physical security controls:

- Swipe card access at all office entrances.
- Video monitoring with footage retained for 90 days.
- Physical intrusion alarm systems with professional monitoring.

4.2. Visitors to Benevity's offices will be required to sign in, will be issued visitor identification badges or stickers, and will be escorted by a Benevity employee at all times. Benevity does not host Client Data in corporate offices. Corporate office infrastructure and corporate network will be restricted to Benevity managed devices which are centrally configured and monitored by Benevity's IT Operations team.

4.3. As part of its subcontractor management practices, Benevity shall ensure that its hosting provider's physical security controls are appropriate for Cloud hosted infrastructure housing confidential information including access and environmental controls, security monitoring and visitor protocols.

5. Personnel Security

5.1. Benevity will ensure that subject to applicable laws, all Benevity employees undergo background screening which includes, at a minimum: a. Identity verification; b. Criminal records check. All Benevity employees and contractors shall be required to sign confidentiality agreements whose scope includes Client Data. Employees will be required to comply with Benevity's policies, including but not limited to: a. Benevity's Privacy Policy; b. Benevity's policies on conduct and business ethics. Benevity will ensure all employees undergo security awareness training upon hire and annually thereafter. Employees with access to Personal Information will receive privacy awareness training.

6. Authentication

6.1. All technology platforms providing access to Client Data must authenticate (verify) the identity of users (or remote systems) prior to initiating a session or transaction. Benevity will require at a minimum password authentication and will enforce the use of strong passwords and password management practices meeting Information Security industry best practices. All Benevity personnel will be held accountable for all activity associated with the use of their User ID and password.

7. Access Management

7.1. Benevity will maintain an access management process to ensure that employee access is controlled and monitored throughout the access management lifecycle including new user provisioning, employee role changes and deprovisioning of terminated users.

7.2. Benevity will perform periodic access reviews for all systems and applications containing Client Data to ensure access is appropriate. Any inappropriate access identified as part of the access reviews will be promptly remediated.

8. Change Management

8.1. Benevity will maintain a change management process to ensure that changes to its infrastructure, applications and Client Data undergo appropriate authorization, testing, approval for migration to a production environment and post-implementation monitoring.

9. Secure Development

9.1. Benevity will implement software security policies, standards, and procedures to ensure that stakeholders, business owners and internal governing bodies have a common understanding of business practices and risk management expectations. Benevity will follow an industry standard systems development life cycle ("SDLC") process to confirm secure coding practices are utilized during development. This includes code reviews of web-facing applications using industry standards, such as Open Web Application Security Project (OWASP).

10. Encryption

10.1. Benevity encrypts Client Data in transit across any external networks and at rest using current industry standard cryptographic algorithms.

10.2. Benevity will perform appropriate management of all cryptographic key material to ensure its confidentiality and will rotate encryption keys associated with Client Data according to best practices.

11. Data Segregation

11.1. Benevity's solutions are offered as multi-tenant Software-as-a-Service (SaaS) applications. Client Data will be logically and/or physically segregated from that of other clients at all times. Benevity will not store or use Client Data in non-production environments.

12. Network Security

12.1. Benevity will employ industry standard network security controls on its networks containing Client Data to prevent unauthorized access. These controls will include at a minimum:

- Firewalls
- Intrusion Prevention Systems
- File Integrity Monitoring
- Anti-Malware Software on production hosts and Benevity issued workstations

12.2. Where applicable, network security solutions will have their definitions/signatures updated on a frequent basis with automatic updates enabled.

13. Logging and Monitoring

13.1. Benevity will maintain electronic logs of user activity and security events at the network, operating system, database and application levels. Benevity centralizes its logs in a Security Incident and Event Management (SIEM) system to facilitate correlation and monitoring of logs. Logs and any security event alerting will be monitored by Benevity's Security Operations team.

13.2. Logs will be maintained for a minimum of one year and pertinent logging will be shared with Client in the event of a Security Incident involving Client Data. A "Security Incident" is defined as unauthorized access, use, disclosure, modification, or destruction of Client Data (including Client Personal Information) or interference with system operations in an information system maintained by Benevity that contains Client Data. The inadvertent unauthorized access of Client Data by a Benevity employee or subcontractor performing Services under the Agreement is not a security breach so long as the employee or subcontractor ends access as soon as the access is discovered, and the inadvertent access is reported to Client immediately.

14. Incident and Breach Response

14.1. Benevity will maintain a Security Incident Management Plan to be followed in the event of a Security Incident. The plan will contain procedures for incident identification, classification, investigation, resolution and reporting/notification.

14.2. In the event of a Security Incident involving Client Data, Benevity will notify Client as soon as it is discovered, and in any event, no longer than 24 hours.

14.3. Benevity shall provide such timely information and cooperation as Client may require in order for Client to fulfill its reporting obligations under (and in accordance with) the timescales required by Applicable Data Protection Law. Such information and cooperation shall include, at a minimum: (a) a description of the nature of the Security Incident (including, where possible, categories and approximate number of Data Subjects and Personal Information records concerned); (b) details of a contact point where more information can be obtained; (c) a description of the likely consequences of the Security Incident; and (d) a description of the measures taken or proposed to address the Security Incident, including measures to mitigate its possible adverse effects.

14.4. Benevity shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Client up-to-date about all developments in connection with the Security Incident.

15. Vulnerability Management

15.1. Benevity will perform network vulnerability scans of its network containing Client Data on a bi-weekly basis. Reputable subcontractor(s) will be engaged to perform network penetration testing against Benevity's network on a semi-annual basis. Benevity will complete application vulnerability scanning on a continuous basis. Any network or application vulnerabilities surfaced by Benevity's internal or third party testing will be tracked and remediated in accordance with Benevity's Vulnerability Management Policy.

15.2. Vulnerability reports from third party penetration testing and application vulnerability scanning will be made available to Client upon request along with the status of any vulnerabilities undergoing remediation.

16. Business Continuity and Disaster Recovery

16.1. Benevity will maintain a Business Continuity Plan that will also address disaster recovery capabilities. The business continuity plan will be regularly reviewed and will be updated in accordance with changes to the business. Benevity will maintain a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) as outlined in the Service Level Addendum (https://b-hive.benevity.com/hc/en-us/article_attachments/27453963318292).
The disaster recovery aspect of the Business Continuity Plan will be tested on an annual basis at minimum. Benevity will make a copy of its current Business Continuity Plan available to Client upon request.

16.2. A status page (https://status.benevity.org) is available to Client and updated in real time. Clients can subscribe to this page for email notifications of disaster declaration and ongoing communications until the Services are restored to normal operations.

17. Subcontractors

17.1. Benevity utilizes subcontractors to support the provision of our Products and Services. Benevity will ensure that any and all agreements entered into with subcontracted service providers who will transmit, process, access, or store Client Data will include appropriate confidentiality clauses and security provisions no less stringent than its own.

17.2. Prior to engaging any subcontractors, Benevity will perform due diligence to ensure the subcontractor's security posture is commensurate with their risk of access and criticality to Benevity's systems and data, including Client Data. Benevity will periodically review subcontractors based on the risk evaluation, with an annual review required for critical subcontractors.

17.3. Benevity may engage a subcontractor that will process the Personal Information of Clients ("**Subprocessor**"). Benevity maintains a list of approved Subprocessors on our website here (https://benevity.com/subprocessors). Benevity engages Subprocessors to Process the Personal Information and: (a) Benevity will provide the Client the opportunity to object

to the use of a Subprocessor by providing at least thirty (30) days' prior notice of the addition of any new Subprocessor (including details of the scope of Processing it performs or will perform and the location and identity of the Subprocessor), which may be given by emailing details of such addition to Client; (b) Benevity carries out adequate due diligence on the Subprocessor to ensure it is capable of providing the level of protection required by this ISA; (c) Benevity imposes data protection terms on any new Subprocessor that protect the Personal Information to the same standard provided for by this ISA; and (d) Benevity remains fully liable for any breach of this ISA that is caused by an act, error or omission of its Subprocessor.

17.4. If Client refuses Benevity's appointment of a Subprocessor on reasonable grounds relating to the protection of the Personal Data, then either Benevity will not appoint the Subprocessor or Client may elect to suspend or terminate the Agreement without penalty.

18. Security Package

18.1. Benevity will make available to Client: (i) Benevity's audit reports performed by an independent third-party auditor; (ii) Benevity's hosting provider's audit report; (iii) PCI DSS attestations of compliance from payment processors used; (iv) information on Benevity's information security and privacy programs; and (v) completed industry-standard information security questionnaires and frequently asked questions (together the "**Security Package**"), to assist with Client's risk assessment & compliance requirements. Benevity will assist Client with reasonable inquiries or clarifications, and items that may not be covered by the Security Package. Where Client requests the Benevity complete Client's custom security questionnaire, or where responses are duplicative of material available in the Security Package, Benevity may charge a reasonable agreed-upon fee to Client for such additional assistance.

18.2. Benevity's Security Package may also be found on B-Hive Trust & Security self-serve portal below:
https://b-hive.benevity.com/hc/en-us/categories/4411210830356-Trust-and-Security

19. Audit and Inspection

19.1. To the extent Client's audit obligations under Applicable Data Protection Law or other regulatory body are not reasonably satisfied through the Security Package, Benevity shall permit Client (or its third-party auditors) to inspect or audit for Benevity's compliance with the Agreement, with mutual agreement on scope, timing and duration, provided that Client gives at least thirty (30) days' prior notice of its intention to inspect or audit, conducts its inspection or audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Benevity's operations. Client shall ensure that its personnel (or its third-party auditors) adhere to Benevity's reasonable internal security measures and are bound to confidentiality obligations no less stringent than those in the applicable Agreement.

19.2. Client will not exercise its audit and inspection rights more than once in any twelve (12) calendar month period, except: (i) if and when required by instruction of a competent regulatory body or Applicable Data Protection Law; or (ii) Client is seeking information at the request of a competent data protection authority which cannot otherwise be reasonably obtained from Benevity or through the use of the Essentials Security Package; or (iii) Client reasonably believes a further audit is necessary due to a Security Incident suffered by Benevity. Except for an audit or inspection as a result of (i), (ii) or (iii) above, Benevity will charge a reasonable agreed-upon fee to Client for such additional assistance.

20. PCI Compliance

20.1. Benevity has fully outsourced all cardholder data functions to third party payment processors. There is no electronic storage, processing, or transmission of any cardholder data on Benevity's systems. Benevity shall utilize third party payment processors that maintain compliance with requirements defined by the Payment Card Industry Data Security Standard, "PCI-DSS"), including the completion Report on Compliance ("RoC"), reviewed by a Qualified Security Assessor ("QSA"). Benevity shall comply with requirements of PCI-DSS for merchants who do not process cardholder data, specifically the requirements of the Self Assessment Questionnaire (SAQ-A) Report.

21. Data Retention, Return, and Deletion

21.1. Upon termination or expiry of the Agreement, the Benevity shall (at the Client's election) destroy or return all Client Data in its possession or control (including any Personal Information subcontracted to a third party for Processing). Notwithstanding the foregoing, and only to the extent necessary for the prevention of fraud and to adhere to taxation record retention requirements, the Benevity retains Client Data pertaining to donation transactions in accordance with requirements under applicable laws, but in general for seven (7) years from the date of termination of the Agreement. The requirement to destroy or return herein shall also not apply to the extent that the Benevity is required by any other applicable law to retain some or all of the Client Data. In the event of any of the foregoing exceptions, the Benevity shall isolate and protect the Client Data from any further Processing except to the extent required for fraud prevention or by such law.

Last Updated: October 2024

Technical and Organizational Measures for the Protection of Client Data and Personal Information

The table below outlines the specific measures in place for the protection of Personal Information, as required by Applicable Data Protection Laws.

Measures	***Description***
Measures of pseudonymisation and encryption of personal data	Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to Benevity is encrypted with 256-bit encryption and supports TLS 1.2 and above.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Benevity maintains an information security program, which includes: (a) having a formal risk management program; (b) conducting periodic risk assessments of all systems and networks that process data on at least an annual basis; (c) monitoring for security incidents and maintaining a tiered remediation plan to ensure timely fixes to any discovered vulnerabilities; (d) a written information security policy and incident response plan that explicitly addresses and provides guidance to its personnel in furtherance of the security, confidentiality, integrity, and availability of data; (e) penetration testing performed by a qualified third party on an annual basis; and (f) having resources responsible for information security efforts.
Measures for ensuring the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident	Benevity takes daily snapshots of its databases and securely copies them to a separate data center for recovery purposes in the event of a regional failure. Backups are encrypted and have the same protection in place as production. Additionally, data is stored cross-regionally with the cloud hosting provider.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	On an annual basis, Benevity performs on its own and engages third parties to perform a variety of testing to protect against unauthorized access to data and to assess the security, reliability, and integrity of the Services. To the extent Benevity determines, in its sole discretion, that any remediation is required based on the results of such testing, it will perform such remediation within a reasonable period of time taking into account the nature and severity of the identified issue.

Measures	Description
Measures for user identification and authorisation	Access to manage Benevity's cloud infrastructure environment requires multi-factor authentication, access to the Services is logged, and access to data is restricted to a limited set of approved Benevity employees. Cloud infrastructure networking features such as security groups are leveraged to restrict access to cloud instances and resources and are configured to restrict access using the principle of least privilege. Employees are trained on documented information security and privacy procedures. Every Benevity employee signs a confidentiality agreement that binds them to the terms of Benevity's data confidentiality policies and access to Benevity systems is promptly revoked upon termination of employment.
Measures for the protection of data during transmission	Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to Benevity is encrypted with 256-bit encryption and supports TLS 1.2 and above.
Measures for the protection of data during storage	Data is stored cross-regionally with cloud hosting providers. Data backups are encrypted. Data is encrypted at rest with AES 256-bit secret keys.
Measures for ensuring physical security of locations at which Personal Information are processed	Benevity uses Amazon Web Services (AWS) and Google Cloud Platform (GCP) (and such cloud hosting providers as may be appropriate to employ from time to time) to provide management and hosting of production servers and databases. Cloud hosting providers employ robust physical security programs with multiple certifications, including SOC 2 and ISO 27001.
Measures for ensuring events logging	All access to information security management systems at Benevity are restricted, monitored, and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. The level of additional detail to be recorded by each audit log will be proportional to the amount and sensitivity of the information stored and/or processed on that system. Read-only copies of all system logs are streamed in real-time to Benevity's read-only log server to prevent tampering.
Measures for ensuring system configuration, including default configuration	Benevity leverages centrally managed images to generate virtual systems in Benevity's AWS environment. We leverage "Infrastructure as Code" scripts to automate numerous security configurations that align to industry best practices, where each configuration undergoes integrity monitoring to detect and alert for any deviations to industry standards.

Measures	Description
Measures for internal IT and IT security governance and management	Benevity maintains a formal information security program with dedicated security personnel reporting to Benevity's Security Operations Manager. Benevity's Security Operations Team is responsible for implementing security controls and monitoring Benevity for suspicious activity. Policies and procedures, including the Benevity IT Security Policy, are updated on an annual basis and reviewed and approved by Management. Benevity's Risk & Compliance team has developed a formal risk management approach to be used for all risk assessments and evaluations. The approach is based on the ISO 31000 framework and defines the process for risk identification, analysis, ownership, evaluation and treatment.
Measures for certification/assurance of processes and products	As of the Effective Date, Benevity undergoes annual independent external audits with respect to controls relevant to processing of its information security programme and systems. As of the Effective Date, the following modules are in scope for external audits: • Employee Engagement Module (formerly Spark) - SOC 2 Type II • Community Investment Essentials (formerly Grants) - SOC 2 Type II • Community Investment Enterprise (formerly Versaic) - SOC 2 Type I
Measures for ensuring data minimisation	Benevity only collects information that is necessary in order to provide the Services outlined in the Agreement. Benevity's employees are directed to access only the minimum amount of information necessary to perform the task at hand.
Measures for ensuring data quality	Benevity maintains logs for user activity and security events at the network, operating system, database, and application levels. Read-only copies of all system logs are streamed in real-time to Benevity's read-only log server to prevent tampering. At minimum, log entries include date, timestamp, action performed, and the user ID or the device ID of the action performed. Users who would like to exercise their rights under Applicable Data Protection Law to update information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy.
Measures for ensuring limited data retention	Benevity will retain information for the period necessary to fulfill the purposes outlined in Benevity's Privacy Policy at https://www.benevity.com/privacy-policy, or where the Agreement requires or permits specific retention or deletion periods. Users who would like to exercise their rights under Applicable Data Protection Law to update

Measures	Description
	information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy.
Measures for ensuring accountability	Benevity has established a comprehensive GDPR privacy compliance program and is committed to partnering with its clients and vendors on GDPR compliance efforts. Some significant steps Benevity has taken to align its practices with the GDPR include: • Enhancements to Benevity's security practices and procedures • Closely reviewing and mapping the data Benevity collects, uses, and shares • Creating more robust internal privacy and security documentation • Training employees on GDPR and Privacy requirements and privacy and security best practices generally • Appointed a Data Protection Officer ("DPO"), who can be reached at privacy@benevity.com. Users who would like to exercise their rights under Applicable Data Protection Law to update information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy
Measures for allowing data portability and ensuring erasure	Benevity provides a mechanism for individuals to exercise their privacy rights in accordance with Applicable Data Protection Law. Individuals may exercise their rights by contacting Benevity at privacy@benevity.com.
For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter	Benevity has measures in place to provide assistance to controllers as needed. Such measures include, but are not limited to, the ability to delete all data associated with the Services, subject to Applicable Data Protection Law. With regard to Data Subject Requests, in the event the controller is unable to address a Data Subject Request in its use of the Service, Benevity will, upon request, provide commercially reasonable efforts to assist the controller in responding to such Data Subject Request, to the extent Benevity is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Law. Data Subjects may also exercise their rights by contacting Benevity at privacy@benevity.com.