SECURITY ADDENDUM

Description of the Data Processor's technical and organisational security measures.

Data Information Security Overview

For purposes of this Security Addendum, the terms "Data Controller" means "Customer" and "Data Processor" means "Zuora". "Data Controller Personal Data" or "Personal Data" for purposes of this Security Addendum means the Personal Data transferred to the Data Processor.

This information security overview applies to the Data Processor's corporate controls for safeguarding personal data, which is processed for, and transferred from, the Data Controller. This data information security overview enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the statement of work as agreed with each customer. Without limiting the generality of the forgoing, Data Processor's security program shall contain the following principles.

Technical and Organizational Measures

1. **Physical entry controls**. Measures to prevent unauthorized persons from gaining entry to data processing systems with which personal data are processed or used:
    a. Data Processor will maintain or require co-location facilities and service partners to maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Data Processor facilities used to host the Services (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.
    b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. Data Processor will revoke access to controlled data center areas upon a) separation of an authorized employee or b) the authorized employee no longer has a valid business need for access. Data Processor will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.
    c. Any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.
    d. Data Processor will take precautions to protect the Services' physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

2. **Logical entry controls**. Measures to prevent processing systems from being used without authorization:

a. Data Processor will maintain documented security architecture of networks managed by Data Processor in its operation of the Services. Data Processor will separately review such security architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense in depth standards prior to implementation.

b. Data Processor will maintain measures for the Services that are designed to logically separate and prevent Data Controller Personal Data from being exposed to or accessed by unauthorized persons.

c. If Data Processor requires access to Data Controller Personal Data, Data Processor will restrict and limit such access to least level required to provide and support the Services. Such access, including administrative access to any underlying components (privileged access), will be individual, role based, and subject to approval and regular validation by authorized Data Processor personnel following the principles of segregation of duties. Data Processor will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or request of authorized Data Processor personnel, such as the account owner's manager.

d. Consistent with industry standard practices, and to the extent natively supported by each component managed by Data Processor within the Services, Data Processor will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

3. **Access controls**. Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have access rights to and that personal data cannot be read, copied, modified or removed without authorization during processing or use and after storage:

a. To the extent described in the relevant Agreement and this DPA, Data Processor will encrypt Data Controller Personal Data not intended for public or unauthenticated viewing when transferring Data Controller Personal Data over public networks and enable use of a cryptographic protocol, such as TLS or SSH, for secure transfer of Data Controller Personal Data to and from the Services over public networks.

b. Data Processor will encrypt Data Controller Personal Data at rest when specified in Agreement and this DPA. If the Services includes management of cryptographic keys, Data Processor will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

c. To the extent supported by native device or operating system functionality, Data Processor will maintain computing protections for systems containing Data Controller Personal Data and all end-user systems that include, but may not be

limited to, endpoint firewalls, full disk encryption, signature-based antivirus and malware detection and removal that shall i) be regularly updated by central infrastructure and ii) logged to a central location, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

d. Where required or determined necessary from an adequate security assessment, Data Processor processes Data Controller Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information using appropriate pseudonymization or anonymization techniques. These techniques are implemented in such a way that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

4. **Transmission controls**. Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged:
   - **a.** Data Processor has put in place a solution to restrict, control, or monitor access to the Services to authorized network addresses as applicable. Data Controller can control access to the Services associated with Data Controller tenant.
   - **b.** Data Controller can control storage of personal data to the Services by limiting the data that it sends to Data Processor.

5. **Input controls**. Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed:
   - **a.** Data Processor will monitor use of privileged access and maintain security information and event management measures designed to i) identify unauthorized access and activity, ii) facilitate a timely and appropriate response, and iii) to enable internal and independent third-party audits of compliance with documented Data Processor policy.
   - **b.** Logs, in which privileged access and activity are recorded, will be retained in compliance with Data Processor's records retention policy. Data Processor will maintain measures designed to protect against unauthorized access, modification and accidental or deliberate destruction of such logs.

6. **Instruction compliance controls**. Measures to ensure that during processing the personal data, is processed strictly in accordance with the instructions of the Data Controller:
   - **a.** Data Processor implements regular access review to assess compliance with instructions with Data Controller as documented in contracts and with applicable laws and regulations.

b. Data Processor will maintain and follow documented incident response policies consistent with acceptable industry standards for security incident handling and will comply with data breach notification terms of the Agreement and this DPA.

c. Data Processor will investigate unauthorized access and unauthorized use of Data Controller Personal Data of which Data Processor becomes aware (security incident), and, within the Services scope, Data Processor will define and execute an appropriate response plan. Data Controller may notify Data Processor of a suspected vulnerability or incident by submitting a technical support case for Data Processor evaluation.

7. **Availability and resilience controls**. Measures to ensure that personal data are protected from accidental destruction or loss:

a. Data Processor will maintain policies and procedures designed to manage risks associated with the application of changes to its Services. Prior to implementation, changes to a Services, including its systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Services and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

b. Data Processor will maintain an inventory of all information technology assets used in its operation of the Services. Data Processor will continuously monitor the health and availability of the Services and underlying components.

documented, maintained and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the Services, if provided, will be established with consideration given to the Services' architecture and intended use, and will be described in the relevant Agreement and this DPA.

d. Data Processor will i) backup systems containing Data Controller Personal Data daily, ii) ensure at least one backup destination is at a remote location, separate from production systems, iii) encrypt backup data stored on portable backup media and iv) validate backup process integrity by regularly performing data restoration testing.

e. Data Processor will maintain measures designed to assess, test, and apply security advisory patches to the Services and its associated systems, networks, applications, and underlying components within the Services scope. Upon determining that a security advisory patch is applicable and appropriate, Data Processor will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to Data Processor change management policy.

f. Supplier will maintain policies and procedures designed to manage risks associated with the application of changes to its Services. Prior to implementation, changes to a Services, including its systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule,

a risk statement addressing impact to the Services and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

8. **Separation controls**. Measures to ensure that data collected for different purposes are processed separately:
    a. Data Processor separates the environment for development from the environment for testing and the environment for production operations. Critical production operations for the Services are further isolated from corporate operations.
    b. Separate access credentials and authentication are used to access production and corporation operations. The separation is supervised by granular logging of access to the production and corporate operations servers. Change control policies and procedures are adhered to when making changes to ensure effectiveness of adequate segregation between environments.

9. **Effectiveness controls**. Measures to regularly test, assess and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing:
    a. Data Processor i) performs penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter, ii) enlists a qualified independent third-party to perform penetration testing at least annually, iii) performs automated management and routine verification of underlying components' compliance with security configuration requirements, and iv) remediates identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Data Processor will take reasonable steps to avoid Services disruption when performing its tests, assessments, scans, and execution of remediation activities
    b. Data Processor conducts internal audits on a regular basis to test operating effectiveness of technical and organizational measures for ensuring the security of the data processing. Reports derived from the internal audits shall be retained and reviewed by management on a periodic basis. Management leverages information from internal audit reports to consider changes necessary to improve the effectiveness of technical and organizational measures.
    c. As applicable, Data Processor maintains controls, policies, procedures, and processes that meet the standard of the following compliance certifications: i) PCI, ii) SOC 1, iii) SOC 2,iv) SOC 3, v) ISO 27001, vi) ISO 27018, vii) HIPAA, viii) EU-US Privacy Shield, ix) Swiss-US Privacy Shield. Where required by relevant Agreement and this DPA, Data Processor shall provide documented evidence of compliance reports completed and signed by authorized third-party auditors of the respective compliance certification.