An executable version of this document can be found here.

Paylocity Corporation Supplier Data Protection Addendum

This Paylocity Corporation Supplier Data Protection Addendum ("DPA") supplements and forms part of the agreement entered into by Paylocity Corporation or any of its Affiliates (each, "Paylocity"), on behalf of itself and/or, where applicable, the Affiliate executing the agreement and Supplier, each a "Party" and collectively the "Parties", that govern Supplier's provision of certain services ("Services") to Paylocity (the "Agreement").

WHEREAS

Paylocity acts as a Controller or Processor and wishes to subcontract certain Services, which imply the Processing of Personal Information, to Supplier that acts as a Processor or Sub-processor, as appropriate.

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. This DPA is effective on the Effective Date of the Agreement, unless this DPA is separately executed in which case it is effective on the date of the last signature.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as a DPA to the Agreement.

1. Definitions

In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, whereas "control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2 "**Applicable Data Protection Laws**" means any applicable law, rule, regulation, decree, order, or regulatory guidance relating to the Processing of Personal Information under the Agreement, including for data security, data protection and/or privacy, in any jurisdiction.

1.3 "**Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household that Paylocity provides or discloses to Supplier or that Supplier otherwise collects, stores, or otherwise Processes on behalf of Paylocity in connection with the Agreement.

1.4 "**Controller**" means the entity which determines the purpose and means of the Processing of Personal Information.

1.5 "**Data Subject**" means an identified or identifiable person to whom Personal Information relates.

1.6 "**Data Subject Request**" means a request from a Data Subject seeking to exercise rights under Applicable Data Protection Laws.

1.7 **"EEA"** means the European Economic Area.

1.8 **"GDPR"** means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9 **"Permitted Affiliate"** means any Paylocity Affiliates that (i) are permitted to use the Services pursuant to the Agreement, but have not signed their own separate agreement with Supplier, (ii) qualify as a Controller of Personal Information Processed by Supplier, and (iii) is subject to Applicable Data Protection Laws.

1.10 "**Personal Data Breach**" means any confirmed accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or acquisition of, or access to, Personal Information under Supplier's control.

1.11 **"Process"** or **"Processing"** means any operation performed on Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12 "**Processor**" means an entity which Processes Personal Information on Paylocity's behalf.

1.13 **"Restricted Transfer"** means a transfer (directly or via onward transfer) of Personal Information that is subject to an Applicable Data Protection Law to a country outside of such applicable country that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable).

1.14 **"Services**" means the services and other activities to be supplied or carried out by or on behalf of Supplier for Paylocity pursuant to the Agreement.

1.15 "**Standard Contractual Clauses**" or "**SCCs**" means the annex to the standard contractual clauses, also known as "SCCs," or "EU SCCs" attached to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council found at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

1.16 "**Sub-processor**" means any Processor (excluding an employee of Supplier or any of its subcontractors) engaged by and/or appointed by or on behalf of Supplier to assist in fulfilling its obligations to Process Personal Information on behalf of Supplier in connection with the Agreement.

1.17 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, found at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

2. Processing of Personal Information

2.1 Each Party shall comply with all Applicable Data Protection Laws in the Processing of Personal Information.

2.2 The Parties agree that, with respect to all Personal Information and purposes of Processing described in Annex 1, Paylocity is the Controller (or Processor, to the extent it is Processing Personal Information on behalf of its business clients, as applicable) and controls the purposes and means of Processing Personal Information, and Supplier is the Processor (or Sub-processor, as applicable) and Processes all such Personal Information on behalf of Client. Supplier further agrees that it shall:

2.2.1 only Process Personal Information pursuant to Paylocity's instructions and as described in Annex 1 hereto;

2.2.2 not sell or share any Personal Information;

2.2.3 not retain, use, or disclose Personal Information outside of the direct business relationship between the Parties or for any purpose other than the purpose of performing the Services specified in the Agreement, which shall include (i) providing the Services under the Agreement; (ii) verifying or maintaining the quality or safety of the Services, and to improve, upgrade or enhance the Services for Paylocity; and (iii) complying with Supplier's legal obligations, but shall not include Supplier's commercial purposes;

2.2.4 not combine Personal Information with other information that Supplier receives outside the business relationship with Paylocity except as required for the fulfillment of the Services; and

2.2.5 not, and shall not permit any third party, to use, access, store, copy, display, or transmit Personal Information for the purpose of improving and enhancing, training, or developing any artificial intelligence ("AI") or machine learning ("ML") models, algorithms, or systems. Supplier further agrees not to input, upload, or otherwise make available any Personal Information to any generative AI, large language model, or similar AI/ML system, whether hosted internally or by a third party, except as expressly authorized, in writing by Paylocity.

2.3 Supplier shall promptly notify Paylocity in writing at privacy@paylocity.com, unless otherwise prohibited under Applicable Data Protection Laws, if Supplier:

2.3.1 reasonably determines that any Processing instructions from Paylocity conflict with, infringe, or violate Applicable Data Protection Laws;

2.3.2 reasonably determines that it can no longer meet its obligations under Applicable Data Protection Laws; or

2.3.3 receives any complaint, notice, or communication that directly or indirectly relates to either Party's compliance with Applicable Data Protection Laws in connection with Processing associated with the Services.

3. Supplier Personnel

Supplier shall take reasonable steps to ensure that any of Supplier's personnel or any Sub-processors who may have access to Paylocity's Personal Information have a need to know the relevant Personal Information and are under an appropriate obligation of confidentiality.

4. Security

Supplier shall, in relation to Personal Information, implement appropriate technical and organizational measures (and document the same in Annex 2) to attain a level of appropriate

security to protect Personal Information that the Supplier may transmit, store, or otherwise Process in its provision of Services to Paylocity. Supplier shall, at a minimum, comply with the technical and organizational security measures specified in Annex 2 and shall comply with the information security controls described in the Paylocity Information Security Controls Overview, available at https://trust.paylocity.com/.

5. Sub-processing

5.1 Paylocity authorizes Supplier to engage the Sub-processors to Process Personal Information as required to provide the Services under the Agreement.

5.2 Information regarding Supplier's current Sub-processors, including their location and services provided, shall be provided by Supplier to Paylocity ("Sub-processor List") at privacy@paylocity.com within thirty (30) days of executing this DPA. Upon reasonable request, Supplier shall provide to Paylocity additional information related to its Sub-processors.

5.3 Supplier shall notify Paylocity at privacy@paylocity.com in advance and in writing of any Sub-processor that Supplier proposes to engage. Supplier shall notify Paylocity at least 30 days prior to the engagement of a new Sub-processor, and respond in good faith to any reasonable objections by Paylocity.

5.3.1 Paylocity may, in good faith, object to Supplier's use of a new Sub-processor by notifying Supplier (email notifications shall be acceptable) within thirty (30) days of Supplier's notice to Paylocity.

5.3.2 If Paylocity objects to a new Sub-processor, Supplier will use commercially reasonable efforts to make available to Paylocity a change in the Services or recommend a commercially reasonable change to Paylocity's configuration or use of the Services to avoid Processing of Personal Information by the objected-to new Sub-processor.

5.3.3 If the Parties are unable to resolve such objection or Supplier is unable to resolve or make available such change within a reasonable period of time, Paylocity may terminate the Agreement with respect to those Services which cannot be provided by Supplier without the use of the objected-to new Sub-processor by providing written notice to Supplier. If it is not possible to partially terminate the Agreement, Paylocity may terminate the Agreement in whole, subject to the terms of the Agreement.

5.4 Supplier shall carry out adequate due diligence to ensure that its Sub-processors are capable of providing the level of protection for Personal Information required by the Agreement.

5.5 Supplier shall remain liable for the actions and omissions of its Sub-processors.

5.6 Supplier shall enter into a written contract with each Sub-processor that complies with Applicable Data Protection Laws and includes terms which offer at least the same level of protection for Personal Information as those set out in this DPA.

6. Data Subject Request

6.1 Supplier shall notify Paylocity at privacy@paylocity.com without undue delay of any Data Subject Requests. Supplier shall not respond to Data Subject Requests itself, and Paylocity shall be solely responsible for handling such Data Subject Requests.

6.2 Supplier shall assist Paylocity in fulfilling its obligations to respond to Data Subject Requests under Applicable Data Protection Laws. Supplier shall promptly comply with any instruction from Paylocity requiring Supplier to provide, amend, transfer, or delete Personal Information, unless any such instruction violates or would cause Supplier to violate Applicable Data Protection Laws, in which case Supplier shall promptly inform Paylocity in writing at privacy@paylocity.com.

7. Personal Data Breach

7.1 Supplier shall notify Paylocity in writing at privacy@paylocity.com without undue delay, but no later than 72 hours, upon Supplier becoming aware of a Personal Data Breach, and shall provide Paylocity with sufficient information to allow Paylocity to evaluate its obligations under Applicable Data Protection Laws to notify Data Subjects, regulatory authorities or other parties of the Personal Data Breach or to notify its clients pursuant to contracts. Supplier shall reasonably cooperate with Paylocity and take commercially reasonable steps to investigate, mitigate, and remediate such Personal Data Breach.

7.2 Supplier shall not make any notification to regulatory authorities or Paylocity's Data Subjects or clients unless Paylocity has given Supplier prior express written permission or such notification is required by Applicable Data Protection Laws.

7.3 Except where otherwise required under Applicable Data Protection Laws, Paylocity shall be solely responsible for determining whether Paylocity will (a) provide notice of the Personal Data Breach affecting Personal Information to any Data Subjects, regulators, law enforcement agencies, clients or others, and the contents and delivery method of the notice; and (b) whether Paylocity shall offer any type of remedy to affected Data Subjects or clients, including the nature and extent of such remedy.

8. Data Protection Impact Assessment and Prior Consultation

Supplier shall, in a commercially reasonable manner, assist Paylocity in meeting its obligations in relation to data protection impact assessments, and prior consultations with regulatory bodies by cooperating with reasonable requests from Paylocity for information about its Processing activities and data protection practices, taking into account the nature of Processing and the information available.

9. Deletion or Return of Personal Information

9.1 Supplier shall be responsible for establishing the document retention periods for Personal Information. Supplier shall delete Personal Information in the ordinary course of business when no longer necessary to perform services under the Agreement. Upon and after termination of the Agreement, Paylocity shall have the ability to obtain or retrieve a copy of Personal Information, subject to the terms and conditions set out in the Agreement.

9.2 Supplier shall delete existing copies of Personal Information after Paylocity has obtained a copy thereof unless retention is required by Applicable Data Protection Laws (or other laws governing the processing of such data) and only to the extent and for such period as required by applicable laws. Supplier shall notify Paylocity at privacy@paylocity.com of any legal requirements preventing or deferring the deletion of Personal Information, and shall remit a certificate of destruction to privacy@paylocity.com when deletion is completed.

9.3 Supplier shall keep such Personal Information confidential and shall Process such Personal Information only as necessary for the purpose(s) specified in the Agreement and in accordance with Applicable Data Protection Laws requiring its storage and for no other purpose.

10. Audit Rights

Supplier shall reasonably cooperate with Paylocity's efforts to verify Supplier's compliance with this DPA, which efforts may include periodic audits (not to exceed one (1) audit in any twelve (12) month period), conducted at Paylocity's expense by Paylocity (or a qualified, independent third party auditor on Paylocity's behalf) as described in this Section 10. Paylocity and Supplier shall mutually agree to the dates, times, and scope of any audit of Supplier, provided that this requirement shall not oblige Supplier to provide access to information concerning: (i) information relating to Supplier's other clients; (ii) Supplier's non-public external reports; or (iii) Supplier's proprietary information. Paylocity or Paylocity's auditor shall not damage Supplier's equipment, injure Supplier's personnel, or disrupt Supplier's business in the course of such an audit. Notwithstanding the foregoing, Paylocity shall be entitled to conduct more than one audit in any twelve (12) month period in the event of a Personal Data Breach or a request from a regulatory body.

11. Controller-to-Controller Scenarios

Certain services may offer integrated processing, export, and import, of Personal Information for each Party's own purposes. In such cases, for the purposes of GDPR, each Party to this DPA: (a) is an independent Controller of the Personal Information that it collects or Processes pursuant to the Agreement; (b) shall individually determine the purposes and means of its Processing of Personal Information; and (c) shall comply with the obligations applicable to it under Applicable Data Protection Laws with respect to the Processing of Personal Information. The Parties agree that they are acting independently as a Controller and not joint controllers as defined under the GDPR. Nothing in this Section 11 shall modify any restrictions applicable to either Party's rights to use or otherwise Process Personal Information under the Agreement, and Supplier will Process Personal Information solely and exclusively for the purposes specified in the Agreement.

12. International Data Transfers

12.1 General Obligations. Supplier shall only transfer Personal Information across international borders and between jurisdictions to the extent permitted by this Section 12 and in accordance with Applicable Data Protection Laws.

12.2 Data transfers from the EU/EEA, UK, and Switzerland to the United States. To the extent Supplier participates in and certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (together, the "Data Privacy Framework"), as required by the Data Privacy Framework, Supplier will (i) provide at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) notify Paylocity if Supplier makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, take reasonable and appropriate steps to remediate unauthorized Processing.

12.3 Data Transfers from the EU/EEA, UK, and Switzerland to a country other than the United States. The Parties agree that when the transfer of Personal Information from Paylocity (as "Data Exporter") to Supplier (as "Data Importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the Restricted Transfer will be made in accordance with Applicable Data Protection Laws, and, if applicable, subject to the SCCs, which are deemed incorporated into and form a part of this DPA, as follows:

(a) EU/EEA Personal Information.

12.3.1 Transfers of Personal Information of EU Data Subjects from Paylocity (Data Exporter) in the EU/EEA to Supplier (Data Importer) outside the EU/EEA shall be conducted in accordance with this DPA and the provisions contained in (as applicable) module 1 (controller to controller), module 2 (controller-to-processor) or module 3 (processor-to-processor) of the SCCs.

12.3.2 Where the transfer of Personal Information is subject to the GDPR and the transfer relies on the SCCs, then the following amendments shall apply to the SCCs: (i) for the purposes of Section I, Clause 7, the optional docking clause applies; (ii) in Clause 9, Option 2 applies and changes to Sub-processors will be notified in accordance with the 'Sub-processing' section of this DPA; (iii) in Clause 11, Data Subjects shall also be able to lodge a complaint with an independent dispute resolution body; (iv) in Clause 17, option 1 shall apply and Parties agree that the clauses shall be governed by the law of the Czech Republic; (v) In Clause 18(b) the Parties choose the courts of the Czech Republic as their choice of forum and jurisdiction; (vi) Annexes of the SCCs will be deemed completed with the information set forth in Annexes to this DPA; (vii) the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR; and (viii) if and to the extent the SCCs conflict with any provision of this DPA, the SCCs will prevail to the extent of such conflict.

12.3.3 Where transfers of Personal Information of EU/EEA Data Subjects are conducted by Paylocity (Data Importer) on behalf of their client (Controller), module 3 (processor-to-processor) of the SCCs is applicable to such transfers, and the following terms shall apply in addition to those in section 12.3.2:

12.3.3.1 For the purposes of Clause 8.1(a), (b) and (c), Paylocity hereby informs Supplier that it acts as Processor under the instructions of the relevant Controller with respect to Personal Information. Paylocity warrants that its Processing instructions as set out in the Agreement, including this DPA and its authorizations to Supplier for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Paylocity is solely responsible for conveying any Sub-processor notifications to the relevant Controller where appropriate.

12.3.3.2 For the purposes of Clause 8.6(c) and (d), Supplier shall provide notification of a Personal Data Breach to Paylocity in accordance with this DPA.

12.3.3.3 For the purposes of Clause 8.9, all enquiries from the relevant Controller shall be handled solely by Paylocity. If Supplier receives an enquiry directly from a Controller, it shall forward the enquiry to Paylocity and Paylocity shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

12.3.3.4 For the purposes of Clause 10 and subject to this DPA, Supplier shall notify Paylocity about any request it has received directly from a Data Subject without obligation to handle it and is not obligated to notify the relevant Controller. Paylocity shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

(b) UK Personal Information.

12.3.4 *Controller-Controller, Controller-Processor and Processor-Sub-processor Transfers*. Transfers of Personal Information of UK Data Subjects from Paylocity (Data Exporter) in the UK to Supplier (Data Importer) outside the UK shall be conducted in accordance with this DPA and the UK Addendum.

12.3.5 *IDTA Additional Terms*. Where the transfer of Personal Information is subject to the UK GDPR and the transfer relies on the UK Addendum, the SCCs will apply in accordance with sub-section (a) and the following modifications: (i) the SCCs will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "Importer"; and (iii) any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) Swiss Personal Information

12.3.6 In relation to Personal Information subject to the Swiss Federal Act on Data Protection (FADP), the SCCs will apply in accordance with sub-section (a) and the following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " (FDPIC) and the "relevant courts in Switzerland".

13. **General Terms**

13.1 Order of precedence. For data transfers from the EU/EEA, UK, and Switzerland to a country other than the United States, in the event of any conflict or inconsistency between this DPA and the SCCs (or, where applicable, the UK or Swiss equivalent), the EU SCCs (or the UK or Swiss equivalent) shall prevail. In the event of inconsistencies between the provisions of this DPA and the Agreement, or any other agreements between the Parties, the provisions of this DPA shall prevail with respect to the subject matter hereof.

13.2 Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision(s) shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1 – Details of Processing

A. List of Parties

Data Exporter:
Name: Paylocity Corporation
Address: 1400 American Lane, Schaumburg, IL 60173
Contact person's name, position and contact details: Ellie Sharp, Chief of Data Privacy, privacy@paylocity.com
Activities relevant to the data transferred under these SCCs: Processing of Personal Information in connection with Paylocity's use of the Services under the Agreement.
Role (controller/processor): Controller or Processor

Data Importer:
Name: Supplier as identified in the Agreement
Address: Supplier's address as set out in the applicable Order Form.
Contact person's name, position and contact details: Supplier's contact details as set out in the Order Form
Activities relevant to the data transferred under these SCCs: Processing of Personal Information in connection with Paylocity's use of the Services under the Agreement.
Role (controller/processor): Controller, Processor, or Sub-processor (as applicable)

B. Description of Transfer

Categories of Data Subjects whose personal data is transferred
The specific categories of Data Subjects depend on the nature of the Services provided for in the Agreement and may include, but not limited to, Paylocity client employees and contractors, Paylocity clients' job applicants, Paylocity client employees' dependents and beneficiaries, Paylocity business contacts (clients, prospects), Paylocity employees and contractors, Paylocity job applicants, Paylocity employees' dependents and beneficiaries.

Categories of Personal Information transferred
The specific categories of Personal Information depend on the nature of the Services provided for in the Agreement and may include, but not limited to, personal identification (name, date of birth), contact details (email, phone, address), real-time or precise location, education and training details, employment-related data, family, lifestyle, and social circumstances, financial, economic and insurance data, including financial account numbers, billing and payment information, digital, device and social media identifiers or digital profiles, account credentials, contents of communications not directed to Paylocity, and any other categories of Personal Information provided by Paylocity in connection with the Services.

Sensitive Data transferred and applied restrictions or safeguards
The specific categories of Special Category of Information depend on the nature of the Services provided for in the Agreement and may include, but not limited to, financial information (bank account information, bank account number, bank statements, credit card number, debit card number, direct deposit information, routing number, credit history, state withholding tax information), racial or ethnic origin, nationality, citizenship status, driving license number, government identifiers (Social Security Number, passport numbers, national identification number, national identity card details), data concerning health, biometric data (retina scan, facial recognition, voice recognition, sleep pattern recognition), disability information (disability description, disability or specific condition linked to an ADA), genetic data (genetic sequence), political affiliation and activities, religion/religious beliefs, trade union membership, sexual orientation, sensory and electronic information.

Frequency of the transfer
Ongoing/regular (Personal Information will be transferred on an ongoing or regular basis, not intermittent)

Nature of the Processing
Personal Information will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Services provided to Paylocity; and/or
2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by Applicable Data Protection Laws and other applicable laws.

Purpose of the transfer and further Processing
As necessary to provide the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Paylocity in its use of the Services.

Period for which the Personal Information will be Retained
Subject to the 'Deletion or Return of Personal Information' section of this DPA, Supplier will Process Personal Information for the duration of the Agreement, unless otherwise agreed in writing.

For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing
Transfers to Sub-processors comprise the same categories of Data Subjects and Personal Information, and duration as set out above. The Sub-processors provide services to Data Importer in connection with its delivery of Services.

Competent supervisory authority/ies in accordance with Clause 13

- For transfers from the European Economic Area: Czech Republic’s Office for Personal Data Protection
- For transfers from the UK: UK Information Commissioner's Office
- For transfers from Switzerland: Swiss Federal Data Protection and Information Commissioner (FDPIC)

ANNEX 2 – Security Measures

These safeguards are designed to align with applicable laws and regulations and include the following measures:

Organizational Security Measures	**Security Roles & Responsibilities.** Roles and responsibilities are defined with regard to data, network, and systems access. Controls are in place that will allow only the necessary personnel access to maintain the day-to-day operations of the system. **Security Documentation**. Documented security policies and procedures are made available to all employees. **Control Assessment**. Conducts regular internal audits of its organization and technical protection measures. **System Monitoring**. Has controls in place that actively monitor the system and its peripheral systems for intrusions and vulnerabilities. **Disaster Recovery; Business Continuity.** Maintains business continuity procedures (including disaster recovery and crisis management protocols) and tests them at least annually, as appropriate to the size, nature, and complexity of its operations. **PCI DSS Obligation**. To the extent applicable, Supplier ensures the security of cardholder data it possesses or otherwise stores, processes, or transmits on behalf of the Client, or to the extent that it could impact the security of the Client's cardholder data environment.
Administrative Security Measures	**Personnel and Training.** All employees are required to complete data privacy and security training at a minimum annually, and personnel with access to Client Data needs to abide by Supplier's confidentiality and security obligations. **Third-Party Access.** Supplier conducts appropriate due diligence on third parties involved in performing the Services or who have access to systems that contain Client Data. **Contractual**. Data Importer will sign appropriate data transfer agreements in accordance with applicable privacy laws. **Change Management**. Change Management process provides technical teams with the tools to help ensure successful implementation of systems or applications that satisfy strategic, compliant, and business objectives.
Technical Security Measures.	**Physical Security.** Maintains physical and environmental security measures that control and restrict physical access to, and provide environmental protection for, systems that contain Client Data. **Network Security.** Network environment has complete control over its network environment, including selection of our own IP address range, creation of subnets and configuration of route tables and gateways. Appropriate network security and information transfer controls are deployed, including the use of firewalls, intrusion detection and prevention systems, proxy servers and secure file transfer technologies, or relevant equivalent technologies, in the operation of systems and facilities, in each case, consistent with industry standard to protect Client Data. Systems are architected based on cloud providers best practices for availability. **Access and Authorization.** Access controls are implemented for accounts created, administered, and operated by Supplier, including physical, administrative, and technological access control mechanisms designed to prevent unauthorized access to Supplier facilities and systems that store or allow access to Client Data. User identities are centrally managed, with security credentials assigned, users grouped, and user permissions controlled. Network access to our

	network is restricted to only the employees who need access for approved job responsibilities, and a uniform password policy is enforced for the SaaS product. Customers who interact with the product via the user interface must authenticate before accessing customer data. **Security and Vulnerability Scanning and Patch Management.** A formal patch management program is maintained, with regular patch management activities performed on relevant systems that process Client Data. **Application Security Tests and Assessments.** Security assessments are conducted at least annually on relevant systems that handle, maintain, or process Client Data. **Security Event Logs.** Access to the systems used to host Client Data and/or provide the Services to the Client is logged for compliance, audit, and incident investigation purposes. **Security of Processing**. Client information is protected through commercially reasonable safeguards over the hardware, software, personnel, and processes supporting the delivery of payroll and related services to the client. Company issued equipment is required to the use of disk encryption and antivirus and anti-malware software.
Data Transmission and Storage	**Data Encryption.** Client Data is encrypted both when in transit and at rest or transported/stored via physical media (e.g., tapes, disks, etc.) using cryptographically secure protocols that are consistent with commercially reasonable standards to encrypt Client Data. **Data Storage.** Data is stored within the network in a secure subnet that is not accessible by the outside network without proper identity and access management controls. Sensitive information, including personal and financial institution data, is encrypted using advanced industry-standard ciphers. User credentials are salted and encrypted using recognized encryption algorithms to prevent unauthorized access and ensure data integrity. **Security of Transmission**. Personal data is only transferred using encrypted mechanisms.