SECURITY ADDENDUM

This Security Addendum (this "**Addendum**") supplements the Master Subscription Agreement (https://www.payscale.com/content/legal/msa.pdf) or other agreement between Payscale and Customer that governs Customer's use of the Payscale Services ("**Agreement**"). Capitalized terms used in this Addendum and not defined shall have the meanings given to such terms in the Agreement. This Addendum is in effect for the period that Payscale processes any information Customer or its Users loads or otherwise inputs into the Payscale Services (or provides to Payscale for loading or inputting into the Payscale Services on Customer's behalf), and any information provided by Customer relating to its use of Professional Services ("**Customer Data**"). The Addendum may be amended from time to time by Payscale provided that such updates do not result in the degradation of the overall security of the Payscale Services.

1. Scope

1.1 Payscale maintains a security program ("**Security Program**") to protect Customer Data following guidance derived from industry standard frameworks such as, but not limited to, AICPA Trust Services Criteria (SOC2), NIST Cybersecurity Framework (CSF), International Organization for Standardization (ISO), and Center for Internet Security (CIS).

1.2 The Security Program is applicable to all Payscale Services (the "**Covered Payscale Services**") except for Benchmark.

2. Operating Plans

2.1 Incident Response Plan. Payscale maintains an incident response plan, including a breach notification process, to assess, escalate, and respond to identified cyber security incidents that impact the organization, the services provided to Customers, or result in data loss. Discovered intrusions are resolved in accordance with established procedures. The incident response plan is reviewed and updated at least annually.

2.2 Business Continuity & Disaster Recovery Plan. Payscale has a business continuity and disaster recovery plan in place to manage significant disruptions to operations and infrastructure. This plan is reviewed and tested annually by information technology, operations, and information security teams. Business continuity and resilience is supported using resilient cloud architectures, services, and providers.

3. Customer Data

3.1 Delineation and Identification. Payscale has implemented processes to delineate and identify Customer Data for special handling within Payscale's organization.

3.2 Data Segregation. Payscale maintains the capability to segregate and isolate Customer Data, disable functionality of applications using Customer Data, and deploy suitable application controls and firewalls so that Customer Data will not be commingled or corrupted by data from other sources.

3.3 Encryption

(a) Data in Transit. When Processing Customer Data, public connections to Customer computing environments and any other transmission via data transmission services or using the Internet will be protected using, as applicable, the following cryptographic technologies: IPSec, SSL/TLS, SSH/SCP, SFTP, or other technologies that provide similar or greater levels of security. Encryption algorithms will be of sufficient strength to protect data to commercially reasonable security levels and will utilize industry recognized hashing functions. Transmission may not use any cryptography algorithms developed internally by or for Payscale.

(b) Data at Rest. Customer Data at rest shall be protected using one or more industry standard and commercially reasonable encryption technologies as supported and applicable to the underlying storage.

(c) Removable Media. Payscale has policies and procedures in place designed to ensure that its employees and contractors are not permitted to copy Customer Data to a removable media device such as a USB flash, external hard drive, or CD/DVD for storage except where such action is authorized for backup purposes or at Customer request. All such media shall have encryption and other reasonable security measures restricting access and use as required by this Addendum.

4. Security. Payscale's systems have been designed to ensure that all physical and virtual hosts, networks, services, or platforms in which Customer Data is stored or processed are: (a) maintained solely on Payscale's or its third-party service providers property or premises and (b) maintained in a secure manner that satisfies the requirements of this Addendum.

4.1 Perimeter Defense. Payscale utilizes private networks and firewalls to secure internal systems, services, and networks from unauthorized access. Networks are protected by Intrusion Detection and Intrusion Prevention systems or designated to allow only authorized traffic.

4.2 Monitoring. Payscale utilizes a security information event monitoring (SIEM) system to pull security log and event information from servers, firewalls, routers, system users, and administrator activity. The SIEM is configured for alerts and is monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events. Security operations personnel monitor items detected and take appropriate action.

4.3 Vulnerability Management. Payscale monitors and scans for vulnerabilities on a regular basis. Vulnerability scans are run on a scheduled basis using industry-recognized scanning tools. Payscale follows a mitigation and remediation process where identified vulnerabilities are assessed and remediated by vendor supplied patches or where not applicable or available, through mitigating controls. On an annual basis, Payscale conducts third-party penetration tests on the Covered Payscale Services to identify security vulnerabilities.

4.4 Vendor Security. Payscale maintains a vendor management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security controls. Payscale communicates security and confidentiality requirements and operational responsibilities to third parties through contractual agreements, as necessary. The impact of any issues identified is assessed and remediated, if necessary.

4.5 Physical Security

(a) Payscale Offices. Physical access to Payscale offices is granted based on job responsibilities and work location. Access to offices can only be approved by appropriate personnel. Physical access is removed when access is no longer required and as a component of the employee termination process. Visitor logs are maintained. Badge readers control access to restricted areas within Payscale offices and data center locations. Unauthorized badge access attempts are denied and logged.

(b) Data Centers. Physical security controls and assurance reports are evaluated on an annual basis for data centers.

- **i.** Data center facilities include (1) physical access restrictions and monitoring that shall include a combination of any of the following: multi-zone security, person-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor.
- **ii.** Payscale hosts Covered Payscale Services in data centers that have attained SOC 2 Type II attestations (or equivalent or successor attestations or certifications). Each data center includes full redundancy and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. Payscale Service

data centers are serviced by multiple network connections, carriers, and/or ISPs for fault tolerance, redundancy, and availability.

iii. Payscale uses industry standard (or substantially equivalent) processes for secure destruction of sensitive materials, including Customer Data, before such media leaves Payscale's data centers.

4.6 Covered Payscale Service Authentication. Payscale has policies and procedures in place that require that, regarding any users of Covered Payscale Services:

(a) Each user must have a unique user ID and must be assigned a password.

(b) The Covered Payscale Services must log the date and time for all failed and successful user attempts to access the Covered Payscale Service.

(c) The Covered Payscale Services must log the date and time for all password changes to the Covered Payscale Service

(d) The Covered Payscale Services must limit the number of failed log-on attempts to a maximum of 10 before disabling the user ID.

(e) The Covered Payscale Offer must authenticate a valid user ID and password or token prior to granting access to network or system resources containing or permitting access to Customer Data.

(f) Authentication data transmitted over a public or shared network must be encrypted.

4.7 Endpoints. Endpoint protection is installed and activated on all endpoint devices to monitor and protect in real-time for virus and malware infections. Virus definition updates are pushed out to endpoint devices automatically on a regularly scheduled basis. Endpoints are provisioned with encrypted disks and remote lock capability. Payscale restricts personnel from disabling endpoint protection measures.

5. Malicious Code

5.1 Payscale utilizes commercially reasonable controls and processes to prevent the operation and transmission of malicious code for all computer systems containing or permitting access to Customer Data and in the delivery of its Covered Payscale Service.

5.2 Covered Payscale Services shall not contain viruses or malware that may result in either (a) inoperability of the Covered Payscale Service or (b) interruption, interference with the operation of the Covered Payscale Service (collectively, "**Illicit Code**"). If the Covered Payscale Service is found to contain any Illicit Code that adversely affects its performance or causes a material security risk to Customer Data, Payscale shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code.

6. Updates to Covered Cloud Offerings

6.1 Payscale follows a software development life cycle for Covered Payscale Services. All software development and releases are tracked and follow industry standard processes for code development, review, and testing. Releases are tracked and approved following best practices supporting separation of duties and least privileged where applicable and feasible. Software changes are tested prior to release with issues being identified and logged.

6.2 Payscale deploys updates to the Covered Payscale Services during scheduled maintenance windows, details of which are posted within the Covered Payscale Services prior to the scheduled period. In the event of a service interruption, Payscale posts a notification to the website describing the affected services.

7. Payscale Personnel

7.1 Background. Payscale performs background screening on all employees and contractors who have access to Customer Data in accordance with Payscale's then-current information technology security policy, subject to applicable laws.

7.2 Compliance. Payscale takes appropriate steps to ensure compliance with the Security Program by its employees, contractors, and subprocessors, to the extent applicable to their scope of performance, and all persons authorized to access Customer Data are under an obligation of confidentiality.

(a) Employee Policies. Payscale policies and operating procedures related to security are made available to personnel via the corporate intranet. Security policies and procedures are reviewed annually and updated as needed. Personnel are required to review and acknowledge these policies and procedures during on-boarding and annually thereafter. Payscale maintains a disciplinary process for personnel that do not comply with its security and confidentiality policies.

(b) Security and Privacy Awareness. Payscale maintains a security and privacy awareness program that includes appropriate training and education of Payscale personnel. Such training is conducted at time of hire and at least annually throughout employment at Payscale. Payscale conducts periodic security awareness education and communications regarding creating and maintaining a secure workplace.

7.3 Data Access. Payscale classifies informational assets in accordance with its data classification policy. Payscale assigns application and data rights based on authorized user roles and responsibilities, which align with the principle of least privilege and separation of duties where applicable and feasible.

(a) Restricted Access. Payscale's policies require that Customer Data will be accessible only by authorized Payscale employees, officers, directors, agents, contract workers and others who have a legitimate business need to access such information, with suitable user authentication, sign-on procedures, and access controls that satisfy the requirements of this Addendum.

(b) Authentication. Payscale has policies and procedures in place, regarding its employees and contractors, that require that: (i) users have a unique account identifier or user ID, (ii) authentication credentials such as passwords and tokens must not be used by anyone other than the users to whom they are assigned; and (iii) authentication credentials such as passwords may not be written down or stored in an unencrypted fashion. Payscale promptly disables authentication access for terminated users.

(i) **Passwords**. Payscale has established password policies and procedures based on industry standards and best practices including, but not limited to NIST Special Publication 800-63(b). Password policies focus on complexity and length and are promptly changed if suspected of being disclosed to unauthorized parties.

(ii) **Multifactor Authentication**. Direct access to production networks and systems is protected by multifactor authentication protocol. Such protocol may include certificate, device, PIN, or unique identifier.

(c) Access Review. Payscale periodically reviews its access to production systems of the Covered Payscale Service for administrative account access, appropriateness, and personnel changes. Where supported and feasible, separate administrator accounts are provisioned and used by authorized personnel to perform privileged functions.

8. Oversight and Review

8.1 Periodic Adjustment. Payscale will regularly monitor, evaluate, and adjust, as appropriate, the Security Program considering any relevant changes to applicable laws.

8.2 Internal Audits. Internal audits are aligned to the Security Program and compliance requirements. Payscale conducts internal control assessments to validate that its controls are operating effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate. Internal controls related to security are audited by an external independent auditor at least annually and in accordance with applicable industry standards.

8.3 External Audit Reports. Payscale will maintain commercially reasonable audit reports such as the AICPA SOC2 (or equivalent or successor attestations or certifications) produced by third parties and updated annually based on an audit performed at least once every 12 months (the "External Audit Reports") to evaluate the continued effectiveness of the Security Program for Covered Payscale Services. Payscale may add or remove standards at any time where such standard changes: (i) do not materially impact the integrity of the Security Program or (ii) are no longer applicable to the Covered Payscale Service. Payscale may replace an External Audit Report with an equivalent or enhanced alternative. Upon request by a Customer, Payscale will make the External Audit Reports available for review by Customer to demonstrate compliance by Payscale with its obligations under this Addendum. Payscale regularly reviews controls as described in the External Audit Reports.

8.4 Review Personnel. Payscale has a designated information security function responsible for the development, maintenance, review, and approval of Payscale's security standards and policies. The function is responsible for the oversight and governance of the Security Program.

9. Customer Responsibilities

9.1 Transfer. Covered Payscale Services provide secure methods for Customers to transfer Customer Data directly to Covered Payscale Services and role-based access controls. Customer is responsible for configuring such access controls within the Covered Payscale Service.

9.2 Access. Covered Payscale Services allow Customers to: (a) integrate with SAML solutions, (b) manage passwords; and (c) prevent access by users with an inactive account. Customer manages each user's access to and use of the Covered Payscale Services by assigning to each user a credential and user role that controls the level of access to the Covered Payscale Service. Customer is solely responsible for reviewing the Security Program and making an independent determination as to whether it meets Customer's requirements, considering the type and sensitivity of Customer Data that Customer processes within the Covered Payscale Services. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Covered Payscale Services.

9.3 Storage. Customer is responsible for its use of the Covered Payscale Service and its storage of any copies of Customer Data outside Payscale's or Payscale's subprocessors' systems.

9.4 Customer's Security Assessment. Customer agrees, based on its current and intended use of the Covered Payscale Service, that the Covered Payscale Service, Security Program, and Payscale's commitments under this Addendum (a) meet Customer's needs and (b) provide a level of security appropriate to the risk in respect of the Customer Data.

9.5 Contact. Customer agrees to identify and maintain appropriate contact(s) for all information security incident and information security-related communication.

9.6 No Assessment of Customer Data. Payscale has no obligation to assess Customer Data to identify information subject to any specific legal requirements.