GREAT PLACE TO WORK® INSTITUTE INC. (GPTW)

EXTERNAL SECURITY POLICY

This Policy is intended to help communicate externally to Companies the Security Policy used by GPTW as well as the Network Affiliates and Partners of GPTW and is incorporated by reference into their respective Agreements.

1. General Business Information

GPTW provides products and services assessing workplace culture, performance, certification, and accreditation to assist companies and organizations in evaluating and improving their workplaces. GPTW was incorporated in the State of California on June 30, 1998 and is a privately-held company. It is headquartered in Oakland CA at 1999 Harrison Street, Suite 2070 and has an affiliated office in Toronto ON at 130 Queen Quay, suite 619.
.

The FEIN for GPTW is 91-1917672 and its DUNS number is 05 1812683 and the Canadian business number (BN) is 800817819 RT 0001. There have been no material claims or judgments against GPTW in the last 5 years and has never suffered a data loss or security breach. To the best of our knowledge, none of our Third-Party Cloud providers suffered a data loss or security breach within the last 3 years.

2. Policy to Safeguard Company Data

GPTW understands the value and sensitivity of Company data. Therefore, keeping Company data secure is of paramount importance to GPTW. GPTW has robust policies in place to manage and secure Company data.

Risk Management

GPTW has a documented Risk Management Policy. Risk assessments are performed quarterly.

Human Resource Security

GPTW's Human Resources takes a number of steps to help protect Company data. GPTW performs background verification checks on all candidates for employment and our employees must sign the terms and conditions of employment. Furthermore, GPTW conducts mandatory semi-annual privacy and security awareness training for all staff. GPTW will notify Company if a GPTW employee who had access to Company data has been terminated or changed roles within GPTW that warrants an "Appropriateness of access review."

Data Collection

GPTW only collects data needed for its intended purposes like Great Workplace Certification, Best Workplaces Lists, Advisory and High Trust Culture Consulting engagements, Accelerated Leadership Performance, etc.

Data Access

Access to Company data is only granted to those with a legitimate need. Company data is only accessed by GPTW employees that are authorized based on job role. Survey access is controlled so that survey respondents cannot see another's responses. Data is partitioned so that Company users cannot see another company's data.

Access Control
GPTW has a documented Access Control Policy which includes a formal user registration and de-registration process to enable assignment of access rights, unique IDs for all users, a periodic review of access rights with owners of the information systems or services, restrictions and control of privileged access rights by management, an authorization process to allocate and control privileged access rights, monthly review of privileged access, a formal Password Policy, a policy that forces users to change their password at first log-on, password requirements (such as minimum length, complexity, periodicity to change, password history), and encrypted passwords in store and transmit. GPTW will notify Company within 72 hours from GPTW becoming aware of any confirmed or suspected leak of Company data. Enforcement mechanisms are applied to GPTW employees who violate privacy policies or confidentiality requirements.

Servers
On premises servers are in a locked, climate-controlled server room with access limited to authorized personnel. Cloud servers reside in data centers with restricted administrative access. Company data is encrypted in transit and in storage using a commercially available dual key AES 256 bit encryption software.

Policy Reviews
Data privacy & security policies are reviewed monthly.

3. Policy to Safeguard Company Employee Data

Data Collection
The Company Employee Data are the survey responses given by the Company's Employees. The nature and purpose as well as the subject matter and duration of the Processing of the Company Personal Data is to collect Company employee survey data for processing and archiving scientific and historical research purposes and statistical purposes assessing workplace culture, performance, and accreditation to assist organizations in evaluating and improving their workplaces. This exact language is found in Article 89 of the GDPR. The types and categories of Company Personal Data to be processed is found in the demographic section and Trust Index questions of the survey.

The survey and analytics software platform operate by uploading to the system an email address list for the Company's Employees taking the survey and, optionally, other information such as pre-coded demographics, etc. by GPTW. The email list is stored encrypted in a separately partitioned area from the Company Employee Data. When the Company survey opens, the email list is used to generate a personalized invite to each Company Employee which is a log-in identifier unique to each Company Employee. When the project is finalized, the email list used to link to the Company Employee Data is deleted. As a result, the Company Employee Data is immediately de-identified and made anonymous.

To protect the confidentiality of the Company Employee Data, GPTW uses a suppression algorithm. GPTW will not report on Assessment results in which fewer than five (5) people in a Company demographic group have responded.

A unique identifier for Data Subjects may be kept as long as it is assigned randomly at the time of survey (e.g. as a sequential number generated by a database upon the insertion of a new record) and is not associated with external data that create a re-association with the Data Subject's Personal Data; the unique identifier is only used as required within a relational database for Survey responses and associated data for a given year.

Data Access
Access to Company data is only granted to those with a legitimate need. Company data is only accessed by GPTW employees that are authorized based on job role. Survey access is controlled so that survey respondents cannot see another's responses. Data is partitioned so that Company users cannot see another company's data.

Access Control
GPTW has a documented Access Control Policy which includes a formal user registration and de-registration process to enable assignment of access rights, unique IDs for all users, a periodic review of access rights with owners of the information systems or services, restrictions and control of privileged access rights by management, an authorization process to allocate and control privileged access rights, monthly review of privileged access, a formal Password Policy, a policy that forces users to change their password at first log-on, password requirements (such as minimum length, complexity, periodicity to change, password history), and encrypted passwords in store and transmit. GPTW will notify Company within 72 hours from GPTW becoming aware of any confirmed or suspected leak of Company data. Enforcement mechanisms are applied to GPTW employees who violate privacy policies or confidentiality requirements.

Servers
The survey platform is hosted by Cloud providers Microsoft Azure and Amazon Web Services. Their security documentation is available on their respective websites. The Cloud providers have physical locations in California and Virginia. All data is back upped between the Cloud providers daily at these fully redundant hot-sites.

Policy Reviews
Data privacy & security policies are reviewed monthly.

4. Data Protection.
GPTW will use commercially reasonable efforts consistent with industry standards to collect, transmit, store, protect and maintain the Data and Company Data obtained through the Services. GPTW complies with Service Organization Controls (SOC) Report 1 and 2 under the Statement on Standards for Attestion Engagements (SSAE) 18 standard as well as with the International Organization for Standardization (ISO) 27001:2013 and ISO 9001:2015 standards and the National Institute of Standards and Technology (NIST 2015) cybersecurity framework. GPTW also complies with the

Payment Card Industry Data Security Standard (PCI DSS). GPTW considers the above-identified third party reports confidential and does not release them to any company. GPTW has thousands of clients and a few have asked for the same information as your Company. There are several reasons for this policy. First, the reports are static in time and may not cover the entire term of the company's engagement. Second, the reports provide no legal protection. Third, a company having possession of these reports places itself at serious risk for no benefit, e.g. should there be a GPTW security breach, any company in possession of these reports would be an immediate litigation target and would have to prove that their possession of the reports did not cause the GPTW breach. Instead, GPTW provides the highest standard of legal protection by warranting to the company that during the entire term of the engagement GPTW will comply with the above industry standards.

5. Data Privacy.

GPTW maintains a full-time Chief Data Protection Officer (CDPO) and staff to ensure compliance with these policies. The CDPO reports directly to the CEO of GPTW. GPTW also employs full-time a Certified Information Privacy Practitioner (CIPP) who is certified by the International Association of Privacy Professionals at www.iapp.org whose credentials are accredited by the American National Standards Institute (ANSI) under the International Organization for Standardization (ISO) standard 17024:2012. ANSI is an internationally respected accrediting body that assesses and accredits certification programs that meet rigorous standards. ANSI's personnel certification accreditation program was the first such program in the United States to fulfill the requirements of ISO/IEC 17011, which represents the global benchmark for accreditation body practice.

GPTW complies with the European Union (EU) 2016 General Data Protection Regulation (GDPR) and all data protection or privacy laws of any other country (Data Protection Laws). GPTW is also certified under the US/EU and US/CH Privacy Shield. GPTW collects Data for processing and archiving scientific and historical research purposes and statistical purposes assessing workplace culture, performance, and accreditation to assist organizations in evaluating and improving their workplaces. This exact language is found in Article 89 of the GDPR.

In connection with the Services, GPTW may receive, process and store Personal Data in the United States or other jurisdictions. Personal Data received by GPTW will be protected by GPTW as described in the Section above. In the event that consent of any individual is required to be obtained before transfer of Personal Information to GPTW, Company is responsible for obtaining the consent of any affected individual. Said consent needs to be freely given, specific, informed, unambiguous and given by a statement or clear affirmative action.

Scoped Data

GPTW has a data classification and retention program for Scoped Data that identifies the data types that require additional management and governance. GPTW has a documented response program to address privacy incidents, unauthorized disclosure or breach of Scoped Data. Scoped Data is not disclosed to third parties, within or outside the United States. GPTW has a documented privacy program with administrative, technical, and physical safeguards for the protection of Scoped Data including the use of encryption tools. Mobile devices are not used by GPTW employees to access Scoped Systems and Data. GPTW does not provide cloud applications.

Compliance and Incident Response
GPTW employees are reminded or informed on a monthly basis of our privacy and security policies. Their physical compliance is monitored daily where appropriate or applicable. GPTW maintains an internal compliance and ethics reporting mechanism and GPTW employees are given training in how to report compliance issues. GPTW also maintains an Incident Management program that is reviewed, approved by management and tested annually. All privacy complaints and privacy incidents are directed and responded to by the Director of Legal Affairs. Enforcement mechanisms are applied to GPTW employees who violate privacy or confidentiality policies.

6. Policy Regarding Ownership and Use of Data

Personal Data
In order to successfully render its services, GPTW may collect Personal Data which means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data excludes information provided by an individual directly to GPTW so long as GPTW was not collecting such information on behalf of Company or in furtherance of completing transactions as required pursuant to this Agreement.

Company Data
Company Data means Company's proprietary data and information that Company provides to GPTW so that GPTW may, as part of the Services, conduct an Assessment (e.g., demographic and corporate information necessary to distribute the Survey to participants (such as email address, employee ID, and other personally identifying information) and the data provided by Company to GPTW for the Culture Audit). For the avoidance of doubt, Company Data does not include either Aggregate Data or Raw Data as defined below. The Company Data and all Intellectual Property Rights remain the exclusive property of the Company. GPTW will use Company Data solely to perform the Services and in a manner that is compatible with the purposes for which such Company Data is furnished to GPTW or subsequently authorized to be used, and GPTW will ensure that any Personal Data included in Company Data is properly maintained and protected.

Aggregate Data and Raw Data
Aggregate Data means (a) the Company-specific information, data, and content contained in any report(s) delivered by GPTW to Company pursuant to this Agreement; and (b) any other aggregated data that is derived from the Raw Data and that is delivered by GPTW to Company pursuant to this Agreement. For the avoidance of doubt, Aggregate Data does not include any Raw Data or Company Data. Raw Data means the confidential and anonymous responses received by GPTW from Company and Company's employees in connection with, among other things, the Trust Index Survey(s) and/or Culture Audit(s), Culture Brief(s), focus groups, and one-to-one interviews administered by GPTW pursuant to this Agreement. For the avoidance of doubt, Raw

Data does not include any Aggregate Data or Company Data. The Raw Data and the Aggregate Data obtained through the Services provided, and all Intellectual Property Rights are and will remain the exclusive property of GPTW. The Raw Data will not be provided to the Company by GPTW in order to protect the confidentiality of Company respondents. GPTW intends to use the Aggregate Data solely for the internal purposes of GPTW, including without limitation for benchmarking, creation of best practices and other R&D purposes. GPTW will not share non-anonymous, Company-specific information about the Company's results with any third parties without first receiving prior written permission from Company (i.e., the Data is not intended to be associated with the Company or any individual Company employee). This will not apply in connection with any of the Best Workplaces Lists. Reports provided by GPTW to Company may be distributed internally by Company, but any external distribution requires prior written approval from GPTW which will not be unreasonably withheld. Aggregate Data and Raw Data are collectively referred to as Data herein.

Intellectual Property
The GPTW Intellectual Property, and all Intellectual Property Rights therein will remain the exclusive property of GPTW or its Affiliate Licensees. The Company is not acquiring any rights to any GPTW Intellectual Property because of the Agreement between both parties. Without GPTW's prior written approval, which may be withheld in GPTW's sole discretion, the Company will not use or re-use any GPTW Intellectual Property in any manner other than pursuant to its receipt of the Services during the Term (including in any surveying conducted either in-house or with another vendor outside of the scope of the Agreement).

Confidentiality
All information provided by the Company to GPTW or otherwise obtained by GPTW as a receiving Party relating to the business or operations of the Company or its clients or any person, firm, company or organization associated with the Company, will be treated by GPTW as confidential, and GPTW will not disclose the same to third parties without the prior written consent of the Company. The Parties acknowledge and agree that the confidential information of the Company does not include the Raw Data and the Aggregate Data, which are confidential information of GPTW.

7. Business Continuity and Disaster Recovery Plan

GPTW has a confidential, documented policy for business continuity and disaster recovery, including an annual schedule of required tests, annual BC/DR tests, a Pandemic Plan, annual Business Impact Analysis, and insurance coverage for business interruptions or general services interruptions.

Additional paper records off-site location:
Iron Mountain – Union City
29555 Kohoutek Way
Union City, CA 94587
Phone: 800-899-4766

8. Operations Security

GPTW has the following policies in place regarding Operations Security:

- Documented operating procedures for Information Processing Facility.
- Documented Change Management process.
- Process for Capacity Management and Capacity Plan for mission critical systems.
- Detection, prevention and recovery controls to protect against malware.
- A formal policy prohibiting the use of unauthorized software by GPTW employees.
- Installed anti-malware software on all computers and information systems.
- Regular monthly updates of anti-malware software.
- An established backup policy to define organizations' requirements for backup of information, software and systems, including encryption of the backup.
- An established Log Management standard including the maintenance of event logs recording user activities, exceptions, faults and information security events that are reviewed monthly.
- An established Vulnerability Management process for all information processing systems.

9. Communications Security

GPTW has the following policies in place regarding Communications Security:

- Firewall protection for all systems and Internet connectivity.
- Special controls implemented to protect information passing over public networks and Wireless networks.
- Maintaining routers and Access Control Lists.
- Maintaining IDS/IPS Technology.
- Two-factor authentication to control access from public accessible networks.

10. System acquisition, development and maintenance

As part of GPTW's information security requirements, we include the information security requirements for new information systems or enhancement of existing information systems, use formal change control process to all changes to systems within the development life cycle, maintain a version control for all software updates and restrict and control modifications to software packages by limiting to necessary changes only.

11. Physical Security

GPTW enforces defined security perimeters to protect Company's sensitive or critical information and information processing facilities. As part of this enforcement, GPTW has restricted access to its sites and buildings to authorized personnel only and implemented physical barriers where applicable, to prevent unauthorized physical access and environmental contamination. GPTW has also separated our information processing facilities we manage physically from those managed by external parties and implemented physical access controls to protect secured areas to ensure that only authorized personnel are allowed access. Access to

areas where confidential information is processed or stored is restricted to authorized individuals only. The use of photography, video, audio and other recording equipment, such as cameras in mobile devices in secure areas is restricted. GPTW has developed and implemented a clear desk and clear screen policy. GPTW has implemented controls to minimize risk from theft, fire, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.

12. Supplier Relationships.

GPTW has a documented policy for supplier relationships and maintains a list of all suppliers we use.

13. Asset Management.

GPTW has a documented Asset Management Procedure and maintains an asset inventory which is accurate, up to date and aligned with other inventories. In addition, GPTW has a documented Acceptable Use Policy. GPTW's termination process includes the return of all previously issued physical and electronic assets owned by GPTW.

GPTW has a secure process for Disposal of Media and sensitive information.

14. Compliance.

GPTW maintains a list of applicable legislative, statutory, regulatory and contractual requirements required by the organization. GPTW has an annual independent review of information security and has monthly technical compliance reviews including penetration testing and vulnerability scans.

October 1, 2018