Notice at Collection and Privacy Policy for Employees Residing in California

Henley Enterprises Inc., Henley Pacific LA LLC and Henley Pacific LLC and their affiliates (herein known as the "**Company**") are providing you with this Notice at Collection and Privacy Policy for Employees Residing In California (**"Notice"**) to inform you about how we collect, use, and disclose your Personal Information.

The Company adopts this notice to comply with the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (collectively, "**CPRA**"), and other California privacy laws. Any terms defined in the CPRA have the same meaning when used in this Notice.

California Notice at Collection: Company collects the personal information identified in Section I for the purposes identified in Sections I and II and retains it for the period described in Section IV. We do not sell your personal information or disclose it for cross-context behavioral advertising ("**sharing**"). We also do not collect or process sensitive personal information for the purpose of inferring characteristics about you. To the extent you provide the Company with personal information about your dependents, spouse, beneficiaries, or emergency contacts, you are responsible for providing this notice to them.

Assistance For The Disabled

Alternative formats of this Privacy Policy are available to individuals with a disability. Please contact us at privacynotice@vioc.net or (833) 204-0493 for assistance.

This Notice explains:

Scope

This Notice applies to the Personal Information of California residents who are (a) employees, or (b) employees' dependents, emergency contacts, and beneficiaries (**"Related Contacts"**), (all collectively, **"HR Individuals"**). This Notice informs HR Individuals about the categories of personal information Company has collected about them in the preceding twelve months as well as the categories of personal information that the Company will collect about HR individuals in the future.

Except where the Notice specifically refers only to a specific category of HR Individuals, e.g., employees, this Notice refers to all categories of HR Individuals collectively.

I. Categories of Personal Information We Collect

The Company collects the following categories of Personal Information. Not all categories may be collected about every HR Individual.

1. Identifiers And Professional Or Employment-Related Information

1.1 **Personal Information Collected:** The Company collects identifiers and professional or employment-related information, including the following:

Identifiers: real name, nickname or alias, postal address, telephone & cellphone number, e- mail address, Social Security number, signature, Internet Protocol address, visual image and likeness, bank account name and number for direct deposits, driver's license number, or state identification card number, passport number, credit card number, and debit card number.

Family Information: contact information for family members listed as emergency contacts, contact information for dependents and other dependent information, medical and health information for family members.

Professional or Employment-Related Information: compensation, bonuses, Henley Unit Growth Plan Grants, benefits, attendance, performance reviews, counseling notices, personnel files, reimbursements, education, corporate credit card details, membership in professional organizations, professional certifications, work eligibility in order to comply with legal requirements, and current and past employment history.

1.2 **Purposes of Use:**

Managing Personnel:

- Managing personnel and employment matters, as well as the relationship with Related Contacts
- To set up a personnel file
- To administer compensation, bonuses, other forms of compensation, and benefits (as permitted by law)
- To manage vacation, sick leave, and other leaves of absence
- To provide training
- To evaluate job performance and consider employees for other internal positions
- To develop a talent pool and plan for succession
- Career development activities
- For diversity and inclusion programs
- Conducting employee surveys
- To engage in crisis management
- To fulfill recordkeeping and reporting responsibilities
- To maintain an internal employee directory and for purposes of identification
- To facilitate communication, interaction, and collaboration among employees
- Arranging team-building and other morale-related activities
- Managing employee-related emergencies, including health emergencies
- To promote the Company as a place to work
- To arrange and manage Company-sponsored events and public service activities
- Workforce reporting and data analytics/trend analysis
- To design employee retention programs
- To protect the health and safety of HR Individuals, visitors, customers, and the public, including, but not limited to, responding to medical emergencies, reducing the risk of exposure to infectious disease and preventing its spread in compliance with applicable laws and regulations, and protecting the safety and security of Company's facilities

Monitoring, Security, And Compliance:

- To monitor the use of Company information systems and other electronic resources
- To conduct internal audits
- To conduct internal investigations
- To administer the Company's whistleblower hotline
- To protect the safety and security of the Company's facilities
- To report suspected criminal conduct to law enforcement and cooperate in investigations
- To maintain the security and integrity of Company's information and electronic resources including, but not limited to, monitoring use of Company's electronic resources, preventing unauthorized access to Company's electronic resources, preventing malicious software distribution, debugging, audits, disaster recovery, business continuity, and cyber security.

Monitoring, Security, And Compliance: continued

- To protect the rights or property of Company, including, but not limited to, detecting and preventing fraud or other types of wrongdoing, managing litigation involving Company, and other legal disputes and inquiries, reporting suspected criminal conduct to law enforcement and cooperating in investigations, short-term transient use of personal information, responding to requests or orders from governmental agencies, exercising Company's rights under applicable law, and supporting any claim, defense, or declaration involving Company in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel.

Conducting Our Business:

- For communications with prospective, current, and former employee and customers
- To make business travel arrangements
- To engage in project management
- Managing business expenses and reimbursements
- To promote the business
- To provide directory and contact information for prospective and current business partners

2. Personal Information Categories from Cal. Civ. Code § 1798.80l

The Company collects categories of Personal Information listed in Cal. Civ. Code §1798.80(e) (other than those already listed in "Identifiers," above) as follows for the corresponding purposes listed below:

- Photograph, physical description, visual image, and likeness: (a) for security and internal identification purposes, and (b) to identify employees to co-workers, prospective and current customers, and other third parties.
- Medical information: (a) to the extent necessary to comply with the Company's legal obligations, such as to accommodate disabilities; (b) to conduct a direct threat analysis in accordance with the Americans with Disabilities Act and state law; (c) for workers' compensation purposes; (d) for occupational health surveillance; (e) for occupational health and safety compliance and recordkeeping; (f) e.g., your body temperature, COVID-19 diagnosis, COVID-19 related testing results, whether you have or display certain symptoms such as fatigue, cough, sneezing, aches and pains, runny or stuffy nose, sore throat, diarrhea, headaches, sudden loss of smell or taste, or shortness of breath, whether you have been in close contact in the last 14 days with anyone who has exhibited any of these symptoms, whether you have been in close contact in the last 14 days with anyone who has tested positive for COVID-19, any COVID-19-related doctor's notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, and correspondence with you and your healthcare provider(s) regarding any request for accommodation or medical leave of absence related to COVID-19, COVID-19 vaccination-related information) (g) to secure fitness-for-duty examinations; (h) to administer leaves of absence and sick time; (i) to provide a wellness program; and (j) to respond to an employee's medical emergency. Note: This Notice does not cover medical information governed by the Health Insurance Portability and Accountability Act or the Health Information Technology for Economic and Clinical Health Act.

- Benefits information: to administer short- and long-term disability benefits.

3. Characteristics Of Protected Classifications Under California or Federal Law

The Company collects information about race, age, national origin, disability, sex, and veteran status as necessary to comply with legal obligations, including the reporting requirements of the federal Equal Employment Opportunity Act, the federal Office of Contracting Compliance Programs (applicable to government contractors), and California's Fair Employment and Housing Act. The Company also collects information about disability status to the extent an employee may need special assistance during emergencies

from the Company or first responders.

The Company also collects the following characteristics (in addition to those listed above) for its diversity and inclusion programs (including analytics): (a) religion, (b) sex, (c) gender, (d) pregnancy, (e) childbirth, (f) breastfeeding, or related medical conditions, (g) sexual orientation, (h) disability, (i) gender identity, (j) gender expression, (k) marital status, (l) age, (m) familial status, or (n) ancestry.

The Company also uses this Personal Information for purposes including: with respect to disability, medical condition, familial status, marital status, and pregnancy, childbirth, breastfeeding, and related medical conditions, as necessary to comply with Federal and California law related to leaves of absence and accommodation; with respect to military and veteran status, as necessary to comply with leave requirements under applicable law and for tax purposes; with respect to age, incidentally to the use of birth date for birthday celebrations and identity verification; with respect to religion and pregnancy, childbirth, breastfeeding, and related medical conditions, as necessary for accommodations under applicable law; with respect to protected classifications, such as national origin and citizenship, to the extent this information is contained in documents that you provide in I-9 documentation; and with respect to marital status and familial status, for Company events and as necessary to provide benefits and for tax purposes.

The Company collects this category of Personal Information on a purely voluntary basis, except where required by law, and uses the information only in compliance with applicable laws and regulations.

4. Commercial Information

4.1 **Personal Information Collected:** The Company collects commercial information including the following: business travel and expense records.

4.2 **Purposes of Use:** reimbursement of business expenses, auditing, data security, preventing illicit activity.

5. Biometric Information

5.1 **Personal Information Collected:** The Company collects biometric information, including the following: a fingerprint and/or facial template which is converted into a mathematical representation – creating a scan template. As a result of this conversation to a scan template, it's not possible to reproduce the original fingerprint image, and the image is not stored within the systems.

5.2 **Purposes of Use:** to track clock-in and clock-out time using biometric information, to control access to secure facilities, to monitor the use of Company information systems and other electronic resources or information systems, and to protect the safety and security of the Company's facilities.

6. Internet Or Other Similar Network Activity

6.1 **Personal Information Collected:** The Company collects information about employees' use of the Internet or other similar network activity, including the following: browsing history, search history, log in/out and activity on the Company's electronic resources, and information regarding an employee's interaction with an Internet web site, application, or advertisement, and publicly available social media activity.

6.2 **Purposes of Use:** to monitor the use of the Company's information systems and other electronic resources or information systems, to conduct internal audits for training and development purposes, to conduct internal investigations, to protect the safety and security of the Company's facilities, to determine whether disciplinary action is warranted, and for the purposes listed above for “Monitoring, Security, and Compliance” and “Conducting Our Business.”

7. Geolocation Data

7.1 **Personal Information Collected:** The Company collects geolocation data, including the following: (a) information that can be used to determine a mobile device's physical location; (b) information that can be used to determine vehicle's physical location; and (c) information that can be used to determine an employee's physical location.

7.2 **Purposes of Use:** to assist with routing, to confirm that an employee has arrived and left an off-site work location when scheduled, for customer service purposes, to provide training, to manage employee-related emergencies, to monitor the safety of an employee, to monitor compliance with Company policies, and to determine whether further disciplinary action is warranted.

8. Sensory Or Surveillance Data

8.1 **Personal Information Collected:** The Company collects sensory or surveillance data, including the following: voicemails, recordings of customer service telephone calls, and footage from video surveillance cameras.

8.2 **Purposes of Use:** for purposes of communications, to protect the safety and security of the Company's facilities and personnel through video surveillance, to monitor compliance with Company policies, to provide training, for quality assurance, and to determine whether to discipline employees.

9. Non-Public Education Information

9.1 **Personal Information Collected:** The Company collects education information, including the following: academic transcripts and completion records.

9.2 **Purposes of Use:** to determine suitability for internal roles, certifications, and promotions, to determine eligibility for training courses, confirm compliance with required state, local, and federal training mandates, and to assist with professional development.

10. Profile Data

10.1 **Personal Information Collected:** The Company collects profile data, including the following: Personal Information to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

10.2 **Purposes of Use:** to determine suitability for internal roles, certifications, and promotions, to determine eligibility for training courses, confirm compliance with required state, local, and federal training mandates, and to assist with professional development.

11. Background Screening Information

11.1 **Personal Information Collected:** The Company collects background screening information, including results of the following types of background screening: criminal history; sex offender registration; motor vehicle records; credit history (only for specifically identified jobs/positions); employment history; drug testing; and educational history. Note: This Notice does not cover background screening governed by the Fair Credit Reporting Act, which is excluded from the California Consumer Privacy Act.

11.2 **Purposes of Use:** to screen employees for risks to the Company and continued suitability for their jobs and to evaluate employees for internal promotions.

12. Preferences

12.1 **Personal Information Collected:** The Company collects employee preferences information, including preferred meals, seating, and other travel preferences, desired working hours, workspace preferences, and preferred work supplies.

12.2 **Purposes of Use:** for travel and event planning, for employee satisfaction, and to plan and arrange work supplies and workspaces.

13. Related Contacts

13.1 The Company only collects contact information about emergency contacts.

13.2 Company may collect the following categories of Personal Information about spouses or domestic partners, dependents, and beneficiaries: (a) identifiers, (b) commercial information if, for example, Company arranges travel for a dependent to attend a Company event; (c) internet activity information if the individual uses Company electronic resources and web sites; (d) sensory or surveillance data if the individual enters Company facilities; (e) § 1798.80 Personal Information, such as insurance policy numbers if the individual is covered by Company insurance of health information, for example, infectious disease testing when a Related Contact attends a Company event; and (f) Protected Categories of Personal Information, for example, childbirth to administer parental leave, marital status to pay taxes, and familial status to administer benefits.

Note on inferring characteristics: Company does not collect or process sensitive Personal Information or characteristics of protected classifications for the purpose of inferring characteristics about the HR Individual.

Note on Deidentified Information: At times, Company converts Personal Information into deidentified information using reasonable measures to ensure that the deidentified information cannot be associated with the individual ("**Deidentified Information**"). Company maintains Deidentified Information in a deidentified form and does not attempt to reidentify it, except that Company may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes ensure that the information cannot be associated with the individual.

II. Purposes For Which We Use Your Personal Information

In addition to the purposes identified above, the Company may also collect and use employees' Personal Information to facilitate administrative functions and information technology operations and for legal reasons and corporate transactions. These purposes include, but are not limited to the following:

- manage and operate information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning;
- manage litigation involving the Company and other legal disputes and inquiries and to meet legal and regulatory requirements;
- in connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of the Company or any of its subsidiaries or affiliates;
- manage licenses, permits, and authorizations applicable to the Company's business operations;
- comply with Company policies and applicable laws and regulations, including, without limitation, applicable tax, health and safety, antidiscrimination, immigration, labor and employment, and social welfare laws;
- monitor, investigate, and enforce compliance with and potential breaches of Company policies and procedures and legal and regulatory requirements;
- comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons; and
- exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.

III. Categories of Sources From Which We Collect Your Personal Information

- You, for example, in your application, forms you fill out for us, assessments you complete, surveys you submit, and any information you provide during the course of your relationship with us.
- Your spouse or dependent with respect to their own Personal Information.
- Affiliated companies.
- Third parties, for example, job references, business partners, professional employer organizations or staffing agencies, insurance companies.
- Automated technologies on Company's electronic resources, for example, to track logins and activity across Company network.
- Surveillance/recording technologies installed by Company, for example, video surveillance, time clocks, voicemail technologies, webcams, audio recording technologies, and blue-tooth technologies, any of these with consent to the extent required by law.
- Government or administrative agencies, for example, law enforcement, public health authorities, California Department of Industrial Relations, Employment Development Department.

IV. Retention Period

We retain Personal Information for as long as needed or permitted in light of the purpose(s) for which it was collected. The criteria used to determine our retention periods include:

- The duration of your employment;
- The length of time we have an ongoing relationship with you or your dependents/beneficiaries and the length of time thereafter during which we may have a legitimate need to reference your Personal Information, such as to address issues that may arise;
- Whether there is a legal obligation to which we are subject (for example, certain laws may require us to keep your employment records for a certain period of time); and
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation, litigation holds, or regulatory compliance).

Generally, we retain your Personal Information no longer than necessary for the purposes described in Sections I and II above and in accordance with the Company's record retention schedule unless Company is required to retain your Personal Information longer by applicable law or regulation, by administrative needs, by legal process, or to exercise or defend legal claims.

V. How We May Disclose Your Personal Information

The Company may disclose your Personal Information for the purposes described in this Notice to the following parties:

- Your direction: We may disclose your Personal Information to third parties at your direction.
- Affiliates and Subsidiaries: We may disclose your Personal Information to our affiliates and subsidiaries.
- Service Providers: We may disclose your Personal Information to service providers, such as recruiters, pre-employment screening services, third-party benefits administrators, background check providers, payroll and expense administrators, worker's compensation vendors, and others.
- Governmental Authorities: As required by law or legal process, we may disclose your Personal Information to federal or state regulatory agencies, law enforcement, courts and other governmental authorities.
- Customers: We may disclose a service representative's business contact information with customers.
- Professional Advisors: We may disclose your Personal Information to our professional advisors, such as auditors and law firms.
- Required Disclosures: We may be required to disclose Personal Information (a) in a court proceeding, (b) in response to a court order, subpoena, civil discovery request, other legal process, or (c) as otherwise required by law.
- Legal Compliance and Protections: We may disclose Personal Information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of our company, our users, or others.
- We may also disclose your Personal Information to a third party in the context of any reorganization, financing transaction, merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Additional Information Regarding Disclosures of Personal Information

The California Privacy Rights Act (CPRA) requires that we provide you with the following information about sales and "sharing" and disclosures of your personal information to third parties for "business purposes", as those terms are defined in the CPRA:

- **Service providers:** Company may disclose to service providers any of the categories of personal information listed in Section I, above, for the business purpose of performing services on Company's behalf and, in particular, for the specific purposes described in Sections I and II, above.

- **Professional advisors engaged by Company:** Company may disclose the categories of personal information listed in Section I, above, to these services providers or contractors for the business purpose of auditing compliance with policies and applicable laws, in addition to performing services on Company's behalf.
- **Affiliated companies:** Company may disclose any of the categories of personal information listed in Section I, above, to other companies within the Henley family of companies for the business purposes of (a) auditing compliance with policies and applicable laws, (b) helping to ensure security and integrity, (c) debugging, (d) short-term transient use, (e) internal research, and (f) activities to maintain or improve the quality or safety of a service or device.

No Sales or Sharing

Company does not sell or "share" (disclose for cross-context behavioral advertising) your personal information in connection with the HR relationship. In addition, we have no actual knowledge that we sell or share the personal information of individuals of any age in connection with the HR relationship, including the personal information of children under 16.

VI. Your California Privacy Rights

Subject to applicable law, HR Individuals have the following rights:

- **Right to Know**: You have the right to submit a verifiable request up to twice in a 12-month period for specific pieces of your personal information obtained from you and for information about Company's collection, use, and disclosure of your Personal Information. Please note that the CPRA's right to obtain "specific pieces" does not grant a right to the whole of any document that contains Personal Information, but only to discrete items of Personal Information. Moreover, HR Individuals have a right to know categories of sources of Personal Information and categories of external recipients to which Personal Information is disclosed, but not the individual sources or recipients.
- **Right to Delete**: You have the right to submit a verifiable request for the deletion of Personal Information that you have provided to Company.
- **Right to Correct**: You have the right to submit a verifiable request for the correction of inaccurate Personal Information maintained by Company, taking into account the nature of the Personal Information and the purposes of processing the Personal Information.

How to Exercise Your Rights

The Company will respond to requests to know, delete, and correct in accordance with applicable law if it can verify the identity of the individual submitting the request. You can exercise these rights in the following ways:

- Call (833) 204-0493
- Email **privacynotice@vioc.net.**

For certain requests to correct, you can also log into UKG Pro to correct information yourself.

How We Will Verify Your Request

If you submit a request through an adequately secure password-protected account that you created before the date of your request, we will use the authentication mechanisms in the account to verify your identity. Otherwise, we match Personal Information that you provide us against Personal Information we maintain in our files. The more risk entailed by the request (*e.g.*, a request for specific pieces of Personal Information), the more items of Personal Information we may request to verify your identity. If we cannot verify your identity to a sufficient level of certainty to respond securely to your request, we will let you know promptly and explain why we cannot verify your identity.

Authorized Agents

If an authorized agent submits a request to know, correct, or delete on your behalf, the authorized agent must submit with the request a document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you or your authorized agent to follow the applicable process described above for verifying your identity. You can obtain an "Authorized Agent Designation" form by contacting us at privacynotice@vioc.net or (833) 204-0493.

In the alternative, you can provide a power of attorney compliant with the California Probate Code.

Non-Discrimination and Non-Retaliation Policy

We will not discriminate or retaliate against you as a result of your exercise of any of these rights under the California Privacy Rights Act.

Questions and Contact Information

If you have any questions, comments, or concerns about our processing activities or this Notice, please contact us at privacynotice@vioc.net or (833) 204-0493.

VII. Changes to This Notice

We reserve the right to amend this Notice at our discretion at any time. When we make changes to this Notice, we will post the updated notice on UKG and update the Notice's "Last Updated" date. If we materially change this Notice in a way that affects how we use or disclose your Personal Information, we will provide a prominent notice of such changes and the effective date of the changes before making them.

EFFECTIVE DATE: Jan. 1, 2023

LAST UPDATED: April 5, 2025