PINNACLE GROUP
WORKFORCE SOLUTIONS PROVIDER

CPRA PRIVACY POLICY FOR WORK-RELATED INDIVIDUALS

1. PURPOSE AND INTENT

Pinnacle Group and its operating groups, parent(s), subsidiaries and affiliates (collectively, "the Company") are committed to protecting the privacy and security of the personal information of our job applicants, employees and their emergency contacts and beneficiaries, independent contractors, medical personnel, and corporate officers who are residents of California ("Work-Related Individuals"). This privacy policy describes how we collect, use, retain, secure and disclose personal information about you (our "Information Practices"). The Company is responsible for deciding how it collects, uses, retains, secures, and discloses your personal information.

This privacy policy is intended to comply with the California Consumer Privacy Act ("CCPA"), California Privacy Rights Act ("CPRA"), applicable regulations, and other applicable data privacy laws. This Privacy Policy does not form part of any contract of employment or other contract to provide services. We may update this policy at any time.

It is important that you understand this privacy policy, together with any other privacy notices we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. If you have any questions about this privacy policy or how we handle your personal information, please contact us at: privacy@pinnacle1.com.

If you wish to access this privacy policy in an alternate format or require an accommodation to access this privacy policy, you can also contact us at: privacy@pinnacle1.com.

2. DATA PROTECTION PRINCIPLES

We collect, use, retain, and share your personal information in accordance with certain data privacy and data protection principles. Specifically, the personal information we collect about you is: (i) used lawfully, fairly and in a transparent way; (ii) collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes; (iii) reasonably necessary and proportionate to achieve these purposes; (iv) accurate and kept up to date; (v) kept only as long as necessary for these purposes; and (vi) kept securely. If we intend to collect, use, retain, or share your personal information for any purpose that is incompatible with the purposes for which your personal information was collected, we will obtain your consent to do so.

For the purposes of this privacy policy, "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. "Sensitive personal information" is a subcategory of personal information and means personal information that reveals: (a) an individual's social security, driver's license, state identification card, or passport number; (b) an individual's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) an individual's precise geolocation; (d) an individual's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of an individual's mail, email, and text messages unless the Company is the intended recipient of the communication; (f) an individual's genetic data; (g) an individual's biometric information used to uniquely identify the individual; (h) personal information collected and analyzed regarding an individual's health; and (i) personal information collected and analyzed regarding an individual's sex life or sexual orientation.

3. PERSONAL INFORMATION WE COLLECT

Below are the types of personal information we may collect from you and/or about you, and examples of each:

- **Identifying information** (such as full name, alias, gender, date of birth, and signature).
- **Demographic data and protected categories** (such as race, ethnic origin, gender, marital status, disability, veteran or military status, and status as a victim of domestic violence, assault, or stalking).
- **Contact information** (such as postal address, telephone numbers, email address, and emergency contact information).
- **Dependents' information** (such as name, address, date of birth, and Social Security numbers (SSN)).
- **National identifiers** (such as SSN, driver's license number, state identification number, passport and visa information, and other similar identifies are well as immigration status and documentation).
- **Educational and professional background** (such as work history, academic and professional qualifications, educational records, and references).
- **Employment details** (such as job title, position, hire dates, compensation, performance and disciplinary records, and vacation and sick leave records).
- **Financial information** (such as banking details, tax information, payroll information, and withholdings).
- **Health and Safety information** (such as health conditions relevant to your employment, workplace illness and injury information, and health insurance policy information).
- **Information relating to use of Company IT systems** (such as search and browsing history, login information, and IP addresses on the Company's information systems and networks).
- **Geolocation data** (such as time and physical location related to use of an internet website, application, device, or physical access to a Company office location).
- **Testing data** (such as summary about preferences, characteristics, attitudes, intelligence, abilities, and aptitudes).
- **Other information** (such as voluntary information you may provide to Pinnacle in the course of your interactions with us).

4. WHY WE COLLECT PERSONAL INFORMATION AND WITH WHOM IS IT SHARED

Our business purposes for collecting and using your personal information include human resources, employment, benefits administration, health and safety, compliance, and to establish and exercise our legal and contractual rights. Many of these business purposes require that we disclose your personal information internally (e.g. human resource and IT personnel) and to third parties such as clients and service providers (e.g. benefits administrators and insurance companies). We may also share or disclose personal information as required or permitted by law, including sharing with governmental agencies, law enforcement, or other third parties in litigation or legal disputes. We do not, however, "sell" your personal information within the meaning of the CCPA.

For example, the Company collects and uses your personal information as appropriate to:

- Comply with applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.
- Conduct background checks.

- Engage clients for employment opportunities for job applicants and candidates.
- Manage your employment relationship with us, including for:
    - onboarding;
    - timekeeping, payroll, and expense reports;
    - employee benefits;
    - employee training and development;
    - the creation, maintenance, and security of your online employee accounts;
    - reaching your emergency contacts or beneficiaries when needed, such as when you are not reachable or are injured or ill;
    - workers' compensation claims management;
    - employee job performance, including goals and performance reviews, promotions, discipline, and termination; and
    - other human resources purposes.
- Manage and monitor employee access to company facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential violations of Company policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.
- Market our services to clients and prospects.
- Exercise or defend the legal duties or rights of the Company and others, including its employees, affiliates, customers, contractors, service providers, and agents.

5. PRIVACY RIGHTS

As a California resident, you have the following privacy rights regarding your personal information:

- The right to know and right to access the personal information we have collected about you, including the categories of personal information; the categories of sources from which the personal information is collected; the business or commercial purpose for collecting, selling, or sharing personal information; the categories of third parties to whom the business discloses personal information; and the specific pieces of personal information the business has collected about the consumer;
- The right to delete personal information that we have collected from you, subject to certain exceptions;

- The right to correct inaccurate personal information that we maintain about you;
- The right of portability, or right to have us transfer your personal information to other persons or entities upon your request;
- The right to limit the use of your sensitive information if we decide in the future to use such information for purposes other than the purposes listed above; and
- The right not to be discriminated or retaliated against for exercising your of privacy rights.

You can exercise you privacy rights by submitting a request to us by emailing us at: [EMAIL ADDRESS] calling us at: [TOLL-FREE NUMBER]; or asking our Human Resources department for a written request form. To protect the security of your personal information, we will require you to provide us with identifying information for you such as personal email address, personal telephone number, employee identification number, and/or other information that we can match with the personal information we have collected about you to verify your identity.

You may use an authorized agent to request access to or deletion of your personal information. We will require your authorized agent to provide us with either (1) a power of attorney authorizing the authorized agent to act on your behalf or (2) your written authorization permitting the authorized agent to request access to your personal information on your behalf. Further, we will require you or your authorized agent to provide us with identifying information to verify your identity. We may also require you to either verify your own identity directly with us or directly confirm with us that you provided the authorized agent permission to submit the request.

Within 10 days of receiving your request to know, we will confirm receipt of your request and provide information about how we will process your request. Generally, we will respond to your request within 45 days. If we need more time to respond, we will provide you with notice and an explanation of the reason we need more time to respond. We may deny your request if we cannot verify your identity or are legally permitted to deny your request. If we deny your request, we will explain the basis for the denial, provide or delete any personal information that is not subject to the denial, and refrain from using the personal information retained for any purpose other than permitted by the denial. We will maintain a record of your request and our response for 24 months.

6. DATA SECURITY

While no data security system can fully protect personal information from unauthorized data breaches, The Company has implemented reasonable safeguards and controls, consistent with its legal obligations under California and other local, state and federal laws. The Company is committed to: (i) seeking to safeguard all personal information that you provide to us; (ii) seeking to ensure that it remains confidential and secure; and (iii) taking all reasonable steps to ensure that personal privacy is respected. All our data is stored in written or electronic form on our servers and computers and in various physical locations. We maintain physical, electronic and procedural safeguards to protect your personal information from misuse, unauthorized access or disclosure and loss or corruption by computer viruses and other sources of harm. We restrict access to personal information to those staff members of the Company and our services providers who need to know that information for the purposes identified in our privacy policy and privacy notices.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

7. DATA RETENTION

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements. Generally, we retain personal information for the duration of our relationship with you plus any legally required record or data retention period and/or any period of time necessary to exercise our legal rights. Thereafter, we will securely destroy your personal information in accordance with the Company's record retention policies.

In some circumstances we may anonymize your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

8. PERSONAL INFORMATION OF MINORS

The Company does not sell or share personal information for individuals under the age of 16.

9. CHANGES TO THIS PRIVACY POLICY

As we strive to improve our practices, we may revise the Company's privacy policy from time to time. This privacy policy is not a contract and we reserve the right to change this policy at any time and to notify you of those changes by posting an updated version of this policy. It is your responsibility to check this policy from time to time for any changes.

This privacy policy was last updated on December 29, 2022.

10. QUESTION SAND FURTHER INFORMATION

If you have any questions or would like further information regarding this privacy policy or our privacy practices, please contact us at: privacy@pinnacle1.com.