PRIVACY POLICY AND NOTICE TO APPLICANTS/EMPLOYEES IN CALIFORNIA

BENESYS, INC.

This applicant/employee Privacy Policy is applicable to BeneSys, Inc. (hereinafter, "Company", "we, "our", or "us") and those individuals residing in the State of California who apply for employment and those who are currently employed by us at one of our California office locations.

Please take notice that the Company collects certain information about you. For more information on the Company's policies, please refer to the Company's privacy policy in our employee handbook:

California's California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA") provide California applicants and employees with certain rights, including the following:

- Knowledge of information collected;
- Deletion of information collected;
- Opt-out of us sharing information collected;
- Opt-in of information collected;
- Correction of information collected;
- Limit use of information collected;
- Not to be discriminated or retaliated against for exercising rights under the law.

Where We Get Your Information. The Company collects information about you from the following sources: 1) you; 2) prior employers, references, recruiters, job-related social media platforms; 3) third-party sources of demographic information; 4) third-party companies, such as background check companies; and 5) claim administrators and investigators. Depending on the Company's interactions with you, we may or may not collect all of the information identified about you.

The Personal and Sensitive Personal Information ("SPI") That We Are Collecting. We are collecting the following information:

- Identifiers, such as name, government-issued identifier (e.g., Social Security number), and unique identifiers (e.g., employee ID);
- Personal information, such as real name, signature, SSN, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, passport number, federal identification authorizing work in the United States, access and/or passcodes, insurance policy number, education, employment, employment history, bank account number, other financial information, medical information, or health insurance information;
- Characteristics of protected classifications under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language,

immigration status, military/veteran status, disability, request for leave, and medical conditions;
- Commercial information, such as transaction information and purchase history (e.g., in connection with employee business travel or other reimbursements [or purchases from Company]);
- Internet or network activity information, such as browsing history and interactions with our online systems and websites and any personal information that you provide while accessing the Company's computer systems, such as personal credit card information and passwords;
- Geolocation data, such as device location from usage of the Company's devices such as Company-issued cell phones, computers, and/or tablets;
- Audio, electronic, visual, and similar information;
- Professional or employment-related information, such as work history and prior employer;
- Non-public education information; and
- Inferences drawn from any of the Personal and SPI listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

How Your Personal and Sensitive Personal Information is Used. We may use Personal and Sensitive Personal Information in the following manner:

- To operate, manage, and maintain our business;
- For hiring, retention, and employment purposes;
- To otherwise accomplish our business purposes and objectives, including, for example:
    - Emergency services;
    - Conducting research, analytics, and data analysis;
    - Maintaining our facilities and infrastructure;
    - Quality and safety assurance measures;
    - Conducting risk and security controls and monitoring;
    - Protecting confidential and trade secret information;
    - Detecting and preventing fraud;
    - Performing identity verification;
    - Performing accounting, audit, and other internal functions, such as internal investigations;
    - Complying with the law, legal process, and internal policies;
        - Maintaining records;
        - Claims processing;
        - Responding to legal requests for information and subpoenas; and
        - Exercising and defending legal claims.
- Any other purposes authorized by the California Privacy Protection Agency, California or Federal law.

We may or may not have used Personal and Sensitive Personal Information about you for each of the above purposes.

Sharing of Personal Information. We share your information with the following third-party entities:

- Paycor for payroll and benefits purposes
- Voya Financial for those employees enrolled in the Company's 401(k) program.
- Benefits providers, such as health, vision, and dental insurance carriers, with whom we contract to provide healthcare benefits to you.

Selling of Personal Information. The Company does NOT sell your personal information.

Data Retention. The Company retains the information it receives about you for a period of five (5) years, unless a shorter or longer period is required by California or Federal law, rule, or regulation.

For Inquiries and/or to Submit Requests for Information, Deletion or Correction. Please contact either: (1) corporate.compliance@benesys.com , or (2) (888) 659-8789 for inquiries about the Company's policy, or to submit your requests for information, deletion, or correction.