BBSI PRIVACY NOTICE TO CALIFORNIA EMPLOYEES

(herein referred to as "Consumers")

Barrett Business Services, Inc. ("**BBSI**," the "**Company**" or "**we**") provide this California Privacy Notice ("**Notice**") to describe our privacy practices with respect to our collection of Personal Information as required under the California Consumer Privacy Act ("**CCPA**"). This Notice applies only to BBSI employees who are residents of the State of California ("**Consumers**" or "**you**")[1] and from whom we collect "**Personal Information**" as defined in the CCPA and in this Notice. We provide you this Notice because under the CCPA, California residents who are employees qualify as Consumers.

1. Information We Collect From or About Consumers

We may collect Personal Information from or about you in a variety of different situations and using a variety of different methods, including, but not limited to, on our website, your mobile device, through email, in physical locations, through written applications, through the mail, and/or over the telephone. Generally, we may at various times throughout your employment with the Company collect, receive, maintain, and use the following categories of Personal Information for any of the purposes listed below in this Notice and to the extent permitted under applicable law:

CATEGORY	EXAMPLES
Personal Identifiers	Name, alias, social security number, date of birth, driver's license or state identification card number, passport number, employee ID number.
Contact Information	Home, postal or mailing address, email address, home phone number, cell phone number.
Account Information	Username and password for Company accounts and systems, and any required security or access code, password, or credentials allowing access to your Company accounts.
Protected Classifications	Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, physical or mental disability, medical condition, veteran or military status, familial status, language, or union membership.
Physical Characteristics or Description	Information on your driver's license (such as eye color, hair color, height, weight), as well as information collected to the extent relevant for workplace investigations or for enforcement of Company policies on appearance and grooming (such as tattoos, piercings).
Biometric Information	Fingerprints, retina scans, facial recognition, handprint.
Financial Information	Bank account number for direct deposit, credit card number, debit card number, or other financial account information.

[1] The use of the term Consumer in this document does not mean that Employees are consumers for purposes of any other law besides the CCPA.

Pre-Hire Information	Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, information recorded in job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, voluntary disclosures by you, and Wage Opportunity Tax Credit (WOTC) information.
Employment History	Information regarding prior job experience, positions held, and, when permitted by applicable law, your salary history or expectations.
Education Information	Information contained in your resume regarding educational history, information in transcripts or records of degrees, and vocational certifications obtained.
Professional or Employment-Related Information	Information contained in your personnel file and in other employment documents and records, including information in new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury and safety records, performance evaluations, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, pension, retirement and 401(k) records, COBRA notifications, business expense records, and payroll records.
Travel Information	Information regarding business travel, vacation and personal travel plans, and for infectious disease contact tracing purposes the locations travelled to within the applicable infectious period prior to coming to the workplace and the dates spent in those locations.
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 related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.
Information of Friends, Co-workers, and Other Associates with Whom You Have Been in Close Contact within the COVID-19 infectious period per applicable guidelines	Medical and health information provided to the Company for an employee's friends, co-workers, and other associates related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.
Medical and Health Information	Medical information contained in such documents as doctor's notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, ergonomic assessments and accommodation records, and correspondence with you and your medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as information in

	post-hire drug test results, and information related to COVID-19 symptoms, exposure, contact tracing, diagnosis, testing, or vaccination. This includes medical information and health benefits information for dependents and beneficiaries.
Internet, Network, and Computer Activity	Internet or other electronic network activity information related to usage of Company networks, servers, intranet, shared drives, or Company-issued computers and electronic devices, including system and file access logs, security clearance level, browsing history, search history, and usage history.
Mobile Device Security Information	Data identifying employee devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.
Online Portal and Mobile App Access and Usage Information	Username and password, account history, usage history, file access logs, and security clearance level.
Geolocation Data	IP address and/or GPS location (latitude & longitude) recorded on Company-issued computers, electronic devices, and vehicles, as well as in timekeeping applications on cell phones that employees use to clock in and out and that log the geographic location at which each time entry was made.
Visual, Audio or Video Recordings in the Workplace	Your image when recorded or captured in surveillance camera footage or pictures of employees taken in the workplace or at a Company function or event, or in pictures or video of employees posted on social media to which the Company or its managers have access or that are submitted to the Company by another employee or third party.
Facility & Systems Access Information	Information identifying which employees accessed secure Company facilities, systems, networks, computers, and equipment and at what times using their keys, badges, fobs, login credentials, or other security access method.
Inferences	Based on analysis of the personal information collected, we may develop inferences regarding Employees' preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes for purposes of employment and management decisions related to staffing, assignments, responsibilities, team composition, hiring, promotion, demotion, and termination, among other things.
Contents of Personal Communications where the Company is not the intended recipient	If you use Company email, phones, computers, online chat applications (Slack, Teams, Zoom, etc.) or other Company systems for personal communications where the Company is not the intended recipient of the communication, the Company retains these communications in the ordinary course of managing its communication and computer systems and pursuant to the Company's data retention policy. Employees have no expectation of privacy with respect to any communications or data they send, receive, access or store on any company computer or system, including any personal communications. The Company may monitor, access, review and use all such communications and data for lawful business purposes detailed below, including to manage and evaluate employee performance and make employment decisions.

Of the above categories of Personal Information, the following are categories of "**Sensitive Personal Information**" the Company may collect:

1. Personal Identifiers (social security number, driver's license or state identification card number, passport number).
2. Account Information (your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account).
3. Protected Classifications (including, but not limited to, racial or ethnic origin, religious or philosophical beliefs, union membership, or sexual orientation).
4. Biometric Information (used for the purpose of uniquely identifying you).
5. Medical and Health Information.
6. Geolocation Data (IP address and/or GPS location, latitude & longitude).
7. Contents of Personal Communications (contents of mail, email, and text messages where the Company is not the intended recipient).

Personal information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the employee or from widely distributed media.
- Information made available by a person to whom the employee has disclosed the information if the employee has not restricted the information to a specific audience.
- De-identified or aggregated information.

2. How We Use Personal Information and Sensitive Personal Information

The Personal Information and Sensitive Personal Information we collect, and our use of Personal Information and Sensitive Personal Information, may vary depending on the circumstances. This Notice is intended to provide an overall description of our collection and use of Personal Information and Sensitive Personal Information. Generally, we may use or disclose Personal Information and Sensitive Personal Information we collect from you or about you for one or more of the following purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to become an employee, we will use that Personal Information in connection with your employment.
2. To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
3. To manage and process payroll and/or Company travel and expenses.
4. To validate an employee's identity for payroll and timekeeping purposes.
5. To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
6. To manage workers' compensation claims.
7. To administer, manage, and maintain group health insurance benefits, 401K and/or retirement plans, and other Company benefits and perks.
8. To manage employee performance of their job duties and/or employee conduct, including by engaging in lawful monitoring of employee activities and communications when they are on duty, on Company

premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.

9. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
10. To evaluate job applicants and candidates for employment or promotions.
11. To obtain and verify background checks on job applicants and employees and to verify employment references.
12. To evaluate, make, and communicate decisions regarding an employee's employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline.
13. To communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
14. To grant employees access to secure Company facilities and maintain information on who accessed the facility.
15. To track employee movement and activity throughout Company facilities and keep the facilities secure.
16. To implement, monitor, and manage electronic security measures on Company internet and WiFi connections, computers, networks, devices, software applications or systems, as well as on employee devices that are used to access Company internet and WiFi connections, computers, networks, devices, software applications or systems.
17. To engage in corporate transactions requiring review or disclosure of employee records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
18. To communicate with an employee's family or other contacts in case of emergency or other necessary circumstance.
19. To manage employee recognition programs.
20. To promote and foster diversity, equity, and inclusion in the workplace.
21. To provide services to corporate customers who may request certain pieces of information about a Company employee (such as name, phone number, and headshot) to permit the employee access or security clearance to their facility in advance of the Company employee being dispatched to provide services at the customer's facility.
22. **COVID-19 RELATED PURPOSES**
    a. To reduce the risk of spreading the disease in or through the workplace.
    b. To protect employees and other consumers from exposure to COVID-19.
    c. To comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19, including applicable reporting requirements.
    d. To facilitate and coordinate pandemic-related initiatives and activities (whether Company-sponsored or through the U.S. Center for Disease Control and Prevention, other federal, state and local governmental authorities, and/or public and private entities or establishments, including vaccination initiatives).
    e. To identify potential symptoms linked to COVID-19 (including through temperature checks, antibody testing, or COVID-19 questionnaire).
    f. To permit contact tracing relating to any potential exposure.
    g. To communicate with employees and other consumers regarding potential exposure to COVID-19 and properly warn others who have had close contact with an infected or symptomatic individual so that they may take precautionary measures, help prevent further spread of the virus, and obtain treatment, if necessary.
23. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company.
24. To manage your employment relationship with us, including but not limited to, for onboarding, performance, and human resource services.

25. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
26. To detect security incidents involving potentially unauthorized access to and/or disclosure of Personal Information or other confidential information, including proprietary or trade secret information and third-party information that the Company receives under conditions of confidentiality or subject to privacy rights.
27. To protect against malicious or illegal activity and prosecute those responsible.
28. To prevent identity theft.
29. To verify and respond to consumer requests under applicable consumer privacy laws.

3. Retention of Personal Information

The Company will determine the length of retention for each category of Personal Information in accordance with various criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

4. Sale/Sharing of Information to Third Parties

The Company does **not** and will not sell your Personal Information or Sensitive Personal Information for any monetary or other valuable consideration. The Company does **not** and will not share your Personal Information or Sensitive Personal Information for cross-context behavioral advertising.

5. Access to Privacy Policy

For more information, please review the Company's Privacy Policy on BBSI's intranet Community, under its Policies and Procedures page.

By signing below, I acknowledge and confirm that I have received and read and understand this disclosure and I hereby authorize and consent to the Company's use of the personal information and sensitive personal information it collects, receives or maintains for the business purposes identified above.

_____ _____

Employee's Signature Date

_____

Print Your Full Name