EMPLOYEE PRIVACY POLICY

A.J. Kirkwood & Associates (the "**Company**" or "**we**") has developed this Privacy Policy out of respect for the privacy of our employees. This Policy describes the personal information we collect, both online and offline, and that we use and disclose about employees who are employed with us. We will collect some information from you for employment purposes.

Collection of Personal Information

In the last 12 months, we have collected the following categories of personal information from or about employees, including information about employees' family members, dependents, and beneficiaries. For each category of information, the categories of third parties to whom we have disclosed or shared the information within the last 12 months are referenced by a letter that coincides with the letter in the list of categories of service providers and third parties that follows soon after this table.

Category	Examples	Disclosed in Last 12 Months to	Retention Period
Personal Identifiers	Name, alias, social security number, date of birth, driver's license or state identification card number, passport number, employee ID number.	A, B, C, D, E, F, G, H, I	Duration of Employment plus 5 years
Contact Information	Home, postal or mailing address, email address, home phone number, cell phone number.	A, B, C, D, E, F, G, H, I	Permanent
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.	Not Disclosed	3 Years
Protected Classifications	Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, disability, medical or mental condition, military status, familial status, language.	B, C, D	3 Years
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).	B, C, D	Duration of Employment plus 5 years

Category	Examples	Disclosed in Last 12 Months to	Retention Period
Financial Information	Bank account number for direct deposit, credit card number, debit card number, or other financial account information.	A, B, F	Duration of Employment plus 5 years
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, 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.	A, B, D, E	Duration of Employment plus 5 years
Employment History	Information regarding prior job experience, positions held, names of prior supervisors, and when permitted by applicable law your salary history or expectations.	B, D, E	Duration of Employment plus 5 years
Education Information	Information from resumes regarding educational history; information obtained from transcripts or records of degrees and vocational certifications obtained.	B, D, E	Duration of Employment plus 5 years
Professional or Employment-Related Information	Information contained in your personnel file and in other employment documents and records, including information contained in the following types of records: new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury records, safety records, performance evaluations and records, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, COBRA notifications, business expense records, and payroll records.	A, B, C, D, E, F, G	Duration of employment plus 5 years, unless related to hazardous exposure records required by OSHA to be retained for at least 30 years.
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.	B, D, E	Duration of Employment plus 5 years
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	B, D, E	Duration of Employment plus 5 years

Category	Examples	Disclosed in Last 12 Months to	Retention Period
	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.	B, D, E	Duration of Employment plus 5 years
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 assessment 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.	B, D, E	Duration of employment plus 5 years, unless related to hazardous exposure records required by OSHA to be retained for at least 30 years.
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	B, E, G	3 Years
Mobile Device Security Information	Data identifying employee's devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider	B, D, E, G	3 Years
Online Portal and Mobile App	Username and password, account history, usage history, file access logs, and security clearance level.	B, D, E, G	3 Years

Category	Examples	Disclosed in Last 12 Months to	Retention Period
Access and Usage Information			
Geolocation Data	IP address and/or GPS location (latitude & longitude) recorded on Company-issued computers, electronic devices, and vehicles, as well as 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	B, D, E, G	3 Years
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.	B, D, E, H, I	Surveillance footage: 90 days. Otherwise, duration of employment plus 5 years.
Facility & Systems Access Records	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.	B, D, E	3 Years
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.	Not Disclosed	Email accounts are retained for at least 3 years, unless related to a category of data identified above that requires a longer retention period

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect from or about employees:

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 (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.

We may collect your personal information from the following sources:

- You, the employee, when you voluntarily submit information for employment purposes
- Company-issued computers, electronic devices, and vehicles
- Company systems, networks, software applications, and databases you log into or use in the course of performing your job, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Surveillance cameras at our physical locations
- Credit and consumer reporting agencies
- Drug testing and physical testing providers and vendors
- HR support vendors, including administrators of benefits, workers' compensation, unemployment claims, payroll, timekeeping, expense management
- Social media platforms
- Recruiters
- Staffing agencies
- Personal references and former employers
- Our other employees, contractors, vendors, suppliers, guests, visitors, and customers based on your interactions with them

We may disclose your personal information to the following categories of service providers or third parties:

A. Financial Institutions
B. Government Agencies
C. Benefits Administrators, including workers' compensation and unemployment administrators or vendors
D. Employee Tracking and Talent Management Systems
E. Payroll Processors
F. Communications Providers
G. Social Media Platforms
H. Our Corporate Customers

By referring to the letter corresponding to the category, the above table specifies to what categories of service providers and third parties we disclose personal information.

We may collect and use your personal information for the following business 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 anyone who interacts with our employees 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 others who interacted with our employees 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 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.
25. 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.
26. To protect against malicious or illegal activity and prosecute those responsible.
27. To prevent identity theft.
28. To verify and respond to consumer requests under applicable consumer privacy laws.

We may disclose your personal information for the following business purposes as numbered above:
1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18, 21, 22(c), 22(f) and 22(g).

We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

Other than these exceptions, we do not and will not disclose your personal information to any third party in exchange for monetary or other valuable consideration.

We do NOT and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services reasonably expected by an average employee who requests those services.
2. To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
4. To ensure the physical safety of natural persons.
5. For short-term, transient use.
6. To perform services on behalf of the Company.
7. To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.

Retention of Personal Information

We will retain each category of personal information in accordance with our data retention schedule, listed above. In deciding how long to retain each category of personal information that we collect, we consider many 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.

Third-Party Vendors

We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail and payroll services. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose.

Business Transfers

In the event we sell or transfer a particular portion of our business assets, employee information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, employee information may be transferred as part of the acquisition.

Compliance With Law and Safety

We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Passwords

The personal data record created through your registration for your employee email account and timekeeping and payroll system applications can only be accessed with the unique password associated with those records. To protect the integrity of the information contained in those records, you should not disclose or otherwise reveal your passwords to third parties.

Employees and Their Family Members, Dependents, and Beneficiaries Under the Age of 16

We do not knowingly share the personal information of employees or any of their family members, dependents or beneficiaries under 16 years of age.

How We Protect the Information That We Collect

The protection of the information that we collect about employees is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.

Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents who are natural persons; it does not apply to any entities (whether business, non-profit or governmental). If you are a California resident, you have the following rights:

1. Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected, shared or sold about you, (2) the categories of sources from which the personal information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your personal information;
2. Right to Access. The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you;
3. Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete personal information that we have collected from you, subject to certain exceptions;
4. Right to Correct. The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;
5. Right to Opt-Out. The right to opt-out of the sharing of your personal information to third parties;
6. Right to Limit. The right to limit the use or disclosure of your sensitive personal information;
7. The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and
8. The right to not be discriminated or retaliated against for exercising any of the above rights.

You Can Submit Any of the Above Types of Requests at the link below Below:

1. Submit an online request on our website at mailto://hrbenefits@ajka.freshservice.com .

How We Will Verify That it is Really You Submitting the Request:

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us. For example, we may need you to provide your name, address, email, phone number, last 4 digits of your social security number, and your date of birth.

Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

Responding to Your Request to Opt-Out of the Sharing of Your Personal Information

We will act upon a verifiable request to opt-out within fifteen (15) business days of its receipt. We will notify all third parties to whom we have shared personal information of your request and instruct them to comply with the request within the same time frame. We will notify you when this has been completed by mail or electronically, at your option.

A request to opt-out need not be a verifiable request. However, we may deny a request to opt-out if we have a good faith, reasonable, and documented belief that a request to opt-out is fraudulent. If we deny your request to opt-out, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide

written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Consent to Terms and Conditions

By entering into an employment relationship with A.J. Kirkwood and Associates, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy

As our services evolve and we perceive the need or desirability of using personal information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check the https://ajk.bamboohr.com/files/ frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Policy, we will post the revised Policy and the revised effective date at https://ajk.bamboohr.com/files/ Please check back here periodically or contact us at the address listed at the end of this Policy.

Individuals With Disabilities

This Policy is in a form that is or will be made accessible to individuals with disabilities.

Questions About the Policy

If you have any questions about this Privacy Policy, please contact us at mailto://hrbenefits@ajka.freshservice.com