Privacy Notice for California Job Candidates and Employees

The purpose of this Privacy Notice (“Notice”) is to inform individuals who inquire about and/or apply for employment with Fluid Components International LLC ("FCI", “Company”, "we" or "us") and our employees of the categories of Personal Information that we may receive and how we use it for employment, human resources, benefits administration, health and safety, and business-related purposes. The Notice is intended to comply with applicable laws including the California Consumer Privacy Act of 2018, as amended from time to time, including by the California Privacy Rights Act of 2020 and its implementing regulations (collectively, “CCPA”). The Notice applies solely to residents of California who are natural persons and are a job candidate, employee, independent contractor, emergency contact or beneficiary of an employee (“you”). Any terms defined in the CCPA have the same meaning when used in this Policy. These disclosures do not reflect our collection, use, or disclosure of California residents’ Personal Information where an exception or exemption under the CCPA applies. If any provision below conflicts with a legal requirement, FCI will comply with the applicable laws.

Information We Collect

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular job candidate or employee ("Personal Information").

Below are the categories of Personal Information we collect:

Identifying and contact information such as your full name, date of birth, signature, postal address, telephone numbers, email address, emergency contact information, account credentials, social security number, driver’s license number, state identification card number, passport and visa information and immigration status and documentation, passwords, and insurance information.

Demographic data (protected classifications) such as race, ethnic origin, marital status, medical condition, physical or mental disability, gender, age, religion or creed, citizenship status, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, and veteran or military status.

Dependents, beneficiaries, or other individual's information such as their full name, address, date of birth, and social security numbers.

Educational and professional background such as your resume or CV, cover letters, current or past work history, academic and professional qualifications, educational records, information from references, driving history and records, professional licenses,

background checks and criminal history (to the extent permitted by applicable laws), interview notes, and other related documentation as part of your job application.

Employment details such as your job title, position, hire and termination dates, compensation (to the extent permitted by applicable laws), performance and disciplinary records, vacation and sick leave records, insurance, beneficiary information and choices, information from expense reports, and independent contractor agreements.

Financial information such as banking details, tax information, payroll information, and withholdings.

Health and Safety information such as health conditions (if relevant to your employment), job restrictions, workplace illness and injury information, and health insurance policy information.

Information Systems, internet or other electronic activity information such as your search history, browsing history, login information and other security information, and IP addresses on the Company's information systems and networks, computer use, use of email, Company-owned cell phones and other devices.

Biometric information such as fingerprints, facial photos, voice data, and other biological characteristics.

Geolocation data such as time and physical location related to use of Company systems, internet websites, applications, devices, or physical access to a Company office location.

Sensory or surveillance information such as call monitoring and video, audio, or other forms of monitoring or surveillance, badge swipes at offices, and device tracking.

Inferences to create a profile about you reflecting your characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

Sources of Personal Information

We obtain the categories of Personal Information listed above from the following categories of sources:

Directly from you, for example, when you contact us or submit a job application or from forms or assessments you complete that we or our third-party service providers provide.

Indirectly from you (passively and from third parties), for example, this might include from emails we send you and you send us, from open source information on our website or other websites, or from references, prior employers, your healthcare

provider, your legal or financial advisors or your bank.

Use of Personal Information

We may use or disclose the Personal Information we collect for one or more of the following purposes:

Perform the services or provide the goods reasonably expected by you in your role, including those services and goods that are reasonably necessary for us to administer the job application process and for our employees to perform their duties.

Communicate with you regarding your job application or our employment relationship.

Recruit and evaluate job candidates for employment.

Determine the need to provide you with appropriate adjustments or accommodations during the recruitment process or employment.

Conduct background checks.

Check and provide references.

In limited circumstances, for example, for some managerial roles, draw inferences about you from Personal Information, other than Sensitive Personal Information) collected in your responses to candidate screening questionnaires and assessments from third party service providers to determine your suitability for employment for the role for which you are a job candidate, or being considered for promotion.

Determine your eligibility to work in a jurisdiction.

Administer the onboarding and separation processes.

Maintaining your contact information and reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill.

Creation, maintenance, and security of your online employee accounts and data, including creating an account in an applicant tracking system.

Timekeeping, payroll, and expense report administration.

Employee benefits and loans administration.

Employee training and development requirements including work related licenses and credentials, and ensuring compliance, training, examination and other requirements of applicable regulatory bodies and customers are met, administering ethics, compliance and other employee training, and conducting talent management and career

development.

Employee claims and workers' compensation claims management.

Employee job performance including for goals and performance reviews, promotions, bonuses, discipline, investigations, and termination.

Administration of other support services such as leave requests, approvals and authorization procedures, and travel.

Conduct internal audits and workplace investigations.

Detect, investigate and enforce compliance with, and potential breaches of, Company policies and procedures or activities that may be fraudulent or illegal.

Provide healthcare-related services such as administering pre-employment and employment-related medical screenings for return to work processes and medical case management, determining medical suitability for particular tasks, and identifying health needs to plan and provide appropriate services.

Facilitate a better working environment, such as conducting staff surveys, providing senior management information about employees, conducting training, and sharing picture books.

Producing and maintaining corporate organization charts, entity and team management, and carrying out workforce analyses, benchmarking, and succession planning.

Manage and monitor employee access to, and use of, company facilities, equipment, and systems such as computers, cell phones, other devices, and email.

Protect and secure Company assets, networks, business operations, and the rights or safety of our employees, customers and other individuals such as using multi-factor authentication, hosting and maintaining computer systems and infrastructure, managing software and hardware computer assets, systems testing, monitoring email and Internet access, and training.

Monitor and ensure compliance with applicable laws and regulations and internal company reporting obligations such as headcount, management information, demographic, and health, safety, security and environmental reporting, administration of and reporting relating to items shown on your paycheck (for example, income, benefits, deductions).

Comply with corporate financial responsibilities, including audit requirements (both internal and external), accounting, and cost/budgeting analysis and control.

Exercise or defend legal rights of the Company, its employees, customers, contractors,

and others before any jurisdictional and/or administrative authority, arbitration, or mediation panel.

Cooperating with or informing law enforcement or regulatory authorities to the extent required by applicable laws including responding to and complying with requests and legal demands from regulators or other authorities in or outside of your home country.

Maintain commercial insurance policies and coverage including for workers' compensation, liability, and other insurance coverage.

Communicate with you, other employees, and third parties such as existing or potential business partners, suppliers, customers, end-customers or government officials.

Use in customer marketing, for example, articles in publications and contact information in brochures.

Engage in corporate transactions requiring review of employee records such as for evaluating potential mergers and acquisitions of or by the Company.

When the reason for disclosure aligns with the reason the information was collected in the first place, for example, if information was collected to hire and evaluate a job candidate, it can be used to determine if the employee should later be promoted or not.

We will not collect additional categories of Personal Information or use the Personal Information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We do not “sell” or “share” any of the above categories of Personal Information or Sensitive Personal Information for cross-context behavioral advertising.

We do not use or disclose Sensitive Personal Information for purposes other than those permitted by applicable laws, including Section 7027(m) of the CCPA, or for inferring characteristics, though we do use non-Sensitive Personal Information to infer characteristics in limited cases as described above.

We may share your Personal Information by disclosing it to our related entities or to a third party for a business purpose. For example, we may share your Personal Information with vendors who perform job search activities for us, or host our job candidate tracking system, our payroll and human resources systems, time clocks, cybersecurity, or marketing email programs, or who assist us in providing other technology or user assistance. We make these third party business purpose disclosures under written contracts that describe the purposes, require the recipient to keep the Personal Information confidential, and prohibit using the disclosed information for any purpose except performing the contract. We also share Personal Information with

regulatory or law enforcement agencies or others to comply with applicable laws, regulations, subpoenas, and court orders.

Your Rights and Choices

The CCPA provides you with specific rights regarding your Personal Information. This section describes your CCPA rights and explains how to exercise those rights.

Right to know/disclose: You have the right to request that we disclose certain information to you about our collection and use of your Personal Information over the past twelve months, such as (i) the categories of Personal Information we collected about you; (ii) the categories of sources from which we collected such data; (iii) the specific pieces of Personal Information we collected about you; (iv) the purpose for collecting or sharing Personal Information about you; (v) the categories of Personal Information about you that we sold or disclosed to third parties; and (vi) the categories of third parties with whom we shared or to whom we shared your Personal Information, subject to legal restrictions.

Right to delete: You have the right to request that we delete your Personal Information, subject to legal restrictions.

Right to correct: You have the right to request we correct any inaccurate Personal Information about you, subject to legal restrictions. If any Personal Information requires correction, we will use commercially reasonable efforts to fulfill your correction request.

Right not to discriminate: You have the right not to be discriminated against for exercising these rights.

Only you, or someone legally authorized to act on your behalf, may make a request to know, delete, correct, or limit your Personal Information.

You may only submit a request twice within a 12-month period.

Your request must (a) provide sufficient information that allows us to reasonably verify you are the person, or an authorized representative of the person about whom we collected the Personal Information, and (b) describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We will pass your verified and non-exempt requests to service providers and, unless it impossible or involves a disproportionate effort, to all third parties to whom we sold or shared the information.

We cannot respond to your request if we cannot reasonably verify your identity or authority to make the request and confirm that the Personal Information relates to you.

We will only use Personal Information provided in a request to verify the requestor's

identity or authority to make it.

To exercise these rights, send us your verifiable request using the “Contact” section below.

Response Timing and Format

We will respond to your request consistent with applicable laws (certain data is excluded) within 45 calendar days of the request, though we may extend this 45 days for another 45 days where reasonably necessary. We will notify you prior to expiration of the first 45 day period of any extension. Subject to legal restrictions, requests to limit the use or disclosure of your Sensitive Personal Information for the purpose of inferring characteristics will be complied with, and the request forwarded to third party service providers with whom we have disclosed or made available your Sensitive Personal Information, within 15 business days after receipt of a properly submitted request.

If applicable, our response will explain the reasons we cannot comply with a request. For data portability requests, we will select a format to provide your Personal Information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your 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.

Data Storage and Security, Retention Period

We may store your Personal Information in the U.S. or in other countries. Except as otherwise permitted or required by applicable laws, we retain your Personal Information only for as long as necessary to fulfill the purposes for which it was collected. 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 unauthorized use of processing by other means, the business purpose for which it is obtained, compliance with applicable laws, the exercise or defense of legal rights, and archiving, back-up and deletion processes.

We maintain reasonable administrative, technical, and physical safeguards to protect your data from accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use. Our service providers are also required to adhere to reasonable security practices to further ensure the safety of your data. That being said, digital transmission and storage of data is not completely secure and we cannot guarantee the safety of your data.

Changes to Our Notice

We reserve the right to amend this Notice at our discretion and at any time. When we make changes to this Notice, we will post the updated policy on the respective website and other places we may make it available and update the Notice's effective date.

Contact Us

If you have any questions or comments about this Notice, the ways in which FCI collects and uses your Personal Information described here, your choices and rights regarding such use, if you wish to exercise your rights under California law, or if you need access to it in an alternative format due to having a disability, please submit a request by:

Calling us at 760-744-6950

Emailing us at legal@fluidcomponents.com or

Mailing us at Fluid Components International LLC, ATTN: Privacy Team, 1755 La Costa Meadows Drive, San Marcos, CA 92078.