**One Capital Management, LLC**
**CA Personnel Policy**
**April 2025**

ONECAPITAL MANAGEMENT, LLC

## CA Personnel Policy

This California Personnel Policy ("Personnel Policy") applies to the employees, former employees, independent contractors and job applicants (including, in each case, individuals associated with their personnel records (e.g., beneficiaries and dependents)) of One Capital Management, LLC and its affiliates (individually and collectively "OCM", "we", "us" or "our") who are residents of California (collectively, "California Personnel", "you" or "your").

This Personnel Policy is designed to meet our obligations under the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), and sets forth our policies for the collection, use, storage, sharing, disclosure and protection of personal information of California Personnel, as required for all California employers. If any OCM policy, statement or notice and this Personnel Policy conflict, then this Personnel Policy will prevail as to California Personnel, unless stated otherwise.

This Personnel Policy does not apply to personal information that OCM collects from or about clients, business partners or any non-California Personnel.

Under the CPRA, personal information includes information that identifies and describes who you are, as well as information that relates to or is capable of being associated with, or could reasonably be linked to you, one of your devices, and/or a member of your household. In this Personnel Policy, we refer to the information subject to the CPRA as "Employee Personal Information."

You have the right to receive information on OCM's privacy practices, including why we collect Employee Personal Information, from whom it is collected, and for what purpose.

OCM collects and uses Employee Personal Information for human resources, employment, benefits administration, health and safety, and business-related purposes and to be in compliance with applicable statutes and regulations. Below are the categories of Employee Personal Information we collect and the purposes for which we intend to use this information.

OCM MAY COLLECT THE INFORMATION BELOW:

- Identifying information, such as your full name, gender, date of birth, and signature.
- Demographic data, such as race, ethnic origin, marital status, sexual orientation, disability, and veteran or military status.
- Contact information, such as your home address, telephone numbers, email addresses, and emergency contact information.
- Dependent's or other individual's information, such as their full name, address, date of birth, and Social Security numbers (" SSN" ).
- National identifiers, such as SSN, passport and visa information, and immigration status and documentation.
- Educational and professional backgrounds, such as your work history, academic and professional qualifications, educational records, references, and interview notes.
- Employment details, such as your job title or position, hire dates, compensation, performance, 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 (if relevant to your employment), job restrictions, workplace illness, injury information, and health insurance policy information.
- Information Systems (IS) information, such as your login credentials and information, search history, browsing history, and IP addresses on our information systems and networks.
- Biometric information, such as facial recognition, fingerprints, iris or retina scans, keystrokes, or other physical patterns.
- Geolocation data, such as time and physical location related to the use of an internet website, application, device, or physical access to an OCM office and/or branch office location.
- Sensory or surveillance information, such as COVID-19-related temperature checks and call monitoring and video surveillance.
- Profile or summary about an applicant or employee's preferences, characteristics, attitudes, intelligence, abilities, and aptitudes.

OCM COLLECTS EMPLOYEE PERSONAL INFORMATION TO USE OR DISCLOSE AS APPROPRIATE TO:

- Comply with all applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.
- Conduct background checks.
- Manage your employment relationship with us, including for:
    - onboarding processes.
    - timekeeping, payroll, and expense report administration.
    - employee benefits administration.
    - employee training and development requirements.
    - the creation, maintenance, and security of your online employee accounts.

## CA Personnel Policy

- reaching your emergency contacts 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 OCM facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of OCM policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of OCM.
- Maintain commercial insurance policies and coverages, including workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain OCM's operations, including for safety purposes.
- For client marketing purposes.
- Exercise or defend the legal rights of OCM and our employees, affiliates, customers, contractors, and or agents.

OCM COLLECTS EMPLOYEE PERSONAL INFORMATION BY:

- Gathering from the applicant or job candidate themselves: either in person, by telephone, by email, or through systems that facilitate the collection of information from you (e.g., the online administrative systems for employment applications, benefits, 401(k), and more).
- Access through publicly accessible sources (e.g., court records, social media sites, social networking sites).
- Directly from a third party (e.g., job boards, recruiters, screening providers, credit reporting agencies, or customer due diligence providers).
- Indirect or passive sources (e.g., cookies on our Sites; our IT systems; building security systems).

OCM MAY SHARE EMPLOYEE PERSONAL INFORMATION WITH:

- Service providers used to help carry out our business functions, such as financial institutions and other financial service providers, IT providers, analytics companies, outside legal counsel, and others;
- Supervisory authorities, law enforcement and/or other regulators and regulatory bodies as required for legal compliance; and
- Prospective and current advisory clients

OCM PROTECTS EMPLOYEES' PERSONAL INFORMATION:

Employee Personal information is stored by OCM using industry-standard, reasonable, and technically feasible physical, technical, and administrative safeguards against foreseeable risks, such as unauthorized access.

Individuals should be aware that the websites and data storage are run on software, hardware and networks, any component of which may, from time to time, require maintenance or experience problems or breaches of security beyond our control. OCM is not responsible for the acts and omissions of any third parties.

We cannot guarantee the security of the information on and sent from the websites. No transmission of data over the internet is guaranteed to be completely secure. It may be possible for third parties, not under the control of OCM, to intercept or access transmissions or private communications unlawfully. While we strive to protect your Employee Personal Information, neither OCM nor any of our Service Providers can ensure or warrant the security of any information you transmit to us over the internet. Any such transmission is done at your own risk.

RETENTION AND SHARING OF EMPLOYEE PERSONAL INFORMATION:

OCM will not sell the Employee Personal Information collected and will not share information with third parties for the purpose of cross-context behavioral marketing. No applicant or job candidate will be discriminated against for exercising their rights under the CPRA. OCM will retain employee information for a reasonable timeframe (usually 1-5 years) after termination.

**One Capital Management, LLC**
**CA Personnel Policy**
**April 2025**

ONECAPITAL MANAGEMENT, LLC

## CA Personnel Policy

CA PERSONNEL RIGHTS AND HOW TO EXERCISE:

The following are a list of CA Personnel Rights:

Right to Know:

You can ask that we disclose to you the categories of Employee Personal Information we collected about you; the categories of sources for the Employee Personal Information we collected about you; our purpose for collecting your Employee Personal Information; and the categories of third parties to whom we disclosed your Employee Personal Information. You also can request that we provide you the specific pieces of Employee Personal Information that we collected about you.

Right to Delete:

You can ask us to delete the Employee Personal Information that we collected from you. Please note that, in certain instances, we may not be able to process your request, such as due to the existence of a legal obligation or pursuant to other permitted exceptions.

Right to Correct:

You can ask us to correct inaccurate Employee Personal Information that we maintain about you.

Right to Limit Use and Disclosure of Employee Personal Information:

CPRA allows you to limit use and disclosure of Employee Personal Information about you, unless an exception applies.

To exercise any of these rights, please submit a request to the OCM Compliance Department at compliance@onecapital.com.

INQUIRIES REGARDING EMPLOYEE PERSONAL INFORMATION:

Individuals with questions regarding the use and retention of Employee Personal Data should similarly submit requests through the OCM Compliance Department email address, compliance@onecapital.com.