Candidate Authorization (CA)

When submitting a candidate, we ask that all referral sources copy and paste the language below into an email that is sent to the candidate to acknowledge. Proof of this acknowledgement should be provided with every submittal.

By acknowledging this email, you hereby authorize me to present your resume and/or credentials to The Siegfried Group, LLP ("Siegfried") and act as your sponsor throughout the recruiting process.

Furthermore, you acknowledge that within the past six (6) months you have not:

(1) been introduced to Siegfried or attended any events hosted by Siegfried through any other Siegfried employees, alumni, search firms, or recruiting sources,
(2) applied to a job posting with the firm; or
(3) agreed to this authorization for any other sponsor.

NOTE: If you have provided this authorization for another sponsor within the past six (6) months, please provide additional details as to **who** you originally provided authorization to and **why** you are signing it again.

- Who:
- Why:

Additionally, we respect the privacy of prospective candidates for employment. This Privacy Notice and the attached Addendum set forth how we collect, process, and use the information we obtain from the referral source on your behalf. By acknowledging this email, you are willingly accepting The Siegfried Group's Privacy Policy and the attached Addendum.

Candidate Authorization (CA) Renewal

As all CAs expire after six (6) months, it is encouraged to obtain a CA renewal by showing proof of acknowledgement of the statement below.

By acknowledging this email, you hereby authorize _____ (FULL NAME) to continue to act as your sponsor throughout the recruiting process with The Siegfried Group for the next six (6) months.

Addendum to Privacy Policy for Siegfried's
Current, Former, and Prospective Employees

In addition to the information set forth in The Siegfried Group, LLP Privacy Policy located at https://www.siegfriedgroup.com/privacy/ (the Privacy Policy), Siegfried may collect and process additional personal information relating to our current, former, and prospective employees in the normal course of our business. This personal information allows us to:

- Complete background checks including, without limitation, county and federal criminal, federal civil, social security and address trace, extended global sanctions list, credit history, motor vehicle record, sex offender registry, drug testing, education verification, and employment verification;
- Verify employee ability to be lawfully employed in the United States of America;
- Collect data voluntarily provided relating to our efforts to foster an equal opportunity workplace;
- Pay our employees' wages, as well as provide benefits such as medical, dental, and retirement savings;
- Properly pay and/or withhold state and federal taxes;
- Further our recruitment efforts;
- Conduct performance reviews and make employment decisions;
- Deploy our employees to work at client locations;
- Send our employees to events to promote their growth and development, as well as provide networking opportunities;
- Monitor workplace and Siegfried's IT systems for potential security violations;
- Protect Siegfried assets, including and in connection with internal investigations, through the (a) monitoring and review of email, communications, and information on Siegfried technology to the extent permitted by and in compliance with law; (b) backup or storage of information on Siegfried desktops/laptops and other Siegfried technology; and (c) authentication of employees' identities and the implementation of security measures;
- Maintain contact information and global directories;
- Maintain and improve workplace and health, safety, and security; and
- Contact a designated party in the event of an emergency.

Sensitive Personal Information We Collect

Some of the personal information we collect about you may be considered "Sensitive" under applicable laws. We will collect Sensitive personal information from you where we have a legal obligation to do so or with your explicit consent. The types of Sensitive personal information we process may include:

- Identity and immigration information such as national identity card, passport, details of residency and work permit for purposes of verifying your legal ability to work and to maintain your employment or status as an independent contractor at Siegfried;
- Demographic data such as your gender, race, ethnicity, sexual orientation, disability, religious or philosophical belief for purposes of Siegfried's developing business initiatives and programs and compliance requirements;
- Health information (for example, to accommodate a disability or dietary restriction);

- Biometric information such as an employee's fingerprint, voiceprint or scan of your hand or face geometry (for example, for authentication purposes when using work-related devices and/or systems); and
- Criminal offenses or convictions for background check purposes to determine a current or prospective employee's suitability for an open position or opportunity at Siegfried where this is permitted by applicable law.

The personal information collected is set forth in our Privacy Policy. In addition, Siegfried may also collect certain biometric information including information to complete a background investigation (for example, a urine sample), as well as relating to granting access to certain secure information (for example, using your fingerprint to access the Workday application or your photograph in marketing materials).

Siegfried will not disclose your personal information to third parties other than as described in the Privacy Policy unless Siegfried has your permission or is required or permitted by law. Your rights to request a copy of, deletion of, or correction of your personal information is set forth in the Privacy Policy.