Policy on Privacy of Personal Data
for
CDI Corporation and its U.S. Related Companies

Objective and Scope of this Policy

The objective of this data privacy policy (the "Policy") for CDI Corporation and its related U.S. companies (collectively referred to in this Policy as the "Company") is to create effective administrative, technical and physical safeguards for the collection, storage, use and transmission of Personal Data (as we define this below) of employees, clients and third parties (such as consultants) that the Company receives in connection with its ongoing operations. Greater restrictions and safeguards apply to certain Personal Data which is referred to in this Policy as Sensitive Personal Data (also defined below). This Policy applies to all of the Company's operations in the United States. However, see page 4 with regard to the GDPR rules applicable to the personal data of European residents.

Statement of Policy

As part of its normal business operations, the Company collects Personal Data. It is the policy of the Company to use Personal Data only for legitimate business purposes and to take steps to safeguard Personal Data and to protect it from unauthorized disclosure.

Definitions of Personal Data and Sensitive Personal Data

For purposes of this Policy, the term "Personal Data" means any data that, together with a person's first and last name or first initial and last name, can be used to uniquely identify, contact or locate the person. Examples of such Personal Data include an individual's home address, personal telephone number or e-mail address (but not the person's CDI telephone number or e-mail address), or surname prior to marriage. Personal Data includes Sensitive Personal Data, which is defined below.

For purposes of this Policy, the term "Sensitive Personal Data" means a person's first and last name or first initial and last name in conjunction with any of the following:

- Social Security Number (SSN)
- Driver's license number
- State-issued identification card number
- Financial account number (with or without a security code, access code or PIN number)
- Credit or debit card number (with or without a security code, access code or PIN number)
- Passport number or immigration visa number
- Compensation or benefit information
- Health or medical Information, including health insurance information, referred to in the HIPAA statute as Protected Health Information (PHI)

However, any of the above items that are lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public or which a person has provided to the Company with the expectation or understanding that the

item(s) will be made available outside the Company will not be considered Personal Data or Sensitive Personal Data for purposes of this Policy.

Personal Data and Sensitive Personal Data include any of the above-described data relating to employees of the Company as well as Personal Data and Sensitive Personal Data of non-employees which Company personnel may receive or have access to in connection with the services provided to clients of the Company.

Provisions relating to Personal Data

The following provisions will apply to all Personal Data, including Sensitive Personal Data:

- No Company employee, director, consultant, vendor or representative will access or use any employee's Personal Data for any reason other than legitimate Company business purposes which such employee, director, consultant, vendor or representative is authorized to perform. The Company will only collect that amount of Personal Data that is necessary to accomplish its legitimate business purposes. The Company will maintain Personal Data in a confidential manner.
- The Company will retain records containing Personal Data for only the time reasonably necessary to accomplish the Company's legitimate business purposes or to comply with state or federal laws or regulations. The Company will take all reasonable steps to delete or destroy (using appropriate means such as shredding) records containing Personal Data in accordance with the Company's record retention policies. The Company will destroy electronic media or physical documents containing Personal Data so that all Personal Data becomes unreadable, undecipherable or impossible to practically reconstruct. Personnel should always confirm prior to destruction that the electronic or physical documents are not subject to a litigation hold requiring their preservation.
- The Company will take all reasonable steps to restrict access to Personal Data to those persons who have a legitimate need for such access to perform a legitimate Company-related business function.
- Employees should create computer passwords that are sufficiently strong (complex), are changed on a regular basis and adhere to the Company's password policy.
- The Company will require that terminated employees return all records containing Personal Data, in any form that they may have in their possession at the time of termination. The Company will block a terminated employee's physical and electronic access to Personal Data following termination of employment.
- If Personal Data is disclosed to third parties, it's expected that the Company will establish contractual or other arrangements with such third parties to confirm the third parties' capability and commitment to maintain the security and privacy of the Personal Data in accordance with applicable law, except when disclosure is (i) pursuant to law, regulation, court order or administrative agency request; (ii) to comply with a legal obligation; or (iii) for use by law enforcement personnel. Company personnel should seek to ensure that when a third party receiving Personal Data from the Company becomes aware of unauthorized access to such Personal Data, or has a reasonable belief that a substantial risk of

unauthorized access exists, the receiving party will provide notice to the Company as soon as practicable.

- The Company will conduct periodic audits to ascertain that Personal Data is collected, used, maintained and communicated consistent with this Policy and other policies of the Company.
- The Company will conduct an immediate post-incident review whenever there is there is a data security incident involving unauthorized access to Personal Data that requires notification under any applicable state or federal law. This review will help determine whether any changes in security practices are necessary or appropriate.

Provisions relating to Sensitive Personal Data

The following provisions will apply only to Sensitive Personal Data:

- The Company will not do any of the following:
  - publicly post or display Sensitive Personal Data;
  - visibly print any Sensitive Personal Data on any check, pay stub or payment advice, timecard or any similar or related document;
  - visibly print any Sensitive Personal Data on any ID badge or card;
  - encode or embed Sensitive Personal Data on any check, pay stub or payment advice, timecard, ID badge or card, or any related document; or
  - place or maintain Sensitive Personal Data in files with unrestricted access.
- When Sensitive Personal Data is disclosed to a third party electronically across public networks, the Sensitive Personal Data should be communicated using approved, industry-standard encryption. If Sensitive Personal Data is transmitted to a third party in paper (hard copy) form, it should be hand delivered or sent via a trusted courier service (such as FedEx).
- Employees who use mobile devices (such as laptops, notebook computers, tablets (e.g., iPads) and smart phones) and portable storage devices (such as Company-issued disks, magnetic tapes, external/removable hard drives, thumb drives, CDs and DVDs) are responsible for ensuring the physical security of such equipment and must adhere to the Company's mobile computing policy.
- The Company will evaluate the ability of third party service providers to implement and maintain appropriate security practices for the Sensitive Personal Data to which the Company has permitted them access. The Company will execute written agreements with any third parties retained by the Company which will possess Sensitive Personal Data, requiring such parties to implement and maintain appropriate security procedures and practices related to the processing, transportation, maintenance and destruction of documents containing Sensitive Personal Data.

Provisions relating to Social Security Numbers

When the Company collects SSNs, the Company will:

- handle SSNs with a high degree of security and confidentiality and in compliance with this

Policy and other Company policies, as well as all applicable laws and regulations;

- collect and store SSNs only when they are essential for approved business processes or to meet legal requirements, such as the generation of W-2 tax forms;
- authorize the fewest number of people possible to access SSNs in both electronic and non-electronic form;
- permit only those authorized to view SSNs to do so only when needed for an approved business purpose;
- dispose of electronic and non-electronic records containing SSNs in a secure manner that minimizes the risk of unauthorized access; and
- restrict each employee's access to SSNs for any purpose other than for a legitimate or necessary purpose related to the conduct of the Company's business.

Technical Safeguards

To reduce the risks to the security, confidentiality and integrity of any records containing Personal Data, the Company will implement appropriate technical safeguards such as firewalls, security patches, malware protection, and security software and services on all Company computers and systems which process or store Personal Data. Such computers and systems will be monitored for use of or access to Personal Data which violates this Policy.

Notifications of Breaches of Sensitive Personal Data

All Company personnel should immediately report to the Director of Information Security, the Chief Information Officer or the Chief Compliance Officer any suspicious or unauthorized use, access, disclosure, loss or theft of Sensitive Personal Data and any loss of a mobile device or mobile storage device which may contain or access Sensitive Personal Data. In the event of a breach of Sensitive Personal Data security, as defined in applicable state or federal law, the Company will notify the individuals affected. The Company may also notify appropriate state or federal agencies and/or law enforcement authorities and will take whatever additional steps may be required or, in the Company's view, advisable to deal with the breach.

Provisions relating to GDPR (Personal Data of European Residents)

On May 25, 2018, a new privacy law went into effect in the European Union (EU) and the European Economic Area (EEA) called the General Data Protection Regulation or the GDPR. Among other things, the GDPR expands privacy rights granted to individuals in the EU and the EEA. While the Company currently possesses only limited amounts of personal data of individuals subject to the GDPR, CDI is committed to compliance with the GDPR with respect to such personal data. See CDI's GDPR Privacy Statement for information about the rights of individuals in the EU and the EEA regarding their personal data and about the Company's practices for gathering, storing and using the personal data of such individuals who apply for or use the Company's staffing, employment or outsourcing services, who use the Company's websites, and who are representatives of the Company's clients (including prospective clients), service providers and suppliers.

Administrative Responsibilities

The Director of Information Security (or such other person who may be designated by the Chief Information Officer) and the Chief Compliance Officer will jointly oversee the implementation and enforcement of this Policy, working closely with the Chief Information Officer and the Information Security Board. The Director of Information Security and the Chief Compliance Officer will periodically review this Policy in light of technological or regulatory changes. They will also be responsible for periodic training of the Company's employees regarding this Policy.

Publication of this Policy

The Company will publish this Policy by posting it on the Company's website. Updates to this Policy will be communicated to the Company's employees. Employees will be provided with a copy of this Policy upon hiring.

Violations

Violations of this Policy will subject the violator to discipline, up to and including termination of employment or, if the violator is a consultant, vendor or representative, termination of that relationship.