Sample Data Privacy Provisions for Employee Handbook

The Company is committed to protecting the security and integrity of data and information that it creates, receives and maintains related to our employees, our clients, our staff, and our operations. For that reason, the Company has developed policies that contain detailed instructions and procedures for keeping our data, information, and property safe and secure. Employees are responsible for reading, understanding, and complying with the requirements in these policies as they relate to the employee's position with the Company. The Company expects all employees to use sound judgment and to act in ways that protects the Company's data, information, equipment, assets, and communication systems.

An important aspect of an effective data security program is that members of our community understand our policies and are alert to risks to our data, information, equipment, assets, and communication systems. We ask that every employee immediately report anything that may place the Company's data, information, equipment, assets, and communication systems at risk.

Ensuring that confidential information about clients, employees, partners and our company is properly protected is a top priority at Company. Examples of confidential information include, but are not limited to:

- Employee records, including social security numbers and any employee health or insurance information or records
- Compensation data
- Unpublished financial information
- Data of customers/partners/vendors, including credit cards and other financial account information
- Customer lists (existing and prospective)
- Unpublished goals, forecasts and initiatives
- Marketing strategies
- Pending projects and proposals
- Scientific and technical data

As part of our hiring process, we may ask you to sign non-compete and non-disclosure agreements (NDAs.) We are also committed to:

- Restricting and monitoring access to confidential information or otherwise sensitive data.
- Developing and maintaining transparent data collection procedures.
- Training employees in online privacy and security measures.
- Building and maintaining secure networks to protect online data from cyberattacks.
- Establishing data protection practices (e.g. secure locks, data encryption, frequent backups, access authorization.)

The protection of confidential information is vital to the interests and the success of Company. Any release of confidential information shall be made by authorized personnel only. We expect you to act responsibly when handling confidential information. Confidential information may not be accessed or disclosed by anyone without the authority to do so. If you have any doubt about whether you have authority to access or disclose confidential information, it is your responsibility to ask your supervisor before doing so. Access or disclosure of confidential information by those with authority may only be made

for legitimate Company business purposes and must at all times be consistent with Company's policies for the protection of confidential information, including but not limited to its Written Information Security Program.