**DATA PROTECTION POLICY**

**Objective**

The objective of Company and its affiliates (“*Company*”) in the development and implementation of this comprehensive Data Protection Policy (“*DPP*”), is to create effective administrative, technical and physical safeguards for the protection of Personal Data. The DPP sets forth Company’s policy for adhering to the Data Protection Principles, as outline herein, and complying with applicable data protection regulations, including the General Data Protection Regulation.

**Definitions**

For purposes of this DPP, Personal Data means any information relating to an identified or identifiable natural person (“*Data Subject*”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

For purposes of this DPP, Special Categories of Personal Data include Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and also include genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.

* Genetic Data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
* Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
* Data Concerning Health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

**Purpose**

The purpose of the DPP is to better:

* Ensure the security and confidentiality of Personal Data;
* Take appropriate measures to comply with relevant data protection laws, including the General Data Protection Regulation;
* Protect against any anticipated threats or hazards to the security or integrity of such information; and
* Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of harm to Data Subjects.

**Data Protection Principles**

It is the Company policy that Personal Data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

**Data Protection Officer**

Company has designated a Data Protection Officer to implement, supervise and maintain the DPP. The Data Protection Officer will be responsible for:

1. Initial implementation of the DPP;
2. Training employees;
3. Regular testing of the DPP’s safeguards;
4. Evaluating the ability of each of the Company’s third party service providers to implement and maintain appropriate security measures for the Personal Data to which the Company has permitted them access, consistent with the regulations; and requiring such third party service providers by contract to implement and maintain appropriate security measures;
5. Reviewing the scope of the security measures in the DPP at least annually, or whenever there is a material change in the Company’s business practices that may implicate the security or integrity of records containing Personal Data; and
6. Conducting training sessions for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to Personal Data on the elements of the DPP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the Company’s requirements for ensuring the protection of Personal Data.

**Internal and External Risks**

To combat internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Data, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

**Purpose Limitation**

1. The Company shall only collect Personal Data of clients, customers, suppliers, vendors or employees that is necessary to accomplish the Company’s legitimate need to access said records, and for a legitimate job-related purpose, or necessary to the Company to comply with state or federal regulations.

**Data Minimisation**

1. The Company shall limit its collection of Personal Data to the minimum necessary information to accomplish the Company’s legitimate purposes.

**Accuracy**

1. Company shall take all reasonable measures to ensure the accuracy of the Personal Data it processes.

**Storage Limitation**

1. Any Personal Data stored shall be disposed of when no longer needed for business purposes or required by law for storage. Paper or electronic records (including records stored on hard drives or other electronic media) containing Personal Data shall be disposed of only in a manner that complies with the regulations and as follows:
	1. Paper documents containing Personal Data shall be either redacted, burned, pulverized or shredded upon disposal so that Personal Data cannot be practicably read or reconstructed; and
	2. Electronic media and other non-paper media containing Personal Data shall be destroyed or erased upon disposal so that Personal Data cannot be practicably read or reconstructed.

**Integrity and Confidentiality**

1. [PHYSICAL ASSET CONTROL PROTOCOL] All assets must be secured from theft by locking up and maintaining a secure workplace, whether that work takes place in the Company’s offices, client site, a car, hotel or a home.
2. [ACCESS CONTROL PROTOCOL]
	1. Access to electronically stored Personal Data shall be electronically limited to those Company employees having a unique log-in ID.
	2. Employees must ensure that all computer systems under their control are locked when leaving their respective workspaces. Employees must not disable any logon access.
	3. [INACTIVITY LOCK-OUT]
	4. [VISITOR ACCESS]
	5. [VISITOR RESTRICTIONS]
3. [FIREWALL, PATCHES, ANTI-VIRUS, ANTI-MALWARE, INTERNET SECURITY] shall be reasonably up-to-date and installed on any computer that stores or processes Personal Data.
4. [ENCRYPTION PROTOCOL]
5. There shall be secure user authentication protocols in place that:
	1. Control user ID and other identifiers;
	2. Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
	3. Control passwords to ensure that password information is secure.

**Employee Training and Compliance**

1. A copy of this DPP must be distributed to each current Company employee with access to Personal Data and to each new Company employee with access to Personal Data at the commencement of their employment. It shall be the employee’s responsibility for acknowledging in writing, by signing the attached Acknowledgment that he/she has received a copy of this DPP and will abide by its provisions.
2. All Company employees with access to Personal Data shall participate in the Company’s training program on the detailed provisions of the DPP. Each such Company employee shall sign and acknowledge his/her completion of the training program and agreement to abide by the DPP. Immediate retraining of Company employees shall occur to the extent the Data Security Coordinator determines a need.
3. [PROCEDURES FOR TERMINATED EMPLOYEES]
4. [DISCIPLINE FOR FAILURE TO COMPLY]

**Data Subject Rights**

**Right of Access**

A Data Subject has the right to access the Personal Data concerning him or her being processed by the Company. The Company will honor such request by providing the following information:

* the purposes of the processing;
* the categories of personal data concerned;
* the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
* where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
* the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
* the right to lodge a complaint with a supervisory authority;
* where the personal data are not collected from the data subject, any available information as to their source;
* information related to the safeguards in place for the cross-border transfer of Persona Data, as applicable.

The first copy of such Personal Data shall be provided at no cost. For any further copies requested by the data subject, the Company will charge a fee not to exceed [AMOUNT]. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information will be provided in a commonly used electronic form.

**Right of Rectification**

The Data Subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

**Right to Erasure (“Right to be Forgotten”)**

A Data Subject has the right to request the erasure of the Personal Data concerning him or her being processed by the Company. The Company will honor such request without undue delay if:

* the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
* the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
* the personal data have been unlawfully processed;
* the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

The Company can decline to honor a request for erasure under the following circumstances only:

* in order to exercise the right of freedom of expression and information;
* in order to comply with a legal obligation which requires processing by Union or Member State law to which the Company is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company;
* for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
* for the establishment, exercise or defence of legal claims.

**Right to Data Portability**

The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to the Company in a structured, commonly used and machine-readable format and transmit those data to another controller. The Company will honor a request to transmit Personal Data from the Company to another data controller if the lawful purpose for processing the Personal Data is based on Data Subject consent or via contract.

**DATA PROTECTION POLICY**

**ACKNOWLEDGMENT**

**Employee Name**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Employee Position**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date of Receipt of Data Protection Policy**:

I acknowledge and agree that:

1. I have received a copy of the Company Data Protection Policy;
2. I have read the Data Protection Policy in its entirety and fully understand the provisions contained therein; and
3. I agree to abide by the provisions contained in the Data Protection Policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date