Document Title:	**Data Privacy Policy**
Document Code:	**HRA 19-1020**
Revision No.:	**0**
Effectivity Date:	**July 15 , 2019**

I. GENERAL POLICY STATEMENT

This policy is hereby issued by Staffhouse International Resources Corporation to collect and process personal information in accordance with the applicable laws and regulations on data privacy, including the Data Privacy Act of 2012 (DPA) and its implementing rules and regulations (DPA IRR).

In processing personal data, Staffhouse International Resources Corporation adhere to the general privacy principles of transparency, legitimate purpose, and proportionality, and such other relevant principles in the collection, processing, and retention of personal data as required by applicable law.

Also, the Staffhouse International Resources Corporation website adheres to guidelines prescribed by the Department of Information and Technology (DICT), which highlights, and others, compliance with the Data Privacy Act of 2012.

II. OBJECTIVE

To be used as a basis to protect and promote the rights and welfare of employees, clients and candidates as we receive various data and information, whether or not constituting personal data, and covered by our responsibility to keep the information confidential.

III. COVERAGE

All employees of Staffhouse International Resources Corporation regardless of rank, position or status, clients and candidates' information shall diligently observe professional obligation in keeping, maintaining and processing information confidential in accordance with the requirement of RA 10173.

IV. DEFINITIONS

A. Data Privacy Act (DPA) refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations.
B. Data Subject refers to an individual whose Personal Information, Sensitive Personal Information or Privileged Information is processed.
C. Company refers to Staffhouse International Resources
D. Personal Data refers to Personal Information, Sensitive Personal Information or Privileged Information.
E. Personal Information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably or directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
F. Processing refers to any operation or set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system.
G. Privileged Information refers to any and all forms of Personal Data, which under the Rules of Court and other pertinent laws constitutes privileged communications.
H. Security Incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes

incidents that would result to a personal data breach, if not for safeguards that have been put in place.

l. Sensitive Personal Information refers to Personal Data:

a. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

b. about an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

c. issued by government agencies peculiar (unique) to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

d. specifically established by an executive order or an act of Congress to be kept classified.

V. ORGANIZATIONAL SECURITY MEASURES

A. Data Protection Officer

A Data Protection Officer ("DPO") shall be appointed by the Company. The DPO is responsible for ensuring the Company's compliance with applicable laws and regulations for the protection of data privacy and security. The functions and responsibilities of the DPO shall particularly include, among others:

1. monitoring the Company's Personal Data Processing activities in order to ensure compliance with applicable Personal Data privacy laws and regulations, including the conduct of periodic internal audits and review to ensure that all Company's data privacy policies are adequately implemented by its employees and authorized agents;

2. acting as a liaison between the Company and the regulatory and accrediting bodies, and is in charge of the applicable registration, notification, and reportorial requirements mandated by the Data Privacy Act, as well as any other applicable data privacy laws and regulations;

3. developing, establishing, and reviewing policies and procedures for the exercise by Data Subjects of their rights under the Data Privacy Act and other applicable laws and regulations on Personal Data privacy;

4. acting as the primary point of contact whom Data Subject may coordinate and consult with for all concerns relating to their Personal Data;

5. formulating capacity building, orientation, and training programs for employees, agents or representatives of the Company regarding Personal Data privacy and security policies;

6. preparing and filing the annual report of the summary of documented security incidents and Personal Data breaches, if any, as required under the Data Privacy Act, and of compliance with other requirements that may be provided in other issuances of the National Privacy

B. Data Privacy Principles

All Processing of Personal Data within the Company should be conducted in compliance with the following data privacy principles espoused in the Data Privacy Act:

a. **Transparency**. The Data Subject must be aware of the nature, purpose, and extent of the Processing of his or her Personal Data by the Company, including the risks and

safeguards involved, the identity of persons and entities involved in Processing his or her Personal Data, his or her rights as a Data Subject, and how these can be exercised. Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.

b. **Legitimate purpose**. The Processing of Personal Data by the Company shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. **Proportionality**. The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed by the Company only if the purpose of the Processing could not reasonably be fulfilled by other means.

C. Data Processing Records

Adequate records of the Company's Personal Data Processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of all the concerned business and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

1. information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;

2. a description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;

3. general information about the data flow within the Company, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;

4. a general description of the organizational, physical, and technical security measures in place within the Company; and

5. the name and contact details of the DPO, Personal Data processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

D. Management of Human Resources

The DPO, with the cooperation of the Company's Human Resources department ("HR"), shall develop and implement measures to ensure that all the Company's staff who have access to Personal Data will strictly process such data in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of the Company and conducting training programs to educate employees and agents on data privacy related concerns.

The DPO, with the assistance of HR, shall ensure that Company shall obtain the employee's informed consent, evidenced by written, electronic or recorded means, to:

1. The Processing of his or her Personal Data, for purposes of maintaining the Company's records; and

2. A continuing obligation of confidentiality on the employee's part in connection with the Personal Data that he or she may encounter during the period of employment with the Company. This obligation shall apply even after the employee has left the Company for whatever reasons.

E. Data Collection Procedures

The DPO, with the assistance of the Company's HR and any other departments of the Company responsible for the Processing of Personal Data, shall document the Company's Personal Data Processing procedures. The DPO shall ensure that such procedures are updated and that the consent of the Data Subjects (when required by the DPA or other applicable laws or regulations) is properly obtained and evidenced by written, electronic or recorded means. Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that Processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

F. Data Retention Schedule

Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by the Company for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO, with the assistance of the Company's HR and any other departments of the Company responsible for the Processing of Personal Data, shall be responsible for developing measures to determine the applicable data retention schedules, and procedures to allow for the withdrawal of previously given consent of the Data Subject, as well as to safeguard the destruction and disposal of such Personal Data in accordance with the DPA and other applicable laws and regulations.

VI. PHYSICAL SECURITY MEASURES

The DPO, with the assistance of HR and Information and Technology department ("IT"), shall develop and implement policies and procedures for the Company to monitor and limit access to, and activities in, the offices of HR, as well as any other departments and/or workstations in the Company where Personal Data is processed, including guidelines that specify the proper use of, and access to, electronic media.

The design and layout of the office spaces and work stations of the abovementioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons.

The duties, responsibilities, and schedules of individuals involved in the Processing of Personal Data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time. Further, the rooms and workstations used in the Processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

VII. TECHNICAL SECURITY MEASURES

The DPO, with the cooperation and assistance of IT, shall continuously develop and evaluate the Company's security policy with respect to the Processing of Personal Data. The security policy should include the following minimum requirements:

a. safeguards to protect the Company's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;

b. the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Company's data processing systems and services;

c. regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Company's computer network and system, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a Personal Data breach;

d. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

e. a process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

f. encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

VIII. RIGHTS OF DATA SUBJECTS

Under the DPA, data subjects have the following rights:

- **Right to object -** As a data subject, clients have the right to indicate his refusal to the collection and processing of his personal data unless the processing is required pursuant to a subpoena, lawful order, or as required by law.
- **Right to access -** upon request, clients may be given access to his personal data that we collect and process insofar as allowed by law.
- **Right to rectification -** Clients have the right to dispute inaccuracy or error on his personal data and may request to immediately correct it. Upon the request, and after correction has been made, Staffhouse International Resources Corporation will inform any recipient of its personal data and the subsequent rectification that was made.
- **Right to erasure or blocking -** The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her Personal Data from the Company's filing system
- **Transmissibility of Rights of Data Subjects -** The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject to which he or she is an heir or an assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her rights.
- **Data Portability -** Where his or her Personal Data is processed by the Company through electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject. The exercise of this right shall primarily take into account the right of Data Subject to have control over his or her Personal Data being processed based on consent or contract, for commercial purposes, or through automated means. The DPO shall regularly monitor and implement the

National Privacy Commission's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

IX. DATA BREACHES & SECURITY INCIDENTS

A. Data Breach Notification

All employees and agents of the Company involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or Security Incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or Security Incident. The DPO shall notify the National Privacy Commission and the affected Data Subjects pursuant to requirements and procedures prescribed by the DPA.

The notification to the National Privacy Commission and the affected Data Subjects shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by the Company to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, as may be updated from time to time.

B. Breach Reports

All Security Incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of Personal Data breaches, the report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Company. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

X. DISCLOSURE PURSUANT TO JUDICIAL OR GOVERNMENT SUBPOENAS, WARRANTS TO ORDERS

Staffhouse International Resources Corporation reserves the right to disclose personally identifiable information as required by law and when we believe that disclosure is necessary to protect our rights and/or comply with a judicial proceeding, court order, or legal process served on us.

XI. EFFECTIVITY

This policy takes effect July 15, 2019 and shall be made known to all employees.

Prepared by:

Diane Lane A. Granado
HR Officer

Noted by:

Aina T. Liwanag
HR Admin Manager

Approved by:

Marc R. Capistrano **Emmanuel S. Gomez**
Managing Directors