[DATA PROTECTION AND DATA SECURITY POLICY]

INTRODUCTION

UNEC, including its affiliates, (the "Company") values the confidentiality of personal data and is committed in ensuring that all personal data handled by us will be processed according to legally complaints standards of data protection and data security.

We confirm for the purposes of the data protection laws, that the Company is the data controller of the personal data in connection with your employment. This means that we determine the purposes for which, and the manner in which your personal data is processed.

The purpose of this policy is to help us achieve our data protection and data security by:

- notifying our employees of the types of personal information that we may hold about them, our customers, suppliers and other third parties and what we do with that information;
- setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring Employees understand our rules and legal standards;
- clarifying the responsibilities and duties of Employees in respect of data protection and data security.

All Employees have a personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The responsible Data protection officer must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.

Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing Employees or customer personal data without authorization or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.
This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

DEFINITION

- **Data protection laws** means all applicable laws relating to the processing of Personal Data, including, for the period during which it is in force.
- **Data subject** means the individual to whom the personal data relates to.
- Personal data means any information that related to an individual who can be identified from that information.
- **Processing** means any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
- **Personal data** refers to all types of:

- Personal information – "any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual";

- Sensitive personal information – "personal information about an individual's race, ethnic origin, marital status, age, color, religious/philosophical/political affiliations, health, education genetic or sexual life, legal proceedings, government issued identifiers and other information specifically established to be kept classified";

- Privileged information – "any and all forms of information which, under the Rules of Court and other pertinent laws, constitute privileged communication, such as, but not limited to, information which a person authorized to practice medicine, surgery or obstetrics may have acquired in attending to a patient in a professional capacity".

WHY DOES THE COMPANY COLLECT YOUR PERSONAL DATA?

The Company collects, uses, processes, stores and retains personal data when reasonable and necessary to perform its business processes effectively, safely and efficiently and in accordance with corporate policies.

In general, the Company may be using your data for any of the following purposes:

- To comply with the Company's obligations under local law and as required by government organizations and/or agencies
- To comply with legal and regulatory requirements or obligations; and,
- To perform such other processing or disclosure that may be required under law or regulations.

In addition, from the general uses mentioned above, we may use your personal information depending on your transactions with the Company in any of the following means:

A. When you want to become part of our team

- To grant access to the Company premises for the performance of individual's duties and obligations;
- To manage security at the workplace;
- To process employee salaries and benefits;
- To execute employee development, communications, health and engagement programs and organizational planning and management;
- To provide assistance in case of emergency, and to account for employees during emergencies and/or crises;
- To grant access to the Company's IT systems and infrastructure, consistent with IT policies and procedures;
- To provide access to services, privileges or job opportunities offered by affiliates and subsidiaries of the Company;
- To process requirements for work purposes, including travel, certification, appointments, and the like;
- To conduct internal investigations in relation to security incidents, disciplinary proceedings and other analogous circumstances;

- To comply with government requirements, including permits, disclosures, orders and reports; and
- To perform such other processing or disclosure that may be required in the course of the Company's business or under law or regulations.

B. When you inquire on our website, social media sites or email:

- To respond to specific complaints, enquiries, requests or to provide requested information;
- Allows us to personalize the site for the user and view how and when specific users visit the site, helping us to improve the site. The use of cookies is an industry standard. Cookies are stored on your computer and are used only to view information on your hard drive that was put there by a cookie from this site. If you do not wish to receive cookies you may set your web browser to prevent them;

C. When you enter the Company premises as guest or visitor:

- To grant access to the Company premises for the performance of individual's duties and obligations;
- To manage security at the workplace;

D. When you are a vendor, a potential vendor, or a contractor:

- To conduct appropriate due diligence checks;
- To evaluate your proposal including your manpower, technical and operational capacity;
- To assess the practicability of your proposal and process your accreditation;
- To communicate the result of your proposal and to execute a letter of award together with the contract;
- To perform any other action as may be necessary to implement the terms and conditions of our contract; and,
- To perform other processes related to or in connection with our business, including those processing or disclosure that may be required under law or regulations.

WHAT TYPE OF PERSONAL DATA DOES THE COMPANY COLLECT?

The types of personal data that the Company will collect from you depends on the particular purpose and/or position for which you are submitting an application. The common type of data collected by the Company generally includes the following:

- Basic personal information such as name, home address, contact details and contact details for your next of kin address, social media accounts (if any);
- recruitment (including your application or curriculum vitae, references received and details of your qualifications);
- Sensitive personal information such as birth date, marital status, age, religion, nationality, gender, dependents, health information, education, employment history, pay records and government identification numbers, as well as biometric information such as full-face photographs, fingerprints, and other similar images; and
- Privileged information such as medical records, court records (if applicable), performance and any disciplinary matters, grievances complaints or concerns in which you are involved.

We will only process sensitive personal information if:

- We have a lawful basis for doing so, e.g. it is necessary for the performance of the employment contract; and
- One of the following special conditions for processing personal information applies:
  - the data subject has given explicit consent.
  - The processing is necessary for the purpose of exercising the employment law rights or obligations of the Company or the data subject.
  - The processing is necessary to protect the data subject's vital interest, and the data subject is physically incapable of giving consent.
  - Processing relates to personal data which are manifestly made public by the data subject.
  - The processing is necessary for the establishment, exercise, or defense or legal claims; or
  - The processing is necessary for reasons of substantial public interest.

The Company also generate personal data in the course of your employment, such as salary and income, payroll bank account, performance ratings, disciplinary proceedings, training and development activities, medical records and certifications.

DOES THE COMPANY USE WEB ANALYTICS?

This website uses Google Analytics, a third-party service to analyze the web traffic data on the Company's behalf. This service does not use cookies or web beacons.

Data generated is not shared with any other party. For you to fully enjoy your visit and browsing experience, only non-identifiable web traffic data are collected and analyzed, including:

- Your IP address,
- The search terms you used,
- The pages and internal links accessed on our site,
- The date and time you visited the site,
- Geolocation,
- The referring site or platform (if any) through which you clicked through to this website/page,
- Your operating system,
- Web browser.

WHAT ABOUT THE LINKS TO THIRD-PARTY WEBSITES?

From time to time, the Company website may provide links to third-party web sites which contain news, articles or advertisements. These links are provided as a service to you and we do not provide any personal data to these websites or advertisers, and therefore, we will not accept responsibility for their privacy practices. These sites are operated by independent entities that have their own privacy policies which you should also review.

UNEC's Privacy Policy does not apply to any such sites or to the use that those entities make of your information. UNEC has no control over the content displayed on such sites, nor over the measures, if any, that are taken by such sites to protect the privacy of your information.

HOW DOES THE COMPANY COLLECT, ACQUIRE OR GENERATE PERSONAL DATA?

The Company collects personal data when you:

- accomplish company forms;
- submit to the Company your resume and other employment requirements;
- disclose personal data through phone calls, email, SMS or verbal communication with Company personnel;

The Company may also acquire personal data through third parties, such as:

- Job-search platforms
- Head-hunters
- Universities and professional organizations
- Accredited hospitals or clinics
- Agencies and contractors
- Other companies (such as former employers and affiliates)

The Company generates personal data when you:

- Accept a job offer;
- Avail of benefits; and
- Participate in Company processes and activities.

HOW DOES THE COMPANY ENSURE ACCURATE AND UP-TO-DATE PERSONAL DATA?

Employees are primarily responsible for ensuring that all personal data submitted are accurate, complete and up-to-date. From time to time, the Company may request updated data from the employees.

The Company takes all reasonable steps to make sure that the personal data the Company collects, generates, uses or discloses are accurate, complete, and up-to-date, such as:

- Periodic reviews and audits of systems, processes and data;
- Verification with the concerned employees and third parties

WITH WHOM DOES THE COMPANY SHARE PERSONAL DATA?

As a general rule, the Company is not allowed to share your data with any third party except in limited circumstances as noted below:

- You authorize the Company to disclose your information to accredited/affiliated third parties or independent/non-affiliated third parties, whether local or foreign in the following circumstances:

- As necessary for the proper execution of processes related to the declared purpose;
- The use or disclosure is reasonably necessary, required or authorized by or under law.

This means the Company might provide personal data to the following:

- Our Associated Businesses, organizations, or agencies including their sub-contractors or prospective business partners that act as our service providers and contractors, consistent with the purposes discussed above;
- Affiliates of the Company;
- Authorities and government agencies;

However, the forgoing may only use such personal data for the purpose(s) disclosed in this Policy and may not use it for any other purpose.

WHAT IS OUR PRIVACY POLICY REGARDING CHILDREN?

The Company is very sensitive to privacy issues and we are especially careful in any communications with one of our most treasured customers – children. The Company would never collect personal data from children directly, without a parent's consent.

Personal data collected from children is used solely by the Company or other entities that provide technical, fulfillment or other services to the Company. For example, such entities may provide services, such as, improving our services/web sites, and fulfilling requests or administering promotions. These personal data are not sold.

Meanwhile, we urge parents to regularly monitor and supervise their children's online activities.

HOW DOES THE COMPANY PROTECT YOUR PERSONAL DATA?

The Company strictly enforces its Policy. It has implemented technological, organizational and physical security measures to protect personal data from loss, misuse, unauthorized modification, unauthorized or accidental access or disclosure, alteration or destruction. The Company uses safeguards such as the following:

- Use of secured servers and firewalls, encryption on computing devices
- Restricted access only for qualified and authorized personnel e.g. only people who are authorized to use the information can access it; where possible, personal data is pseudonymized or encrypted; information is accurate and suitable for the purpose for which it is processed; and authorized persons can access information if they need it for authorized purposes.
- Strict implementation of information security policies e.g. Personal information must not be transferred to any person to process (e.g. while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist;

Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency Employees, trainees, homeworkers and fixed-term Employees and any volunteers

WHAT WE PRACTICE TO KEEP YOUR DATA SECURE?

- ✓ Any desk or cupboard containing confidential information are kept locked.
- ✓ Computers are locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
- ✓ Data stored on CDs or memory sticks are encrypted or password protected and locked away securely when they are not being used.
- ✓ The Data Protection Officer must approve of any cloud used to store data.
- ✓ All servers containing sensitive personal data are protected by security software.
- ✓ Servers containing personal data are kept in a secure location, away from general office space.
- ✓ Data are regularly backed up in line with the Employer's back-up procedure.
- ✓ Particular care is taken by Employees who deal with telephone enquiries to avoid inappropriate disclosures. In particular:
  a. the identity of any telephone caller is verified before any personal information is disclosed;
  b. if the callers' identity cannot be verified satisfactorily then they are asked to put their query in writing;
  c. if the Callers try to bully our employees into disclosing information, they are trained to forward the call any problems or uncertainty to the highest authority in the office or site.
- ✓ Copies of personal information, whether on paper or on any physical storage device are physically destroyed when they are no longer needed. Paper documents are shredded and CDs or memory sticks or similar must be rendered permanently unreadable

WHERE AND HOW LONG DOES THE COMPANY KEEP PERSONAL DATA?

The personal data is stored in both local and off-shore facilities, such as data centers (on premise and cloud) and document storage facilities. Data collected will be retained in accordance with the following retention standards, unless you request your data to be deleted in our database immediately. Once deleted, the data will be completely removed from all the storage location.

- If the data subject has an existing contract and transaction with the Company, information will be retained all throughout the contract period and 15 years after its completion or termination.
- If the data subject has no existing contract but has existing transaction with the Company, information will be retained during the transaction and 15 years after its fulfillment.
- If the data subject has no existing contract and transaction with the Company, information will be retained for a retention period of 2 years.

WHAT IF THERE ARE CHANGES IN OUR PRIVACY POLICY?

From time to time, it may be necessary for the Company to change this Policy. If we change our Policy, we will post the revised version here and will take effect immediately, so we suggest that you check here periodically for the most up-to-date version of our Privacy Policy. Rest assured, however, that any changes will not be retroactively applied and will not alter how we handle previously collected personal data without obtaining your consent, unless required by law.

WHAT ARE YOUR RIGHTS UNDER THE DATA PRIVACY?

As data subjects, you have the following rights:

- Right to be informed;
- Right to object;
- Right to access;
- Right to rectify or Correct erroneous data;
- Right to erase or Block;
- Right to secure Data Portability
- Right to be indemnified for damages
- Right to file a complaint

The Company's decisions to provide such access or consider any request for correction, erasure and objection to process your personal data as it appears in our records are always subject to any exceptions under applicable and relevant laws.

Data impact assessments

Some of the processing that the Employer carries out may result in risks to privacy.

Where processing would result in a high risk to Employees rights and freedoms, the Employer will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If we discover that there has been a breach of Employees personal data that poses a risk to the rights and freedoms of individuals, we will report it to the concerned department within 72 hours of discovery.

We will record all data breaches regardless of their effect.

If the breach is likely to result in an elevated risk to your rights and freedoms, we will tell the affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures to be taken.

Individual responsibilities

Employees are responsible for helping the Employer keep their personal data up to date.

Employees should let the Employer know if personal data provided to the Employer changes, e.g. if you move to a new house or change your bank details.
You may have access to the personal data of other Employees members and of our customers during your employment. Where this is the case, the Employer relies on Employees members to help meet its data protection obligations to Employees and to customers.

Individuals who have access to personal data are required:

- to access only personal data that they have authority to access and only for authorized purposes;
- not to disclose personal data except to individuals (whether inside or outside of the Employer) who have appropriate authorization;
- to keep personal data secure (e.g. by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Employer's promises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devises that are used for work purposes.

Training

We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

WHO SHOULD YOU CONTACT IN CASE OF INQUIRY, FEEDBACK OR COMPLAINTS?

Should you have any inquiries, feedback on this Privacy Policy, and/or complaints, you may contact us through the following details:

[UNEC]

Al Fattan Plaza, Office 209,

Airport Road, Dubai, UAE

T +971 4 282 8242

F +971 4 282 9929

E info@unec.ae

PO Box 7510, Dubai, UAE