KBG

KING ENERGY GENERATION INC.

IT POLICY

I. OVERVIEW

- The purpose of these Information Technology (“IT”) policies and procedures is to establish guidelines for the use and management of IT equipment (workstations, servers, printers, etc.) by the company which will provide for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside the company.
- This policy safeguards the company’s entity against malicious use of properties for personal gain.
- The procedures listed in this document establish the methods of the company which will be used to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our clients and the mission of the company.
- This policy applies to all employees of the company and to all IT resources whether owned, leased, or contracted by the company.
- IT Officer is responsible for implementing and monitoring the procedures described in this document.
- IT Officer has the authority to purchase or lease and install software to monitor or enforce the policies and procedures described herein.

I. **EMPLOYEE'S ROLES AND RESPONSIBILITIES**

- All employees with access to the company's information assets (laptops, desktops, internet etc.) are responsible for the safe handling, and protection of business information assets.

I. **POLICY PRINCIPLES**

- ***Timely and Accurate Reporting***

- All employees are responsible to report information security violations, problems, or threats to the company's IT guidelines to his/her immediate supervisor. In the absence of the latter, the employee shall report the violation committed to the HR and/or IT officer.

- Specific information regarding violations and vulnerabilities must not be distributed to or shared with persons who do not have a valid 'need-to-know'.

- ***Enforcement and Compliance***

- All department managers, supervisors, and rank and file personnel are responsible for pro-actively enforcing the policies and standards described herein. Employees who violate the policy may be subject to disciplinary action up to and including termination. *Due process will be observed in taking disciplinary actions.*

- ***Authority***

- IT Officer is responsible for working with the ADMIN/HR Department to ensure that employees are well-informed, and they fully understand that disciplinary action shall take place upon non-compliance with the Information Technology Policies.
- IT Officer has the authority to strictly implement the policy and coordinate to Admin/HR if there is a violation for disciplinary action.
- IT Officer has the authority to immediately block the use of the internet at his discretion if the employee violated this policy.

I. **INFORMATION TECHNOLOGY POLICIES**

A. ***COMPUTER SYSTEM, NETWORK AND INTERNET USE***

- The company reserves the right to monitor any and all aspects of its computer system and network to ensure compliance with company policies. Monitoring includes, but is not limited to, tracking the sites that users visit on the internet, monitoring chat groups and news groups, and reviewing material downloaded or uploaded. *Violation therefore, shall be regarded to disciplinary action. C.54*

ACCEPTABLE PRACTICES

- Access to the internet is specifically limited to activities in direct support of *official company business.*
- In addition to access in support of specific work related duties, the Company Internet connection may be used for educational, research and official purposes only.
- If any user has a question of what constitutes acceptable use, he/she should check with their immediate superior for additional guidance. Management or Supervisor shall consult with IT Officer for clarification of these guidelines.

UNACCEPTABLE PRACTICES

- The Company's internet access shall not be used for any illegal or unlawful purposes, such as but not limited to:

- Transmission of violence,
- Threatening,
- Defrauding,
- Obscene or otherwise illegal or unlawful materials.
- Sexually explicit sites (pornographic)
- Hacker sites
- Warez (pirated software or hacker tools) related sites
- Sites that may conflict with the company policies and/or Business interests

- Downloading or installing of freeware and/or shareware is prohibited unless approved by the IT Officer.
- Re-mailer services, drop-boxes, or identity stripping may not be used.
- Employees must not use the Internet for playing games.
- Sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the network.

- Use of company’s electronic mail or messaging services shall be used for the conduct of company business only. These services shall not be used to harass, intimidate or otherwise annoy another person.
- The company’s internet access shall not be used for private, recreational or other non-company related activity.
- The company’s internet connection shall not be used for commercial or political purposes.
- Use of the company’s internet access shall not be used for or by performing work for profit with company resources in manner not authorized by the company.
- User shall not attempt to bypass security measures on the company’s network resources or any other system connected to or accessible through the internet.
- Company users shall not use internet access for interception of network traffic for any purpose unless engaged in authorized network administration.
- Company users shall not make use or use illegal copies of copyrighted material, store such copies on Company equipment, or transmit these copies over the company network.

COMPUTER PHYSICAL SECURITY

- Portable computers (Laptops) must be kept physically secure. Employees assigned to a portable computer by the company must assume all responsibilities of the security of the portable computer and the information/programs/data stored in it. *Violation therefore, shall be regarded to disciplinary action. B.18.*

BACK-UP OF LOCAL COMPUTERS

- Employees using the company's desktop/laptop computers are responsible for ensuring that locally held Company information is properly backed up and recoverable.

COMPUTER PREVENTIVE MAINTENANCE

- IT Officer may conduct a random audit at any time.
- Computer related issues should only be consulted to the IT Officer.
- In case that the IT Officer is unavailable to attend the immediate repair request, the user must seek approval or clearance first before seeking for local repairs. *Violation therefore, shall be regarded to disciplinary action. B.8*

UNATTENDED COMPUTERS AND INFORMATION

- Systems must have a feature that protects access to the information on the screen (screen lock) for at least a minute if being left unattended after a defined time and must not allow access until released by a valid password.

PROTECTING PASSWORDS

- Passwords must not be disclosed or shared. In general, users should never disclose their password to anyone (including to IT personnel) in any circumstances. User password must remain personal and confidential even in the event of a user lock-out. IT Officer should be able to assist users without knowing the users' password. The sharing of user IDs *is prohibited* except in specific, approved situations. *Violation therefore, shall be regarded to disciplinary action. C.12*

A. ***CLEAR DESK***

- Removable media and documents containing sensitive information, should not be left unattended where someone could easily pick it up, such as in the copying machine, printer, or in any unsecured office or workspace. Sensitive documents that are not needed anymore should be shredded immediately.

VIRUS PROTECTION

- Anti-virus software must be installed and activated on each desktop, laptop, and server with real-time scanning enabled at all times.
- Each USBs and external drive or other media to transfer data into a computer must be scanned for viruses.

I. **COMPANY INTERNET AND EMAIL ETIQUETTE**

- Company employees shall ensure that all communication through Company Email or messaging services is conducted in a professional manner. The use of vulgar or obscene language is strictly prohibited.

- Company users shall not reveal private or personal information without specific approval from management.
- Users should ensure that electronic mail messages should only be sent to those concerned users who needs to know the specific.
- Electronic Mail is not guaranteed to be private. Messages transmitted through the company electronic mail system or network infrastructure are the property of the Company and are therefore subject to inspection.

- **INFORMATION TECHNOLOGY POLICY**
- **ACKNOWLEDGEMENT RECEIPT**

Access and use of the Internet, email, authorized software, local area networks, computers, and other related equipment is a privilege for the user. The Company Information Technology Policy details the responsibilities and expectations of all employees with regard to the access and use of all company technology.

- I acknowledge that I have received information regarding the copy of the Information Technology & Procedure Manual.
- I understand that this copy provides guidelines for the use of the Internet, authorized software, local area network, computers, and other related equipment.
- I acknowledge that any changes made by the management with respect to company's technology can be modified at any time to serve the best interest of the employees and maintain the integrity of the networking systems.
- I accept fully responsibility for familiarizing myself with the technology, and will seek clarification and/or guidance from my immediate superior if questions arise concerning technology protocol and employee responsibility.
- I understand that a copy of this acknowledgement form will be held in my Personnel Record as evidence of my receipt and knowledge of Information Technology Policies.