INFORMATION TECHNOLOGY POLICY/STRATEGY OF HMRDC

Contents

Information Technology Policy/Strategy of HMRDC

1. Policy Statement

1.1 HMRDC recognises the importance of and necessity to have a policy to develop, safeguard and adopt state of the art IT.

1.2 HMRDC complies with the requirements of the Data Protection Act.

1.3 **We have identified that the following are particular risks for our business**:

- Outage of critical IT systems and Loss/corruption of critical business data.
- Unauthorised access to our computer systems, data and introduction of malicious computer viruses.
- Failure of electronic communication systems, and computerised control systems.
- Usage of unlicensed operating system and other business software.

To address those risks we have:

- ✓ Restricted access to our IT systems to relevant employees with passwords, conducted risk assessments, Trained employees on the importance of safeguarding Company information, particularly via email, and the selective use of portable memory devices, conducted regular audits on our IT systems and data storage.

- ✓ Ensured that our systems are protected with anti-virus software and live updates.

- ✓ Developed a business continuity plan that specifies actions needed if there is an interruption to our IT systems and ensured that regular back-ups are made of critical data by using only licensed versions of operating systems and other business software.

2. Who is covered by the policy?

This policy applies to all employees working at all levels and grades, (whether permanent, fixed-term or temporary) and all individuals come into contact with HMRDC for official purpose or otherwise.

3. Organisation and Responsibilities

3.1 The arrangements made to implement this policy and the allocation of duties and responsibilities for IT matters are stated in the guidelines mentioned in this policy.

3.2 You must ensure that you read, understand and comply with this policy and any breach attracts disciplinary action.

4. **Software Upgrades & Servicing**: The Company intends to keep all IT equipment updated to safeguard the effectiveness of its IT systems and security of data.

5. **Abuse of Equipment**

The following are prohibited on the Company's computer systems:

- Un-authorised alterations, accessing, copying and upgrading to any Company software, data, information, documents or internet downloads and also unauthorised usage of any portable data storage format, eg., CD/DVDs, USB drives.
- for unlawful activities such as harassment or the dissemination of offensive/obscene material, pornography, threats or defamatory statements.
- Installing, copying, distributing or using proprietary software in violation of copyright or any licensing agreement.
- Loading software, including games on to Company machines without prior authorisation.

6. **Internet, E-mail and Social Media**

6.1 The Company's e-mail facility is intended to promote effective communication on matters relating to company business. All such communications must be sent from the company domain (company's email address – ceohmrdc@gmail.com or hmrdc website emails) to internal or external recipients.

6.2 Internet access is provided on the basis of business need; however employees may access the Internet for personal use only as authorised and for legal and moral purposes only. What is legal and moral is decided by the company.

6.3. Each employee is solely responsible for the security of his/her computer and other electronic equipments.

7. **General Guidelines**

This policy establishes guidelines governing proper use of information technologies and Internet by all HMRDC employees including Consultants.

(A) INFORMATION TECHNOLOGIES

(a) Information technologies includes, without limitation, computers, computer-based networks, computer peripherals, operating systems, e-mail, Intranet, software or any combination thereof, that are made available by HMRDC for the purpose of supporting its goals of providing quality products and services to customers, increase shareholder value and foster employment satisfaction.

(b) In order to preserve the integrity of the information technology systems against accidents, failures or improper use, HMRDC reserves the right to limit, restrict or terminate any user's access and to inspect, copy, remove or otherwise alter any data, file or system resources.

(c) These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to those resources.

(B) Access and Use

Users of HMRDC's information technologies accept the following specific responsibilities:

1. Access to the information technologies is intended for the pursuit of HMRDC's business goals and its administrative functions and shall not be used for personal commercial reasons or any other unauthorized use.

2. A computer username and password is intended for the exclusive use of the person to whom it is issued and all responsibility must be borne by the person to whom a username is initially issued.

3. Users shall not attempt unauthorized access to computing resources either within the Company or outside.

4. Users shall use all systems in compliance with proprietary rights and be aware that, in addition to disciplinary action, as described in paragraph 16 below, any violation of proprietary rights will result in the liability of the user.

5. Users shall protect confidential or sensitive data and the computer equipment from theft.

6. Users shall not use, install, load or download any unlicensed commercial software or any unauthorized software. Non-commercial or personal commercial software must not be loaded unless approved by the information technology management.

(C) Administration

The CEO or any other officer nominated by him is responsible for the implementation of this policy.

8. Training and Communication

8.1 Management will ensure that all information, instruction, training and leadership necessary to ensure appropriate IT systems and equipment are provided for all employees that need them for their work. Training on IT equipment and software is part of employee induction for new employees and for employees that are moving to a new work place or role. Training on IT will be provided to employees when systems are changed or updated and at regular intervals to keep employees skills up to date.

9. Monitoring and Review

This policy will be reviewed for continued suitability from to time.

Chief Executive Officer