BEACH AUTHORITY

INTERNET, E-MAIL AND COMPUTER ACCEPTABLE USE POLICY

1.0 POLICY STATEMENT

The use of Beach Authority electronic systems, including computers, fax machines, and all forms of Internet/intranet access, is for authorised purposes only. Personal use of the electronic mail system or the Internet is acceptable provided that it is not excessive or inappropriate and, occurs during (lunch or other breaks), and does not result in expense or harm to the Authority or otherwise violate this policy.

Use is considered to be "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily duties. Electronic communication should not be personally used to distract, intimidate, or harass coworkers or third parties; or disrupt the workplace; or solicit or sell products or services.

1.1 Objective

The purpose of this policy is tooutline the acceptable and unacceptable use of the Authority's Information &CommunicationTechnology (ICT) facilities and resources as well as to comply with the applicable laws and policies.

This policy requires the users to manage responsibly the ICT facilities that are provided to them and to fulfill the missions and goals of the Authority, in order to maintain availability, integrity and confidentialityof information assets and protect the Authority against damaging legal issues.

1.2 Scope of Policy

The scope of this policy extends to all its personnel including employees, trainees, contractors, consultants, board members and affiliated third parties who use/access the Authority's ICT facilities and resources.

Users must not use technological assets to intentionally view, download, store, transmit, retrieve or communicate any materials, which are:

- Harassing or threatening;
- Obscene, pornographic or having any sexual contents;
- Defamatory;
- Discriminatory regarding race, age, gender, sexual orientation, religious or political beliefs, national origin, health or disability;
- Untrustworthy and fraudulent;
- Illegal or promoting illegal activities

- Intended for personal benefits;
- Facilitating internet gaming or gambling;

Use of the Authority's computers, networks, and Internet access is a privilege granted by management and may be withdrawn at any time for inappropriate use.The different acceptable use policy devised by the Beach Authority are described in **Chapter 2.0** below**.**

1.3 Review of Policy

This policy will be reviewed as and when required and deemed to be necessary by the Authority to ensure the appropriateness and the effectiveness of acceptable use policies and that it is always up to date. These reviews may result in the modification, addition, or deletion of acceptable use policies to better suit the Authority information needs and to ensure that any changes to the Authority's organisation structure and business practices are properly reflected in this policy.

2.0INFORMATION SECURITY MANAGEMENT SYSTEM ACCEPTABLE USE POLICY

2.1Security and Proprietary Information

Users must not try to access any data, document, email correspondence and programs regarding the Beach Authority for which they do not have the authorisation of the management.

Users must respect the confidentiality of other users' information and must not attempt to:

- obtain other user's login names or passwords.
- defeat or crack computer or network security measures.
- intercept or access electronic files or communication of other users without approval.
- pursue the files or information of another user without specific need to do so or prior approval from owner.
- destroy, or change data in such a way that it reduces the accuracy or reliability of the data.
- download, install or run security programs such as password cracking programs that reveal or exploit weaknesses in the security of the Beach Authority's Information Technology (IT) resources.
- violate copyright law, including but not limited to, illegally duplicating or transmitting copyrighted logos, pictures, video, software, etc.

2.2 Computing Assets

Employees are responsible for ensuring the protection of assets, such as computer devices, cables, laptops, external storage devices and printers that are assigned to them by the Authority. Laptops left at the Authority's office overnight must be securely placed in a locked drawer or cabinet. Any theft of assets must be promptly reported to management of the Authority.

Users manipulating mobile computing and communication facilities e.g. notebooks, laptops, external drives, tablets or smart phones are strictly advised to take special care to ensure that information regarding the Authority is not compromised.

All computers, mobile computing devices and workstations must be secured with a password-protected screensaver with automatic activation set to 10 minutes or less.Employees must make sure to lock the screen or log off when a device is unattended.

The management reserves the right to have access to all its computing assets in order to carry out regular checks/spot-checks and verification at any time.

2.3 Information Backup for Security and Recovery Purposes

Employees from all departments (to be determined as and when required) provided with external storage devices for information backup purposes. Heads of respective departments (where applicable)must ensure that:

(i) they regularly backup all information on their assigned storage devices on a daily basis.
(ii) storage devices are secured with a password provided by management and information backups, especially those containing confidential and restricted information, are kept safe and secure at an approved location.
(iii) information backups must be regularly tested to make sure that data recovery can be carried out following a hardware or software failure or any accident e.g. fire outbreak in office.

2.4 Handling of Information

2.4.1 Information on Screens and Printers

(i) Confidential information may be viewed on a screen by unauthorised persons in an office space. Staff responsible for handling confidential information on screens must therefore take appropriate action like setting passwords to lock screens to avoid access to unauthorized persons and disclosure of confidential information.
(ii) Printing, copying or exchanging any confidential data should be handled with utmost security to safeguard the confidentiality and integrity of information.

2.4.2 Disposal of Electronic Information

All Information must be properly retrieved and backed up prior initiating action for disposal of any storage devices.

Great care needs to be taken when permanently disposing of equipment containing storage media; all electronic data and software must be irretrievably deleted to ensure that information assets are not illegally disclosed. Electronic information must otherwise be rendered inaccessible prior to leaving the possession of the Authority.

In case a storage system is required to be returned to its supplier it should be securely erased before being returned unless contractual arrangements guarantee the secure handling of information found on the returned equipment.

2.5 Network Security

Users are advised to report any weaknesses in the network security system to the management so as to take necessary action.Weaknesses in computer security include unexpected software or system behaviour, which may result in unintentional disclosure of information or exposure to security threats.

The Authority will ensure that virus scanning software is available and regularly updated on every desktop and laptops. Users who receive a virus warning message must promptly notify the management or IT department to determine the authenticity of any potential threat and to take appropriate remedial measures.

Using the Authority's resources for intentionally introducing malicious codes including viruses, Trojan horses, spyware, etc is strictly prohibited and will lead to disciplinary actions taken by the management.

3.0 INTERNET ACCEPTABLE USE POLICY

This policy has been established to outline appropriate and inappropriate use of the Authority Internet resources, including the World Wide Web, electronic mail and the intranet.

Users of the Authority Internet resources are subjected to the following conditions:

- Not to send unreasonably large electronic mail attachments (2 Mb or more) in order to maintain the network performance.
- Not to download unlicensed and/or pirated software, music, songs, films and any unauthorized item.
- For security purposes, users should not share account or password information with other persons.

- Attempting to obtain another user's account password is strictly prohibited.
- Take all the necessary precautions to prevent unauthorized access to internet services.
- Not to participate in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging.
- Not to deliberately propagating any virus, worm, Trojan horse, or file designed to disrupt, disable, impair, or otherwise harm the Authority's networks.

4.0 E-MAIL ACCEPTABLE USE POLICY

E-mail is a vital tool at work as it is a valuable mean of effective communication which must be used with great diligence in accordance with the objectives of the Authority.

Hereunder are the followingconditions regarding the use of the e-mail service:

- E-mail access is granted by the management of the Authority through specific accounts provided to sections (where applicable) and passwords depending on the nature, scope and responsibilities of each department.
- It is the responsibility of the user to protect the confidentiality of their account and password information.
- Email users are also expected to abide with the normal standards of professional and personal courtesy and conduct.
- Users of e-mail account are expected to check their mailbox regularly in a timely manner as very often important official communications are being delivered via e-mail.
- E-mail users are responsible for their mailbox management, including organizing and cleaning.
- E-mail users are encouraged by management to acquire and share necessary information via mail in regard with their assigned duties.
- Use of e-mail for illegal or unlawful purposes, including copyright violation, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, imitation or soliciting is strictly prohibited.
- Confidential information or files should not be sent to other individual outside the Authority without authorized permission.
- Ensure that the total size of an individual e-mail message sent (including attachment) should be 2 MBs or less.
- E-mail users should be cautious regarding unknown or unsigned sources of e-mail attachments as it can be a primary source of computer virus.
- Sharing of e-mail account passwords with another person or attempting to obtain another person's e-mail account password is considered as an offence and it is strictly prohibited.
- There should be backup copies of e-mail messages to ensure system reliability and prevention of data loss.

- E-mail messages suspected to incompliance with applicable laws or this policy will be legally responsible for explanations.
- Email users are invited to report any suspicious e-mail received, users should not forward, delete or reply to the message, instead this should be immediately reported to the management.
- E-mail access will be terminated when the employee terminates their association with the Authority.

5.0 DISCLOSURE

Employees have a duty to report the following to management:

- obscene/illegal material found on a computer/laptop
- loss of Authority's data or loss of machines and devices containing Authority's data
- any downloading of illegal/obscene/offensive material
- suspect emails/email attachments/websites

6.0 Failure to Comply

Violations of this policy will be treated like any other malpractices at The Beach Authority. Allegations of misconduct will be sanctioned according to the Authority's in-house disciplinary measures and as per the laws of Mauritius. The sanctions may not be limited to, one or more of the following:

- Disciplinary action according to applicable Authority's policies;
- Suspension or Termination of employment;
- Legal actions according to ICT laws of Mauritius.

Acknowledgement

I have read and understood the above policy and agree to abide with all the conditions mentioned in them.

Name: …….. Signature: ……
(in BLOCK LETTERS)

Date: ……