The State Investment Corporation Ltd

SIC

Acceptable Use Policy

SIC ICT DEPT

Employee Information & Communication Technology Usage Agreement

Any employee who uses Information & Communication Technology (ICT) in the course of their work for The State Investment Corporation Ltd or SIC Group companies is required to sign this document before accessing any ICT system. ICT includes any PC/Laptop, network, Internet access, e-mail, telephone system, smart phones, fax/printer/photocopy/scanner and any other electronic equipment.

- Each user account creation should have a written request either through a request form or through e-mail from the manager of that department authorising its purpose and use.
- Employees shall use only accounts authorised by the head of department.
- Employees should access only those resources for which they are specifically authorised.
- Employees are personally responsible for safeguarding their account and logon information.
- No IT equipment/data/software owned by the SIC Group can be taken off-premises without prior authorisation from senior management.
- All portable computers should have a password either at boot level or operating system level to prevent unauthorised access to their contents.
- Non-SIC equipment should only be allowed on the premises of SIC prior to authorisation from the ICT Dept and senior management.
- Non-SIC equipment is not allowed to be connected to any system or network of SIC.
- Employees are not permitted to script their user IDs and/or passwords for logon access.
- Employees are not permitted to allow another person to logon to their computer using either their personal account, or using someone else's account. If any such need arises for urgent business matter, authorisation should be sought from management and ICT Dept should be informed accordingly.
- Employees should not leave their workstations logged onto the network while away from the equipment. Employees should either lock the workstation or log off when leaving for very short time periods.
- Installation of any unauthorised software is not allowed. Any installation should be authorised by the ICT Dept. SIC ICT Dept should uninstall any unauthorised software without prior notice or any permission.

Approved by: **I. Mallam-Hasham, Managing Director**

Signature:................................

Date:...........30/10/2012

Prepared by:

V Dumree, ICT Tech

- Employees should not remove, modify, erase, destroy or delete any computer software without the written approval in advance from the ICT Dept.
- Employees shall promptly report logon problems or any other computer errors to the ICT Dept.
- Employees shall promptly notify the ICT Dept if they have any reason to suspect a breach of security or potential breach of security.
- Employees should not move and/or change any computer hardware, data or software for any reason, without prior approval and/or guidance from the ICT Dept.
- Employees should not copy any data and/or software from any SIC resource for personal use.
- Employees should not make misuse of SIC printing, photocopy and fax equipment.
- Employees should not use SIC computer systems or networks for any of the following reasons:
    - Game playing, Watching movies online
    - Internet usage not required for their work activity
    - Downloading of files not required for their work activity
    - Any illegal activity
- Employees should not give out any SIC computer information to anyone.
- All data storage media shall be erased or destroyed prior to disposal.
- All equipment issued to employees should be returned in good condition to SIC upon termination of the SIC/employee relationship.
- Employees should not use SIC information technology to send or receive threatening, obscene, abusive, and sexually explicit language or pictures. Any use perceived to be illegal, harassing, and offensive or in violation of other company policies and existing laws can be the basis for disciplinary action.
- Employees are prohibited from causing SIC to break copyright laws.
- Storage Medias should be stored in cabinets when not in use, especially outside working hours.
- Employees should ensure security of their equipment. Example; office door should be locked when unattended.
- Only authorised people should have access to the IT Server Room.
- Employees should take good care of the equipment provided to them to ensure a high level of availability and integrity.
- Employees should not eat or drink near electronic equipment. Food and liquids spilled on such equipment can cause malfunction or other damages.

Approved by: **I. Mallam-Hasham, Managing Director**

Signature:...............................

Date:...30/10/2012...

Prepared by:

V Dumree, ICT Tech

- Employees should keep area around computer free so that fans and circulation of air are not hampered. This will prevent the computer to overheat.
- All users should abide to password policies.
- Access to the Internet and Mail services should strictly be done through the company's proxy server and e-mail server. The ICT Dept should decide otherwise depending on specific cases.
- Access to the Internet from a company-owned laptop and private connections must adhere to the same policies that apply to use from within company facilities.
- Employees should not allow family members or other non-employees to access company computer systems.
- All employees using email accounts provided by the corporation must include a company disclaimer as part of each message.
- SIC provides electronic mail to employees for business purposes. Users must not allow anyone else to send email using their accounts. This includes their supervisors, secretaries, assistants and any other subordinates.
- Any user suspected of misuse should have all transactions and material logged for further action.
- All users are strongly advised and it is their responsibility to regularly back-up important data stored on the local hard disk to CD/DVD or network directories allocated to them.
- Employees should not store any movie or music files on any network directory provided to them.
- Antivirus software should be installed on all computers by the ICT Dept. Employees should check on a daily basis if the antivirus software is up to date. Any issue should be reported.
- SIC reserves the right to review all employee email communications, use of SIC & Group property and Internet access. SIC reserves the right to review, audit, or monitor any information technology used by employees.
- Employees should be aware of Mauritius ICT laws: The Computer Misuse and Cybercrime Act, The Information and Communication Technologies Act, The Data Protection Act and the Electronic Transaction Act.
- Use of any SIC Information & Communication Technology implies acceptance to comply with all policy statements depicted in this document (Acceptable Use Policy) and SIC Group IT Security Policy Handbook. Employees who violate any of these policies shall be subject to disciplinary action.

Approved by: **I. Mallam-Hasham, Managing Director**

Signature:.........................

Date:..30/10/2012.........

Prepared by:

V Dumree, ICT Tech