General Conference
Southern Africa-Indian Ocean Division
Information Technology

27 Regency Road, Route 21 Corporate Park,
Nellmapius, Irene 0157 Pretoria, South Africa

PO Box 4583, RIETVALLEIRAND, 0174
Pretoria, South Africa

itsteering@sid.adventist.org
+27(12)345-7000

SOUTHERN AFRICA – INDIAN OCEAN DIVISION

COMPUTER USAGE POLICY

POLICY SUMMARY/INTENT:

The Southern Africa - Indian Ocean Division has adopted a Computer Use Policy, which outlines acceptable uses of computer equipment and electronic communication systems provided to employees. These requirements are in place to protect the employee and the SID. The policy detailed below applies to all employees and others who use SID provided equipment. This list summarizes some of the highlights but employees must read the complete policy and acknowledge having read the policy by submitting a signed copy to the IT Steering Committee.

- **While personal information may be stored on the equipment, employees should note that the SID has the right to inspect and monitor computer and network equipment, as well as internet usage, email and other electronic information and files for appropriate usage and content.**
- **All software installed on the equipment must comply with all licensing, copyright and intellectual property laws.**
- **Employees must ensure that SID equipment must not be used for outside business ventures, personal solicitation or for political campaigns or causes.**
- **Employees should ensure that confidentiality of sensitive information is protected at all times and storage, transmission or creation of illegal, inappropriate harassing or offensive material is not acceptable.**
- **Violation of this Computer Use Policy may result in disciplinary action.**
- **Definitions:**
  - Computer Equipment: Computer hardware, including the computer, and peripherals (such as printers, scanners, copiers and USB devices)
  - Electronic Communication Systems: System used as a means of sending and receiving messages electronically through connected computer systems (ie. Email, Instant and Text messaging etc.)
  - Hardware: Physical components of a computer system
  - Instant and Text Messaging (IM), blogging, social networks: A collaboration tool that allows real-time communication between two or more individuals
  - Malware: Any malicious software/program that is harmful to a computer system and includes viruses, worms, Trojan horses, and spyware
  - Mobile Computing Devices: Portable or hand-held computing devices including, laptops, notebooks, tablets, personal digital assistants (PDAs), pocket PCs and smart phones
  - Network: A number of computers connected together to share information and hardware
  - Sensitive Information: Information classified by information owners as confidential or restricted,
  - Software: A collection of computer programs, procedures and documentation that performs some tasks on a computer system

AFFECTED DEPARTMENTS/SERVICES:

This policy applies to all employees, contractors, consultants, temporary employees and volunteers. This policy applies to all hardware and software equipment that is owned by or leased to SID.

POLICY

A. SID Rights

1. Computer equipment connected to SID systems and networks must be owned by, leased to, or licensed to SID. SID may provide network services for unmanaged or non-SID devices where it deems appropriate. This includes but is not limited to setting up Wi-Fi Access Points, DHCP servers, port scanning, or other such network monitoring. Prior notification and authorization from the IT Steering Committee must be obtained.

2. Any equipment brought into the building, which interferes with business operations, will not be permitted. e.g. cordless phones as some use the same frequency as Wi-Fi; Wi-Fi Access points as it may interfere with SID's Wi-Fi environment.

3. The SID owns the rights to all data and files in any computer, network, or other information system used or owned by the SID and to all data and files sent or received using any SID system or using the SID's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. Employees must be aware that such information is not private and is subject to viewing, downloading, inspection, release, and archiving by SID as provided for elsewhere in this policy.

4. SID reserves the broadest right to investigate any activity, threat or potential violation of policy on any of its computer systems or networks to ensure that electronic systems are used appropriately and efficiently for the maximization of job performance. Access to, and use of electronic systems is intended to facilitate the business processes and legitimate business communication between users. To ensure appropriate use and information control, users are required to exercise good judgment in using electronic systems.

5. SID reserves the broadest right to inspect and monitor computer and network equipment, Internet usage, email, and other electronic information and files for appropriate usage and content consistent with business use. Users should have no expectation of privacy.

6. SID equipment must not be used for outside business ventures, personal solicitation, political campaigns or causes that oppose or contradict the mission and values of SID.

7. SID computing resources, software, systems and network must not be used to violate any local, state and/or federal laws. SID will cooperate with investigations by any legitimate law enforcement entity.

8. Computer equipment and networks shall never be used to create, display, store or transmit illegal, inappropriate, derogatory, harassing or offensive material.

9. Users must comply with all software licenses, copyrights and all other state and federal laws governing intellectual property, copyright, trade secret, patent, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the SID.

    a. Unauthorized copying of copyrighted material including but not limited to, digitization and distribution of photographs, from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the SID or the end user does not have an active license is strictly prohibited.

    b. The SID assumes no liability and will hold the offending employee(s) responsible for the consequences of any prohibited use of computer equipment or of any unauthorized use of software on SID equipment resulting in any loss, cost, expense, legal action or liability including, but not limited to, any claim of or liability for any infringement upon or any violation of any patent, copyright, trade secret or any other proprietary right of any third party.

    c. SID reserves the right to require that any software or hardware be tested by the IT Steering Committee before installing on, or attaching to, SID computer equipment and networks.

    d. Incidental personal use of SID computer resources may be permitted providing it does not consume more than minimal resources, interfere with worker productivity, pre-empt any business activity or violate any SID policy.

B. Sensitive Information and Confidentiality

Employees shall maintain the confidentiality of sensitive electronic information including personal information i.e. ID numbers, credit card info, passport and visa info, in the creation, handling, transmission, storage and destruction of such information stored on, or transmitted over SID computer equipment

and networks. This type of information is only available via a secure connection to the network servers. Any exceptions must be made to the IT Steering Committee and only stored on an encrypted device. This type of information should only be maintained where absolutely necessary and as part of one's job requirement.

a. Prior to the release of any personal or sensitive information for any reason unless required by law, or in the course and scope of employment related functions, the permission of the individual whose information is being released must be obtained.

b. Computer monitors and screens shall be positioned to reduce the visibility of sensitive or confidential information by unauthorized individuals.

c. Sensitive information shall not be transmitted to, or stored on personal desktop or mobile computing devices without prior approval by the IT Steering Committee.

d. To avoid loss, all sensitive information must be stored and/or replicated on SID servers.

C. Security

Security starts with each individual. Security products provide effective theft deterrents and access controls, but ultimately it is up to the individual users to prevent laptop theft. Individuals need to be particularly careful in public locations, such as airports, hotels and conference centers, and take appropriate steps to ensure someone does not try to steal their machine. An individual needs to understand the sensitive nature of their data, the cost of its loss and the potential risk of this data being accessed. Laptop users are encouraged to contact the IT Steering Committee to discuss these security issues and preventative measures.

1. Appropriate malware protection software approved by the IT Steering Committee shall be active on all computers and mobile computing devices at all times other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network. Any exceptions to this policy must be explicitly approved by the IT Steering Committee.

2. Each user shall be given an individual username and password.

    a. Each user is responsible for ALL actions associated with this username.

    b. Each user shall ensure this password is not shared, revealed or "allowed to be discovered" due to carelessness.

    c. If a user shares their password with another employee who has been assigned to temporarily carry out the tasks of the employee, it is the responsibility of that user to change the password immediately upon completion of the work or assignment by the employee.

3. Unattended computers must be locked, logged out or the password-protected screensavers must be activated to secure the computer or mobile computing device.

4. Any computer equipment and mobile computing devices, which accesses corporate data, shall have inactivity timeouts no greater than (30) thirty minutes.

5. Any unauthorized activity may be treated as a hostile attack against SID. Employees must not knowingly attempt to disable, defeat, overload, or circumvent any enterprise security implementation. Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to, access data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purpose of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Port scanning or security scanning is expressly prohibited unless prior permission is obtained from IT Steering Committee. Executing any form of network monitoring which will intercept data not intended for the employee's host is prohibited, unless this activity is a part of the employee's normal job/duty.

6. Users shall promptly report computer policy breaches and security threats against SID equipment and information to the IT Steering Committee.

7. Users must not attempt to bypass or subvert, or assist others in bypassing or subverting, content filtering, electronic mail filtering, firewall, software backup, screensavers, PIN's, transaction histories, computer virus/spam/malware protection software, or other security measures

which are put in place to protect the integrity of the SID computer/device environment without the explicit direction and approval from IT Steering Committee.

8. All SID owned laptops (Portable storage devices) must be encrypted using the IT managed encryption system. Laptops and portable storage devices that do not meet standards for encryption may be exempted from this policy by the following exemption specifications. By default, all SID laptops, regardless of what data they store, send, or receive, should be encrypted. Exemptions shall be considered on a case-by-case basis. Exceptions will be made where:

    a. The laptop operating system is incompatible with the encryption system.

    b. Applications running on the laptop are incompatible with the encryption system.

    c. Unacceptable system or application slowdown is caused by the encryption system.

    d. The encryption system causes other problems or possible issues resulting in unacceptable system behavior.

9. elf none of the issues above are identified, or if no other issues that would cause undue hardship or difficulty for the user of the laptop can be identified, the laptop must be encrypted using IT-managed encryption software.

D. Licensing, Software and Hardware

All computer software installed on SID computers must be owned by or licensed to SID. Deviation from these provisions shall have prior written approval from the IT Director.

1. The IT Steering Committee will not be responsible for, and not support any personally owned software installs, and setups but will assist in moving data. It is also the responsibility of the employee to keep such software current with the latest patches to address such security.

2. Users may not upload any software licensed to SID to any external device or location.

3. Personal or vendor equipment shall be connected to SID computer equipment, networks and systems only through authorized remote access solutions. Use of SID terminal services or SID approved web interfaces are pre-authorized remote access solutions.

4. Users who remove computers and mobile computing devices from SID premises shall be responsible for the physical safety of the equipment and its stored information.

E. Electronic Communication

1. Electronic communications containing sensitive information sent outside of the SID email system must be password protected. The password must not be part of the email and its associated attached file. A follow-up communication via email, phone, fax etc. is strongly recommended to communicate the password of the file, and subject to the provisions of Section B above.

2. SID electronic communication systems may not be used for unauthorized, inappropriate and/or illegitimate purposes. Inappropriate use includes but is not limited to: Pornography, sexual harassment, defamation and/or harassment, profanity, obscenity, derogatory remarks, unsolicited internal email messages, including the sending of "junk email or other advertising material to individuals who did not specifically request such material (email spam including but not limited to personal or advertising of local events/sales, department newsletters etc. Users must be given the option not to receive such emails.

3. An employee may not use personal e-mail addresses or systems to send or reply to business-related e-mail generated or received on any SID electronic system unless copies of such e-mails sent or received are also copied to the employee's assigned SID e-mail address. (Any email related to SID business must include the employee's assigned SID email address).

4. SID will maintain a systematic process for the recording, retention, and destruction of electronic communication.

F. Internet Access

1. SID uses monitoring software to categorize Internet sites for allowed and blocked access. If an inappropriate site is accidentally displayed or accessed, the user must disconnect from the site immediately.

2. When participating in online chats, newsgroups, forums, social networks or blogs, employees shall identify himself/herself honestly, accurately, and completely and disclose that such participation is personal rather than corporate.

3. Only employees duly authorized may post on behalf of SID.

4. The use and provision of the Internet is for business purposes and not for self entertainment.

G. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

AUTHOR: SID IT Steering Committee

APPROVED: SID ADCOM Action _____

EFFECTIVE DATE: 15 June 2012

I acknowledge receipt of the Southern Africa - Indian Ocean Division of Seventh-day Adventist Acceptable Computer Use Policy. I understand that it is my responsibility to read and comply with the policy, and that a violation of the policy may result in disciplinary action, up to and including termination. I further understand that my e-mail, voice mail and computer may be monitored at any time and I acknowledge that I have no personal privacy right to any communications sent or received through SID systems.

Employee Information		
Full Name		
Organization/Entity Name		
Mailing Address		
City	Province/State	Postal Code/Zip
Phone Number	Work Number	Email Address
Passport No./ ID Number		

Acceptance of Agreement

Organization Employee		Organization Representative	
Printed Name		Printed Name	
Title		Title	
Signature	Date	Signature	Date