INFORMATION TECHNOLOGY

POLICY AND PROCEDURES

A MANUAL FOR

"SAHARA FOR LIFE TRUST"

TABLE OF CONTENTS

Acronyms

Term	Description
IT	Information Technology
ASP	Assessment & Strengthening Program
LAN	Local Area Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
SOP	Standard Operating Procedure
WWW	World Wide Web
PC	Personal Computer
MIS	Management Information System
ID	Identification Document (login)
SNMP	Simple Network Management Protocol
Documentation	The system design, maintenance and support manuals
MAC Address	Media Access Control Address
DoS	Denial of Service
ICMP	Internet Control Message Protocol
QE	Quality Engineer
ARP	Address Resolution Protocol
Bootp	Bootstrap Protocol
SSH	Secure Shell

1. Policy Statement of "SAHARA For Life Trust" for Information Technology

The Information Technology (IT) resources and services of the organization are provided to the employees for enhancement of their productivity in their routine office work and to facilitate their interaction, coordination, communication and collaboration. Any access or use of IT resources and services that interferes, interrupts, or conflicts with these purposes, is not acceptable.

This Policy Statement provides notice of the Organization's expectations and guidelines to all who use and manage IT resources and services (including but not limited to computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, and physical facilities).

This policy also produces guidelines and minimum requirements governing the acceptable use of IT equipment and resources it may be modified at any time. It is the responsibilities of every computer user of organization to follow these guidelines, in letter and spirit to ensure optimum efficiency without compromising security of official information.

The policy will be reviewed from time to time in the light of actual experiences/comments of the end-user.

1.1 Purpose:

Information technologies (IT) are vital to any organization's operation. They are tools that improve the quality and efficiency of our daily routine work. They are the repositories for critical and sometimes highly proprietary corporate information. The improper access to or the destruction of these resources will have serious consequences for the organization. It is the purpose of this policy to:

- Ensure that the IT resources are appropriately protected from destruction, alteration or unauthorized access.
- Ensure that these protections are accomplished in a manner consistent with the business and workflow requirements of the organization.

1.2. Objectives:

The key objectives of using IT (systems, services and infrastructure) are to:

- Provide infrastructure to meet dealing requirements at all levels. That includes all hardware, software and Network access (Internet and Intranet)
- Provide required systems to improve efficiency in routine jobs. That includes automation and integration of various dealing processes at different levels.
- Improve interaction and collaboration among employees through the use of electronic communication tools e.g., email, messaging etc.
- Improve internal/external communication and access to information via internet and email services.
- Provide required services like assistance, helpdesk support and Basic IT skills training. This includes personal assistance or support via email or intercom/telephone.

- Provide assessment on IT equipment requirements and advice on procurement.
- Provide skilled IT personnel and assess training needs of the staff.

1.3. DEFINITIONS:

IT Systems: These are the computers, servers, printers, networks, emails, online and offline storage media and related equipment, software, website and web based information management systems, and data files that are owned, managed, or maintained by organization.

IT Department: Consists of one or more designated IT persons to manage and keep IT Systems functional and to determine who is permitted access to particular IT resources.

Management: Includes the designated staff that is responsible for ensuring compliance of IT users with this policy.

User: A "User" is a person who uses/accesses any or all of the above mentioned IT Systems owned by organization.

Intranet: Is the generic term for a collection of private computer networks within an organization. An Intranet uses network technologies as a tool to facilitate communication between people or workgroups to improve the data sharing capability and overall knowledge base of an organization's employees.

1.4. SCOPE:

This policy covers all employees, consultants, agents, and others working on any premises of **"SAHARA For Life Trust"** using any kind of IT services or equipment.

1.4.1. IT DEPARTMENT:

The IT Department will have administrative responsibility to:

- Take necessary steps to ensure smooth implementation of this policy
- Develop and maintain SOPs (Standard Operating Procedures) in accordance with the IT Policy.
- Ensure that the IT Policy and its prescribed procedures and developed SOPs are strictly adhered to by all concerned
- Provide necessary support and guidance to end-users to fulfill their routine duties.
- Install and maintain hardware, LAN/WAN & software applications etc.
- Create and manage Intranet, Internet, and email accounts where necessary.
- Develop and maintain inventory of all IT related equipment.
- Ensure security of all the systems by deploying necessary and up-to-date anti-virus programs, firewalls etc.
- Provide backup of crucial data from individual machines, shared folders and servers etc.
- Keep and Maintain records of all software licenses held by the organization and ensure their timely updating and renewal.

- Ensure timely maintenance, support and up-gradation of the entire IT infrastructure.

1.4.2. MANAGEMENT:

The management will:

- Implement Policy & Procedures and Issue clear and concise directives to the employees.
- Ensure that all concerned personnel are well aware of, and comply with the policies and underlying directives.
- Set appropriate standards, performance evaluation criteria, and control procedures designed to guide and provide reasonable assurance that all users observe these policies.
- Have proper and prompt coordination with the IT department to timely inform to initiate or revoke any account upon arrival or departure of an employee.
- Constitute an IT Compliance committee or focal person to investigate all violations of this policy to determine possible levels of applicable disciplinary actions.
- Devise penalty for misuse of the IT policy and procedures, and equipment (including hardware, software, network, Internet & email etc.)

1.4.3. USERS:

All users will:

- Meticulously comply with this IT policy and follow standards and procedures laid down by the management while accessing the organization's networking system
- Not misuse organizational IT equipment and resources in any way prescribed in this policy.
- Report any misuse, breakdown or IT related incidents to the designated officer in the IT Department or elsewhere.
- Read, understand, and seek guidance and clarifications from the designated officer(s) in the course of implementing and conforming to these policies and procedures.
- Strictly refrain from installing any unapproved, inappropriate, malicious or pirated software on the organizational systems or networks.
- Ensure that all important/sensitive data is regularly backed-up on separate and secure external media/drives.
- Follow security procedures to prevent fraud, waste, or abuse of the IT resources. Staff is authorized to use it only in conformation to security policies and procedures that minimize the risk.
- Not disable, remove, install with the intent to bypass or otherwise alter security settings or administrative settings designed to protect organizational IT resources.
- Be responsible for the protection of their accounts, and hence will not share passwords with any other person.

1.5. License Agreements:

- Only licensed software will be installed on the computers.
- IT Department will be responsible of installation/configuration of software. User will be restricted from doing so.
- Software license record will be maintained by the IT Department.
- Requirements for new software will be discussed in advance with the IT Department to assess detailed specification and implications.
- Software installed on the computers should be appropriate, licensed, and reliable.
- Copyrighted materials must not be transmitted without permission.
- Any problem/s with software will be reported to the IT Department.

1.6. Intellectual Property & Copyright:

As a condition of use of the Software, the employees must represent, warrant and covenant that they will not use the Software to:

- Infringe upon the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party;
- Violate any law, statute, ordinance or regulation;
- Disseminate information or materials in any form or format ("Content") that is infringing, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or
- Disseminate any software viruses or any other computer code, files or programs that may interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- Acknowledge that all content that s/he accesses through the Software is at his/her own risk and s/he shall be solely responsible for any damage to any part resulting therefrom.

2. Local Area Network Policy:

Following are some key procedures to use local area network:

2.1. Access Codes & Passwords:

- All users will require prior written approval from the Management on the System Access Request Form
- The designated officer of IT Department upon receipt of the approved System Access Request Form will create user accounts and passwords. Each user will be allocated a unique user name (ID) and user's personal password.
- Passwords will be unique with minimum of 5 characters (preferably alphanumeric).
- Users will set their PCs in a manner that the screen automatically gets locked after 10 minutes of being in idle state. They will also lock these when leaving their workstations.

2.2. PHYSICAL SECURITY:

- Each staff member will be responsible for the physical security of the officially assigned IT equipment by the organization.
- Staff members will be required to keep the IT equipment in safe and secure place when leaving the office.
- Such areas must be locked when not attended. Security guard may manage physical Access to the premises.
- Visitors to the area must have a valid business purpose and must be escorted by an authorized person.

2.3. ROUTERS SECURITY:

In order to protect the routers connected with the organization's network, the following procedures will be followed:

- The Graphical User Interface (also known as web interface) of the router must be password protected and accessible only by the IT Department.
- Only designated IT person is allowed to configure/reconfigure the router. Users must have explicit permission from the Management to access or configure this device.
- Wireless Internet is accessible to organization staff through Wi-Fi Protected Access Pre-Shared Key (WPA-PSK). WPA-PSK is basically an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password.
- Staff is not allowed to share the WPA-PSK with anyone outside the organization.
- Each Router must have the following statement posted in clear view:

  "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED". All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to the law enforcement agency. Authorized Users who utilize this device have no right to privacy.
- Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such become subject to disciplinary action.

3. INTERNET & EMAIL POLICY:

This policy provides guidelines on acceptable use of Internet access and e-mail service. The purpose of this policy is to ensure proper use of organization's email system by making users aware of what it deems as acceptable and unacceptable use of its Internet and email system.

3.1. ACCEPTABLE USE:

- Access to the Internet is intended primarily to assist staff to perform routine work.
- Staff will be allowed to make a reasonable personal use of organization's IT resources provided that they do so in their own time and it does not materially affect the amount of time required to devote to the organization.

- While being committed to the use of the Internet for business purposes, the organization expects from the users that they will abide with the security measures and procedures to minimize the risk.

3.2. UNACCEPTABLE USE:

The end-users will ensure that Internet or e-mail is never used for purposes that are illegal, unethical or unacceptable. Unacceptable and unethical use includes:

- Accessing chat rooms, playing games and using social networking sites during working hours.
- Communicating confidential corporate information to external sources without prior approval of the concern department.
- Personal contact credentials of employees to external parties without any prior permission.
- Any usage related to sexually explicit, libelous, harassing, fraudulent, defamatory or other offensive material.
- Infringement of organization's Equal Opportunities Policy or be in any way discriminating or harassing (whether sexually, racially, or because of disability, religious or other belief or otherwise)
- Statements or images of a pornographic, sexual or obscene nature.
- Sending or forwarding chain e-mails.
- Conducting a personal business using organizational resources.
- Anything which may result in financial or legal liability or which may damage the goodwill and reputation of the organization.

3.2. INFORMATION MONITORING:

- Monitoring system should be a mandatory part of IT infrastructure.
- All messages created, sent, or retrieved over the Internet are the property of the organization and may be regarded as corporate information.
- The organization reserves the right to access the contents of any messages sent over its facilities if the organization believes that there is a need to do so.
- All communications, including text and images can be disclosed to management or law enforcement agencies without prior consent of the sender or the receiver.
- Historical information is stored on each user's PC indicating which Internet websites were accessed. In cases of suspected misuse this will be checked and reported to the management for possible disciplinary action.
- The use of IT resources to be recorded and monitored is subject to management's discretion.

3.3. DOWNLOADS

Downloads from the Internet are not permitted unless specifically authorized by the management. Downloading of files from the Internet should be carried out only after asserting the following:

- Files origination is from trusted sources.
- Files are not for personal business use.
- Files downloaded should be properly scanned for viruses before being placed on a local storage media/drive.
- Appropriate preventive measures are taken to detect and clean any viruses that might be attached with the downloaded files.

3.4. EMAIL:

Email is the organization's prime means of communication. It is just like any other business record e.g., letter, memo etc. Therefore, it must be treated in the same manner just as any other business correspondence. The organization encourages employees to use this facility in a professional, ethical manner and in accordance with the organization's rules and regulations so as to best serve the communication requirements of the organization. Following policies will be followed for email usage:

- Ensure that all communications are for official reasons and that they do not interfere with an employee's productivity.
- Know and abide by all applicable organization policies dealing with security and confidentiality of organization records.
- Run a virus scan on all files received/downloaded through the Internet.
- Encryption, digital signature, and digital certificates must be used in order to ensure confidentiality, integrity and authenticity.
- Email facility will be offered to all concerned employees identified by management.
- IT department upon management's instructions will issue the user-name and password.
- Passwords will not be shared with other people except when necessary and will be notified to the IT Department and will be changed at least once every 60-90 days.
- Employees must ensure safekeeping of historical data (previous emails) and must maintain an organized mailbox by deleting all unnecessary and junk emails.
- IT department will install appropriate antivirus software on each machine to scan the contents of incoming and outgoing messages in order to prevent the spread of viruses, worms and other executable items that could pose a threat to the security of the systems.
- It is recommended that Microsoft Outlook is used for email access and mail records.
- It is recommended that only commonly used files e.g., doc, xls, ppt, PDF, GIF, JPG, BMP etc., are allowed for transmission through email. Emails with unknown file type attachments should be rejected by the system.

4. IT SECURITY POLICY:

4.1. GENERAL SECURITY INSTRUCTIONS:

- The IT department will list allowed software applications and users are restricted to use listed software only.
- Installation of pirated software on Workstations and Servers is strictly prohibited.
- Only authorized users will be allowed to use the Network and Internet.
- Removable Storage Media e.g., USB etc., may be blocked by the IT Department.
- Local administrator accounts must not be used by anyone other than the authorized administrator and such privilege may be blocked by the IT Department.
- External users are not allowed to use the Network and Systems unless authorized by management.
- Users are allowed to work on limited computer user accounts assigned by the IT department.
- Shared home directories on the Servers will be created for each user for storage of their important official files/data.

4.2. PHYSICAL SECURITY:

It is the policy of the organization to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. The directives below apply to all employees:

- Portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be kept under lock and key and also encrypted using at least 128 bit of encryption or more.
- Removable Storage Media e.g., Flash Drive, Compact Disc, External Hard Drive etc., should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS).
- IT Department is responsible for all equipment installations, disconnections, modifications, and relocations, so that employees are not supposed to perform these activities. This does not apply to temporary moves of portable computers (Laptops etc.) for which an initial connection has been set up by the IT Department.
- Employees shall not take shared portable equipment such as laptop computers out of the premises without the informed consent of their immediate supervisor. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may be caused to the equipment(s).

4.3. INTRANET SECURITY:

See IT Security Section.

4.4. INTERNET SECURITY:

See Internet Email Usage Section.

4.5. Virus Protection:

Since data is deemed as the most vital asset of the organization, it is therefore the policy of the organization to protect/prevent its data and information assets stored on computer systems from corruption or destruction by computer viruses by adopting the most appropriate means.

- Effective anti-virus software will be installed and maintained on all computer servers and personal computers.
- A firewall will be maintained to control suspect incoming data and downloaded material.
- Users will not be allowed to copy executable files, also referred to as applications (i.e., files whose names end with '.exe' or '.com'), or archived Zip files containing such files, onto any personal computer from any kind of external drive.
- Also they will not be allowed to load USB storage devices of unknown origin onto any computer. They will be required to scan all incoming USB devices for viruses before they are read.
- Any workstation suspected of virus infection, must immediately be brought to the notice of the IT Department and no work should be done on it unless the machine is fixed.
- Any person found knowingly introducing any virus on to any official computer system will tantamount to a serious offence liable for disciplinary action.

4.6. Internal & External IT Audits:

- Internal IT Audit will be conducted on a quarterly basis to review the compliance of security policy.
- External IT Audit will be conducted bi-annually, while a partial audit may also be considered for specific part of an IT Infrastructure such as security audit of the network or security audit of the agency specific software.
- Director Communications & Security will be responsible to conduct the information technology security audit.
- Security policy should be reviewed after six month in the light of recent threats.

5. Backup and Disaster Recovery Policy:

5.1. Purpose:

The primary purpose for the backup system is to provide for disaster recovery of key network servers and services (email, applications, databases, web pages, and servers hosting user's home and group directories).

5.2. General Information:

Backups can be scheduled to run after office hours. Recoveries can be done at anytime during the day when the backup system is idle. The earliest point in time that the backup system can recover a given file is from the most recent successful backup of that file. Several rare variables may prevent a file from being backed up successfully. These include, but are not limited to,

network outages, file corruption, or the file being in an "open" state when it's backup is being created. Backups fall into one of three categories:

- **Baseline** - A full backup of every file on a give network server.
- **Level** - A consolidation backup of any file that changed, or was created, since the last level or baseline backup.
- **Incremental** - A backup of any file that changed, or was created, since the last backup was performed.

5.3. Data Protection Principles

- Personal data should be processed fairly and lawfully.
- Personal data should be obtained only for the purpose specified.
- Data should be adequate, relevant, and not excessive for the purposes required.
- Accurate and kept up-to-date.
- Data should not be kept for longer period than is necessary.
- Data processed in accordance with the rights of data subjects under this act.
- **Security**: Appropriate technical and organizational measures should be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
- Personal data shall not be transferred outside the organization unless the individual ensures an adequate level of data protection.

5.4. Types of Disaster:

- Natural Disasters
- Man-made Disasters

Some types of disasters you should specifically plan for,, include:

- **Physical Break-ins**: Theft and/or destruction, terrorist attacks.
- **Remote Attacks**: Attempts to steal, destroy, or corrupt data, theft of service, Denial of Service (DoS), computer viruses.
- **Hardware Failures**: Malfunction of servers, databases, networks, and power outages.
- **Environmental Disasters**: Fire, flood, hurricane, etc. (Generally, all these result in power outages too)
- **Accidents (Human Error)**: File loss, DB record loss, data corruption etc.
- **Other Disruption**: Disgruntled employees, organized criminal activity, strikes, legal actions (e.g., shutdown orders), etc.

5.5. Data Backup/Replication:

IT department will ensure that all personal and identifiable data is recoverable in the event of accidental loss or damage. For this purpose, the following procedures will be followed:

- Ensure that all media containing organizational data is appropriately marked and labeled to indicate the sensitivity of the data.
- Individual users will be responsible of taking full system backup on regular basis as guided by the IT Department. This will include all data present/available on individual computers.
- External hard drives or personal network drives will be used as backup drives.
- Regular maintenance of the backup derives will be carried out to ensure that these are kept in good working order. When the back up is done, these drives will be kept in safe and secure place.
- In the event of an unsuccessful backup, the staff responsible for checking the backup will immediately note any messages/information on the monitor; record the failure in the backup log-sheet as well as any actions taken as a result thereof.
- The IT Department will validate the backup drive every three months, to ensure that the data can be fully restored from the drive.
- Drives will be replaced at the earliest sign of deterioration. Drives will be labeled to show age and due date for replacement as per manufacturer's recommendations. Old and discarded drives will be reformatted or physically disrupted so as to render any data on them unrecoverable.

6. IT SUPPORTS:

6.1. HELP DESK FACILITY:

Key duties and responsibilities of the helpdesk staff is to:

- Identify, diagnose, and resolve Level One problems for end users, and provide personal assistance or support via email or intercom/telephone.
- Deliver, tag, set up, and assist in the configuration of end-user PC desktop hardware, software and peripherals.
- Diagnose and resolve end-user network or local printer problems, PC hardware problems and mainframe, e-mail, Internet and Local-Area Network (LAN) access problems.
- Coordinate timely repair of PC computer equipment covered by third-party vendor maintenance agreements.
- Perform minor desktop hardware repair for PC computer equipment and peripherals that are not covered by third-party vendor maintenance agreements.
- Help install local area network cabling systems and equipment such as network interface cards, hubs and switches.

6.2. TRAINING:

For the end-users, the following computer-based training should be made available:

- **Team Leadership Training** – Covering Working Together, Manage Your Mind, Manage Your Words, Manage the Unspoken, and Putting Diversity to Work.

- **Team Development Training** – Includes Effective Meeting Skills, Increasing Employee Productivity, Mentoring, Team Leadership, Team Problem Solving, and Working Together.
- **Successful Management Training** – Includes Excellence in Supervision, Project Management, Giving & Receiving Feedback, Managing Disagreement, and Supreme Teams.
- **Basic IT Skills Training** – Basic training on "how to use a computer" includes PC, Operating system, peripherals etc.
- **Software Training** – Training on the custom developed applications for the organization.

7. IT POLICY IMPLEMENTATION:

7.1. COMPLIANCE:

- It is the responsibility of the IT Department to implement the IT policy and the management should issue directives and devise penalty for violation of any clause of this policy.
- The IT Department may intervene in helping and assisting end-users in any clarification, assistance or training, which might be essential in the implementation of this policy.

7.2. ACCOUNTABILITY:

Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may be caused to the equipment.

7.3. CONTRAVENTION OF THE IT POLICY:

- Computer users shall not, by any willful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Unauthorized access to a computer (sometimes called "hacking") or other unauthorized modifications to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences.
- The organization reserves the right to amend this policy at its discretion. In case of amendments, users will be informed accordingly.

7.4. PENALTY CLAUSE:

- Contravention of the organization's IT policy or any act of deliberate sabotage of computer systems may be considered a disciplinary offence.
- A physical damage caused to the IT assets may result in replacement or recovery and termination of contract depending upon the circumstances.
- Similarly, any breach of this IT policy may result in the dismissal of services as deemed necessary by the organization.