INFORMATION TECHNOLOGY POLICIES AND PROCEDURES MANUAL

SEPLAA Foundation

TABLE OF CONTENTS

1. POLICY STATEMENT FOR INFORMATION TECHNOLOGY

OVERVIEW

The Information Technology (IT) resources and services of the foundation are provided to the employees for enhancement of their productivity in their office work and to facilitate their interaction, coordination, communication and collaboration with people and other IT systems. Any access or use of IT resources and services that interferes, interrupts, or conflicts with the above mentioned purpose, is not acceptable.

This Policy Statement provides overview of the Foundation'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, as modified from time to time. It is the responsibility of every computer user of organization to follow these guidelines, to ensure optimum efficiency without compromising security of official information.

PURPOSE

Information technology (IT) is vital to any organization's operation. It comprises of the tools that improve the quality and efficiency of our daily routine work. It has 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.

OBJECTIVES

The key objectives of having the IT policy are to:

1. Ensure that the IT infrastructure meets the business requirements at all levels – including all hardware, software and Network access (both Internet and Intranet)
2. Ensures that employees have the required systems to improve efficiency in routine jobs.
3. Improve interaction and collaboration among employees through the use of electronic communication tools e.g., email, messaging, shared network space etc.
4. Improve internal/external communication and access to information via internet and email services.
5. Provide required services like assistance, helpdesk support and Basic IT skills training.
6. Provide assessment on IT resource requirements and advice on procurement.
7. Ensure the provision of skilled IT personnel and assess training needs of the staff.

SCOPE

The policy covers all employees, consultants, agents, and others personnel working on any premises of SEPLAA Foundation, using any kind of IT services or equipment.

DEFINITIONS

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

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 foundation.

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.

2. ROLES AND RESPONSIBILITIES

IT DEPARTMENT

The IT Department will have administrative responsibility to:

1. Take necessary steps to ensure smooth implementation of this policy
2. Develop and maintain SOPs (Standard Operating Procedures) in accordance with the IT Policy.
3. Ensure that the IT Policy and its prescribed procedures and developed SOPs are strictly adhered to by all concerned
4. Provide necessary support and guidance to end-users to fulfill their routine duties using IT systems
5. Install and maintain hardware, Local Area Network (LAN)/Wide Area Network (WAN) & software applications both on server and individual systems etc.
6. Create and manage Intranet, Internet, and email accounts where necessary.
7. Develop and maintain inventory of all IT related equipment.
8. Ensure security of all the systems by deploying necessary and up-to-date anti-virus programs, firewalls etc.
9. Establish mechanism for obtaining he backup of crucial data from individual machines, shared folders and servers etc.
10. Keep and maintain records of all software licenses held by the foundation and ensure their timely updating and renewal.
11. Ensure timely maintenance, support and up-gradation of the entire IT infrastructure.
12. Review the status of all IT System and updating of the record.
13. Create and maintain organization's website

MANAGEMENT

The management will:

1. Implement IT Policy & Procedures and Issue clear directives to the employees.
2. Ensure that all concerned personnel are aware of and comply with the directives.
3. Set appropriate standards, performance evaluation criteria, and control procedures designed to guide and provide reasonable assurance that all users observe these policies.
4. 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.

5. Constitute an IT Compliance committee or focal person to investigate all violations of this policy to determine possible levels of applicable disciplinary actions.

6. Devise penalty for misuse of the IT policy and procedures, and equipment (including hardware, software, network, Internet & email etc.)

USERS

All users will:

1. Comply with this IT policy and follow standards and procedures laid down by the management while accessing the organization's network and other IT resources.

2. Not misuse organizational IT equipment and resources in any way prescribed in this policy.

3. Report any misuse, breakdown or IT related incidents to the designated officer in the IT Department or management.

4. Read, understand, and seek guidance and clarifications from the designated officer(s) in the course of implementing and conforming to these policies and procedures.

5. Strictly refrain from installing any unapproved, inappropriate, malicious or pirated software on the organizational systems or networks.

6. Ensure that all important/sensitive data is regularly backed-up on separate and secure external media/drives as per policy

7. Follow security procedures to prevent fraud, waste, or abuse of the IT resources.

8. Not disable, remove, install with the intent to bypass or otherwise alter security settings or administrative settings designed to protect organizational IT resources.

9. Be responsible for the protection of their individual accounts thereby not sharing passwords with any other person.

10. Obtain written approval from their supervisor if they have to take the IT equipment (e.g. Laptop) outside the office premises, in that case user has to observe the following:

    - ✓ Do not connect to any open networks (wifi, intranets) which are not secure or might be prone to viruses.
    - ✓ Do not keep your sensitive organizational files opened where anyone can view or access it.
    - ✓ Keep your system locked if you are leaving it unattended. Shut down the system if you have to be away for more than 15 minutes.
    - ✓ Do not connect any secondary storage device e.g. USB Flash drives, DVDs which can harm your system.
    - ✓ Do not allow your family members or anyone else to access your system/account.

3. LICENSE AGREEMENT

1. Only licensed software will be installed on the computers.
2. IT Department will be responsible of installation/configuration of software on servers and on individual systems. Users are restricted from doing so.
3. Software license record will be maintained by the IT Department.
4. Requirements for new software will be discussed in advance with the IT Department to assess detailed specification and implications.
5. Software installed on the computers should be appropriate and reliable.
6. Copyrighted materials must not be transmitted without permission.
7. Any problem/s with software will be reported to the IT Department.

4. 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:

1. Infringe upon the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party;
2. Violate any law, statute, ordinance or regulation;
3. Disseminate information or materials in any form or format that is infringing, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or
4. Knowingly 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.
5. 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.

5. LOCAL AREA NETWORK POLICY

Following are some key procedures to use local area network:

SYSTEM ACCESS REQUEST EMAIL

1. All users will require prior written approval from the Management for obtaining Access to the System.

2. The User will write an email with Subject titled – "System Access Request "to immediate Supervisor.

3. The Email will specify user information vis-à-vis Name, Designation. Department & Joining Date and the level of Access required vis-à-vis creation of a new user account, new official email ID, Network Access, Internet Access & Printing Access.

4. The Supervisor will review/modify the request and after approval send the same to the designated officer of IT Department, who upon receipt of the approved System Access Request Email will create user accounts and passwords.

ACCESS CODES & PASSWORDS

Each user will be allocated a unique user name (ID) and user's personal password. Passwords will be created by using the following best practices:

- ✓ Password must contain at least 3 of the following 5 elements:
  - English uppercase characters (A-Z)
  - English lowercase characters (a –z)
  - Base 10 digits (0 – 9)
  - Non-alphanumeric (for example: !,$,#,or %)

- ✓ The password may not contain three or more consecutive characters from the user's account name.

- ✓ All passwords must be changed every 90 days.

- ✓ Passwords must be at least 8 characters in length. Users should avoid using the following while creating their passwords:
  - Birth dates;
  - Names;
  - Unaltered words that could be found in a dictionary, including non-English words and words spelled backwards;
  - Telephone numbers;
  - National Identity Card Numbers;
  - Famous or other proper names; and
  - Alphabet or keyboard sequences (e.g. "QWERTY").

- ✓ 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.

PHYSICAL SECURITY

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

Routers Security

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

1. The Graphical User Interface (also known as web interface) of the router must be password protected and accessible only by the IT Department.
2. 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.
3. 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.
4. Staff is not allowed to share the WPA-PSK with anyone outside the organization.
5. 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".
6. 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.

6. 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.

Acceptable Use

1. Access to the Internet is intended primarily to assist staff to perform routine work.
2. Staff will be allowed to make a reasonable personal use of organization's internet facility 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.
3. While being committed to the use of the Internet for official purposes, the organization expects from the users that they will abide with the security measures and procedures to minimize the risk.

Un-Acceptable Use

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

1. Accessing chat rooms, playing games and using social networking sites during working hours.
2. Posting anything on the social networking site that can harm the organization's reputation.
3. Communicating confidential corporate information to external sources without prior approval of the concern department.
4. Disclosing personal contact credentials of employees to external parties without any prior permission.
5. Any usage related to sexually explicit, libelous, harassing, fraudulent, defamatory or other offensive material.
6. 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)
7. Statements or images of a pornographic, sexual or obscene nature.
8. Sending or forwarding chain e-mails.
9. Conducting a personal business using organizational resources.
10. Anything which may result in financial or legal liability or which may damage the goodwill and reputation of the organization.

Information Monitoring

1. Monitoring system should be a mandatory part of IT infrastructure.
2. All messages created, sent, or retrieved over the Internet are the property of the organization and may be regarded as corporate information.
3. 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.
4. All communications, including text and images can be disclosed to management or law enforcement agencies without prior consent of the sender or the receiver.
5. Historical information is stored on each user's PC indicating which Internet websites were accessed. Furthermore the browsed history is also saved and accessible to network administrator through monitoring software, In cases of suspected misuse this will be checked and reported to the management for possible disciplinary action.
6. The use of IT resources to be recorded and monitored is subject to management's discretion.

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:

1. Files origination is from trusted sources.
2. Files are not for personal use.
3. Files downloaded should be properly scanned for viruses before being placed on a local storage media/drive.
4. Appropriate preventive measures are taken to detect and clean any viruses that might be attached with the downloaded files.
5. For any uncertainty about the downloadable content, user should contact the IT department before downloading that material.

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:

1. Ensure that all communications are for official reasons and that they do not interfere with an employee's productivity.
2. Know and abide by all applicable organization policies dealing with security and confidentiality of organization records.
3. Run a virus scan on all files received/downloaded via email.
4. Encryption, digital signature, and digital certificates must be used in order to ensure confidentiality, integrity and authenticity.
5. Email facility will be offered to all concerned employees identified by management.
6. IT department upon management's instructions will issue the user-name and password to the user to access the email. As a common practice, it is recommended that login may comprise of first letter of first name and the last name in full f e.g. account for Faiz Malik would be fmalik@xyz.org
7. Passwords will not be shared with other people except when necessary and will be notified to the IT Department.
8. Password will be changed at least once every 60-90 days.
9. Employees must ensure safekeeping of historical data (previous emails) and must maintain an organized mailbox by deleting all unnecessary and junk emails and taking the backup of their emails.
10. 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.
11. It is recommended to use Microsoft Outlook for accessing email.
12. 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.

7. IT SECURITY POLICY

General Security Instructions

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

Physical Security

1. 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:
2. Portable storage devices should be stored in a secure place when not in use. They must be kept under lock and key and also protected by password in accordance with the password best practices discussed in section 2.1. If they contain highly sensitive or confidential data, they should be encrypted using at least 128 bit of encryption or more.
3. 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.
4. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS).
5. 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.

6. Employees shall not take portable equipment such as laptops 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.

7. 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).

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.

1. Effective anti-virus software will be installed and maintained on all computer servers and personal computers.

2. A firewall will be maintained to control suspect incoming data and downloaded material.

3. 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.

4. Users will not be allowed to connect USB storage devices of unknown origin onto any computer. They will be required to scan all incoming USB devices for viruses before they are accessed.

5. 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.

6. Any person found knowingly introducing any virus on to any official computer system will tantamount to a serious offence liable for disciplinary action.

8. BACKUP AND DISASTER RECOVERY POLICY

Purpose:

The primary purpose for Backup and Disaster Recovery Policy is to provide mechanism for recovery of key network servers and services (email, applications, databases, web pages, and servers hosting user's home and group directories).

General Information:

Backups can be scheduled to run after office hours. Recoveries can be done at any time 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:

1. **Full Back up:** Full backup is a method of backup where all the files and folders selected for the backup will be backed up. When subsequent backups are run, the entire list of files and will be backed up again. The advantage of this backup is restores are fast and easy as the complete list of files are stored each time.

2. **Differential Backup**: Differential backup is a backup of all changes made since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. The result is a much faster backup then a full backup for each backup run.

3. **Incremental Backup**: is a backup of all changes made since the last backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changes made since the last backup. The result is a much faster backup then a full backup for each backup run.

Data Backup/Replication

IT department will ensure that all personal and identifiable data is recoverable in the event of any disaster, accidental loss or damage. Some of these events are:

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

For this purpose, the following procedures will be followed:

1. Ensure that all media containing organizational data is appropriately marked and labeled to indicate the sensitivity of the data.
2. 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.
3. External hard drives or personal network drives will be used as backup drives.
4. Regular maintenance of the backup derives will be carried out to ensure that these are kept in good working order. When the backup is done, these drives will be kept in safe and secure place.
5. 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.
6. The IT Department will validate the backup drive every three months, to ensure that the data can be fully restored from the drive.
7. 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.

9. CONTRAVENTION OF THE IT POLICY

It is the responsibility of the IT Department to implement the IT policy and the management will 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.

Contravention of the organization's IT policy or any act of deliberate sabotage of computer systems may be considered a disciplinary offence.

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.

A physical damage caused to the IT assets may result in replacement or recovery and termination of contract depending upon the circumstances. Similarly, any serious breach of this IT policy may result in the dismissal of services as deemed necessary by the organization.