TDEA Information Technology Manual

As Updated on: November 2014

Free and Fair Election Network (FAFEN) is a network of Pakistani civil society organizations, governed by the Trust for Democratic Education and Accountability (TDEA).

Contents

Purpose
The purpose of this policy is to outline the acceptable use of the TDEA network, computers, software applications and information resources. These rules are intended to protect TDEA, its clients, donors and employees. Inappropriate use of these resources exposes TDEA to security risks, damage due to computer viruses, denial of business-critical services and systems, adverse publicity, potential loss of business and the liability associated with violating the numerous contractual and regulatory requirements affecting TDEA and its employees.

Authority
Approved by the Board of Trusties.

Applicability
Applies to all TDEA & related projects 'staff, and guests using computer and communication technologies, including TDEA or the related projects' network, whether personally or Project owned, which access, transmit or store TDEA & its projects' information.

Policy Statement
Use of TDEA & related projects' networks and computer resources should support the basic missions and Business process, tracking; monitoring, evaluation & research Users are responsible to properly use and protect information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information resources, their safeguard disaster management and continuity contingency planning.

Summary
This policy covers the appropriate use of all information resources and lays out a basis for disaster recovery and continuity planning.

Section Headings:
- DEFINITIONS
- SCOPE
- POLICIES
- OVERSIGHT OF INFORMATION RESOURCES
- BACKUP AND BUISNESS CONTINUITY
- MISUSE OF INFORMATION RESOURCES
- CONSEQUENCES OF MISUSE OF INFORMATION RESOURCES

1. DEFINITIONS

As used in this policy:

- "Information resources" are all computer and communication devices and other technologies, which access, store or transmits DEAS, its Projects or related staff information.
- "Information" includes TDEA, its projects as well as staff information.
- Disaster management and continuity implies contingency planning to mitigate the effects of a catastrophic or an untoward event on the IT operations of the trust and its projects.

2. SCOPE:

This policy is designed to guide the staff in the acceptable use of computers, information systems, and networks owned by the TDEA, related projects & satisfy compliance. More

importantly, it is meant as an application of best practices to ensure availability, integrity, reliability, privacy, and confidentially of information systems, and networks. The policy is not designed to cover any situations and circumstances beyond the defined scope.

3. POLICIES:

3.1. General Policy

The computing and network resources and services owned by the trust are limited and should be used wisely and carefully with consideration for the needs of others. A user, by using computers, information systems, and networks owned by the trust implicitly assumes personal responsibility for acceptable use and agrees to comply with this policy, as well as applicable laws and regulations. Failure to uphold acceptable uses constitutes a violation of this policy and may be subject to disciplinary procedures. Users of the trust's resources must protect.

Their online identity from use by another individual, the integrity of computer based information resources, and the privacy of electronic information.

In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other information resource.

3.2. Access

Access rights must be authorized on a job requirement basis, i.e. users must be granted only the access rights they need to perform their jobs, and no additional access rights beyond that. This concept is called "least privilege"; which is a basic IT security principle implying that users should be given the least level of system access they need to do their work. Determination of access level rests with the head of respective departments and must be communicated to IT department initially as well as subsequently when access requirements change. Access rights must be revoked when the individual no longer requires access to the data to perform their job. If the user is a temporary employee, subcontractor or other non-TDEA employee, the manager who authorizes their system access is required to provide the IT Department with the expected termination date. The user's account will be made to expire automatically. However, authorized IT team may access information resources, but only for a legitimate operational purpose, namely support and help desk activities and backup.

3.3. Prohibition against Sharing User IDs and Passwords

Sharing an online identity (user ID and/or password) violates this policy. Every individual is responsible to safeguard their user name and password thus the logs, in case of an audit, are authoritative. Users therefore are urged to regularly change their passwords and avoid simple easily guessable passwords. The systems maintain a track of user activities which are logged against the user's login id.

3.4. Information Belonging to Others

Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.

3.5. Abuse of Computing Privileges

Users of TDEA and its related Project's information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by TDEA and its projects. For example, abuse of the networks to which the TDEA and its Projects belongs or the computers at other sites connected to those networks will be treated as an abuse of the trusts computing privileges.

3.6. Usage

Use of the trust's information resources must comply with the following:

3.7. Prohibited Use:

Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or TDEA policy.

3.7.1. Copyrights and Licenses:

Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the TDEA information resources is a violation of this policy.

3.7.2. Social Media:

Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.

3.7.3. Political Use:

TDEA information resources must not be used for partisan political activities.

3.7.4. Personal Use:

TDEA information resources should not be used for activities unrelated to appropriate TDEA functions, except in a purely incidental manner.

3.7.5. Commercial Use:

TDEA's information resources should only be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages when directly related to TDEA activities. TDEA's CEO will determine permitted commercial uses.

3.8. Integrity of Information Resources

Users must respect the integrity of information and information resources

3.8.1. Modification or Removal of Information or Information Resources

Unless proper authorization, users must not attempt to modify or remove information or information resources that are owned or used by others

3.9. Other Prohibited Activities

Users must not encroach, disrupt or otherwise interfere with access or use of the TDEA's information or information resources. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of TDEA information or information resources. "Information resources" are all computer and communication devices and other technologies which access, store or transmit the projects' or its related staff information.

3.10. Locally Defined and External Conditions of Use

Individual units within the TDEA will define "conditions of use" for information resources under their control and have the right to establish more restrictive policies and procedures governing their use. These Usage conditions must be consistent with this overall policy but may provide additional detail, guidelines restrictions, and/or enforcement mechanisms.

When such conditions of use are implemented, the individual units, (e.g. Finance) are responsible for publicizing and enforcing both the conditions of use and this policy. Where use of external networks is involved, policies governing such use are also applicable and must be followed. Responsibility for, and management and operation of, information resources is delegated to the head of a specific subdivision of the TDEA governance structure ("department"), such as a Director, Manager, Administrative Department head etc. Such persons will be responsible for compliance with all TDEA policies relating to the use of information resources owned, used or otherwise residing in their department

3.11. Access for Legal and TDEA Processes

Under some circumstances, as a result of audit or compliance, TDEA may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties.

Additionally, the TDEA may in its reasonable discretion review information records, e.g., for the proper functioning of the TDEA to protect the safety of individuals, the trust itself or the trust's community. TDEA may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to TDEA.

4. OVERSIGHT OF INFORMATION RESOURCES

- Users of computing resources must be aware that although many computing facilities provide and preserve the security of files and passwords, security can be breached through actions or causes beyond the reasonable control of the facility. Users are urged, therefore, to safeguard their data, to take full advantage of file security mechanisms, and to change account passwords frequently. Users of email systems must also be aware that e-mail is not a secure form of communication by default. Sensitive confidential information therefore should not be distributed via email.
- All e-mail systems operated by the TDEA, either intended for the business of TDEA or in the performance of contractual obligations for a client/ donor, are the property of TDEA. Users of these email systems should have no expectations of privacy related to their use of these systems. TDEA reserves the right to access any e-mail content residing in any of its e-mail systems, for any TDEA business or IT security purpose, unless such access is prohibited by local laws.

- The IT Department will respect and strive to ensure users' privacy and intellectual property while managing the computing and network infrastructure and information application transactions and data. The IT Section does not actively monitor network traffic or view content. However, while researching computing and/or network issues, IT staff may need to use tools or utilities that expose content or users' internet habits.
- At times the IT Section may need to reconfigure network and/or computing resources to mitigate situations that negatively impact access to IT resources. These actions include, but are not limited to, temporarily disabling access to an individual system, temporarily disabling access to/from a specific segment of the LAN or modifying priorities. Though rare and short in duration, these steps are necessary to isolate problems and enable a quick resolution.

4.1. Responsibilities

The system administrator is responsible for managing and operating information resources in compliance with TDEA and department policies, including accessing information resources necessary to maintain operation of the systems under the care of the system administrator. (System administrator should refer to the line supervisor for access beyond that necessary to maintain operation of the system.) The system Administrator will maintain the following logs:

- Data Backup & Restoration
- Printing
- Network & Internet usage
- Down times and the reasons thereof and will produce such logs for audit, reference, billing & related procurement purposes.

The system administrator will take all “appropriate actions” to protect the security of information and ensure business continuity & disaster recovery.

The cornerstones of “appropriate actions” encompass:

- Prevention
- Protection
- Detection/Investigation
- Incident Assessment and Damage Control
- Recovery

The System Administrator will:

- Take precautions against theft of or damage to information resources.
- Faithfully execute all licensing agreements applicable to information resources.
- Communicate this policy, and other applicable information use, security and privacy policies and procedures to their information resource users.
- Ensure employees do not have unrestricted access in the system nor should they be permitted to introduce unauthorized changes made to the system.
- Ensure a central authentication mechanism, resource sharing and access to information resources
- Ensure only licensed software (AnnexA) is used and will regularly check users' computer for unwanted installations on the basis of the check list (Annex B) which will be pasted at a visible location in users' cubicles/offices
- Ensure that there is no Unauthorized (Refer AnnexA) and unproductive software like UTorrent, hotspot shield, gaming software’s and Skype on users systems.

- Will conduct regular training sessions for the end users to educate them with regards to available services, their optimum usage, backup plan and recovery measures.

4.2. Suspension of Privileges

System administrator may temporarily suspend access to information resource if he believes it is necessary or appropriate to maintain the integrity of the information resources under his oversight.

4.2.1. Physical Security

The System administrator is responsible for physical security of equipment under his direct supervision. This includes all equipment housed in the data center/server and all network active and passive devices in the TDEA & related projects' offices. Physical security of any IT equipment including Laptops and Desktop Computers, once issued is the responsibility of the users. Laptops or any other IT equipment can only be taken off premises if a written approval from the Administration is granted.

- The Data Center must be equipped with locks to limit access, and those access devices must be properly assigned and accounted for.
- Three Keys to the server room/data center and other IT equipment cabinets will be maintained. One key must be securely kept with the Administration department and other two keys shared between the System Administrator and the line supervisor.
- Access log to the server room will be maintained & should contain at least the signatures of individuals who are not regularly on duty in the server room System Administrator will put in place mechanisms to determine how any unauthorized hardware components added to the network would be detected.
- The Server Room & the area immediately surrounding the Server Room must be free from combustible materials & servers and critical network devices must be protected by AnUninterrupted Power Source (UPS) to ensure smooth transition of operations in the event of power failure & guard against sparking due to voltage alteration.
- Desktop and laptop computers must be secured with a password-protected screen saver, approved and installed by the IT department, with a maximum automatic inactivity activation of 15 minutes.
- Individuals must not attempt to disable the password-protection on their unattended workstations when accessing confidential or sensitive information. Individuals must not attempt to access information for which they lack authorization. Anyone having knowledge of such attempts, or other security breaches, must notify their supervisor or their local IT department.
- Depending on contractual agreements, users may be required to sign Non-Disclosure Agreements, Data Usage Agreements or Security Pledges before receiving access rights to sensitive data.

4.3. Back up, Disaster Management and Business Continuity

& its projects' data encompasses any electronic data which directly supports Business operations. While the System Administrator will take necessary steps in light of this manual to regularly back up users' data, users are well advised to be proactive & always take measures to safeguard their own operational and critical data in extreme case scenarios as the worst

effete of a critical data loss is to the operations of the concerned unit itself. The backup policy itself encompasses only electronic data on the trust's owned computers. This does not include data in personal computing devices, any personal data, sub-contractors or any other electronic data which is not pre- declared by the users as critical “TO BE BACKED UP” data. Any new application or data not pre-declared will not be backed up and will be the direct responsibility of the relative section head. The trust's data is classified into four main categories in the order of priority and risk factor:

- Information Systems.
- Staff Emails including attachments.
- All pre-declared official electronic data of the end users.
- TDEA and its related PROJECT’s Websites

4.4. Information Systems

Information Systems directly support TDEA functions and constitute the most critical piece of TDEA operations. The Director IT is the custodian of the Privacy, Security, Integrity & flawless Continuous operations of the Information System under the direct supervision of the CEO. The Information system and the information therein will be managed as follows:

4.5. The Core Operations:

- The Information Systems must enforce segeration of user rights and roles
- Tracking, Feedback Loop & Anti Tamper Mechanisms must be in place & complete transaction trail must be visible to the respective owners of the data.
- User driven & and friendly reporting interfaces.

4.6. Access Rights:

Multiple types of access rights exist in Information Systems with the most important being:

- View Only
- Insert information
- Update information

The general flow of the permissions and roles follow:

The grant of access rights to the all information systems will be a segregated operation with the project head being the authority for the provisions of the access rights and roles to the users. Respective information system managers will only grant access rights, to the level desired, and for the duration of the exercise. It is the responsibility of the end user [TDEA Staff] to update about the completion of a said task where after, the permissions will be immediately revoked.

4.7. Historical View:

Information Systems will always maintain “States” stored indefinitely for back tracking and transparency

4.8. Segregation of Duties:

The handling of Information Systems will be a segregated operation with the access of rights applicability already detailed above.

4.9. Change Requests:

Information systems, the information they capture and represent are only as good as the domain specific information provided by the users of the system. Unit heads, therefore, must provide timely & distilled information in the form required by the development teams.

All feature based, functional, view or reporting additions and changes will be handled via change requests – Each change request would be handled on an individual basis as the time and resources involved in implementation will vary based on the requirements. All change requests will be routed through the Director IT. Direct contact with the developers must be avoided.

4.10. Data Owner Ship:

The IT department is directly responsible for development, deployment and maintenance of Information systems. They do not and cannot claim to be the “owners” of the data contained in the systems. The validity, integrity & accuracy of the data being populated in the systems is the responsibility of the user entering the data. IT personnel will not enter/update/delete any data in the system/website on behalf of end users. End users must ensure that they use difficult passwords and refrain from sharing password or related information with others to avoid any untoward situation. In case of a breach, audit logs against the user and the ip address will be authoritative.

The ownership of the data is of the concerned unit who is responsible for ensuring that the data is always up todate as required by the business objectives.

4.11. Continuity:

Pre-emptive measures to ensure business continuity will be put in place in case of an untoward incident t/disaster. Possible situations which may compromise the IS operations include but are not confined to: a Fire Hazard, b. Terrorists Attack, c. Natural Catastrophe, e. Hardware Failure.

4.12. To mitigate the affects

Full backups of the system [Database, Software, Files] will be taken on a daily basis at midnight and stored on:

- Local Disks
- External USB drives
- Back up Severs
- Synced with off-site storage at TDEA/Projects' offices

At least one hot backup/Standby/Replica will be maintained in house 24/7 and synced with designated master servers on an hourly basis i.e. in case of a localized, electronic disaster the total difference of data loss will be the data uploaded/transactions committed in one hour.

4.13. Staff turns over:

Staff turnover must not jeopardize the Information Systems operations in any way. To achieve this end, the following focus will be maintained:

- The building block of the systems will be modular and layered.
- The chosen development environment will be such that its expertise is readily available in the market.
- There will always be more than one individual handling the operations of the Information Systems at any given time.
- The Information Systems will be technically documented and handed over to the CEO.
- All the passwords to the systems will be written down in a sealed envelop and handed over to the CEO.

4.14. Software failure

A development environment/server will be extended to the developers to write, test and debug the code. Only a piece of code which has been thoroughly tested will be uploaded on the production environment. In case of buggy software finding its way to the production server, milestone backups will be restored to mitigate the damage.

4.15. Restoration Drills

All backed up data will be restored on test environments on a weekly basis and logs shared and incidents documented

4.16. Acceptable Downtime

Acceptable downtime in case of any untoward incident shall not exceed 3 working hours.

4.17. Enhanced Bandwidth

In order to avoid bandwidth starvation during critical phases enhanced bandwidth will be acquired from the service providers.

4.18. Incident Reporting:

Any incident relating to a system breach or unauthorized data/system access/handling will be documented and immediately brought to the notice of the CEO. The logs will be preserved and depending on the decision of the CEO, an investigation into the incident will be carried out the findings of which will cover reasons of occurrence and mitigation in future.

The following relates to sub Para 2,3 & 4 of the data classification

- Multiple copies will be managed in house (Server Rooms and IT rooms or, TDEA & project offices.
- The System Administrator will download and maintain PSTs of users' emails to avoid data loss in case
- of server crash/untoward incident. Multiple copies of PSTs will be maintained in multiple locations
- In case PSTs are not available the Network Administrator will physically visit each staff member and download the emails from the web client. The downloaded archive will be

password protected and kept safely in NAS and other backup devices. The network administrator will maintain the backup history and share the backup plan with all staff one week prior to the physical backup

- Users will save official data in non-windows drive (D, E etc.). No official and operational data will ever be stored in C: drive.
- All data must be saved in user named folder e.g. (D:\Waqas).
- Only the data stored in the aforementioned user specific folder will be backed up by the IT section.
- The System Administrator will implement daily, weekly and monthly backups which will include incremental and full backups. Backups must be restored on test computers to validate backups and accuracy of data backed up.
- Data stored in the NAS drive will be password protected.
- All data on every other device will be encrypted.
- Critical data stored in TDEA and its project servers will be securely copied onto off-site storage. Copies of the data will also be maintained in-house.
- All passwords to all resources will be written down and sealed in an envelope and submitted to respective project heads. Any changes in the passwords must be updated and submitted in a new envelop accordingly.
- Hot backups and replica copies will be maintained. In case of a critical service being compromised, the standby must take over with minimum downtime.
- Multiple connections to the Internet will be maintained at all times and failure of one link sho uld not compromise service delivery with automatic fail-over.
- Network traffic & servers' health management software will be installed and monitored 24/7 by the means of automated alarms whenever a threshold or a traffic pattern is breached.

5. MISUSE OF INFORMATION RESOURCES

Besides explained elsewhere in this document, the misuse or unacceptable use includes any activity that is illegal under local, federal or international law while using the trust's resources; violations of sexual harassment, hostile workplace, export, copyright, patent or other intellectual property laws; introducing malicious programs into the TDEA's computer network; attempting to breach system or network security; attempting to access unauthorized data or information; security scanning, port scanning or network monitoring that is not job related; interfering with other users' access to resources; using TDEA resources for personal gain or profit, or to serve the interests of other organizations without TDEA approval; and any activity that might adversely affect TDEA ability to maintain the confidentiality, integrity and availability of client, donor and TDEA data and computing resources.

6. CONSEQUENCES OF MISUSE OF INFORMATION RESOURCES

A user found to have violated this policy may also have violated the Code of Conduct & TDEA policies, and will be subject to appropriate disciplinary action up to and including termination on repeated violations. Contractors, consultants or others violating this policy will be subject to loss of network privileges and the possible abrogation of their contract.

6.1. Annex-A

Operator:

- Microsoft Windows 7 Professional (Service Pack1)
- Microsoft Office Professional Plus 2010.
- Antivirus (AVG Anti-Virus Free Edition S)
- Readers (Adobe , Foxit)
- Browser (Mozilla Firefox and Google Chrome).
- Printing and Scanning Software's.
- Compression software's (WinRAR).
- Document Converters (Free Pdf to word, excel converter).
- Designing Software's for IT or Relevant Department (PHP, HTML and Graphic.)
- Quick Book software for Finance.
- Backup software (Cobian)
- any other software duly authorized for business purposes. Respective Manager MIS will be the authority

6.2. Annex-B

Operator:

- BIOS password in place
- Dual operating system.
- User Account (Standard).
- User Account (Administrator for Backup).
- Genuine Windows and Microsoft Office check
- Antivirus.
- Browser
- PDF Reader.
- Printer Drivers.
- Backup Settings
- Unauthorized Software
- Start Up Services
- Email Backup
- Documents Backup
- protected screen saver element

6.3. IT User Guidelines

6.3.1. Acceptable Use:

- All network and computer resources are TDEA property and are to be used for business purposes serving the interests of the TDEA and its clients/ donors.
- All data stored on TDEA systems remains the property of the TDEA. While the organization makes every effort to maintain privacy of e-mail and data, TDEA cannot guarantee confidentiality.
- Incidental personal use of network resources is permitted. However, authorized users are
-

- expected to exercise good judgment regarding their occasional personal use of these resources. Such personal use must not consume excessive IT resources, degrade the performance of the network or connections to the Internet, or result in incremental cost to the organization. Examples of excessive use are downloading large libraries of music files (MP3) and movies for personal use (this includes copyright issues as well), storing large amounts of personal content on file servers intended for business use, or watching movies/ videos for personal entertainment that are broadcast over the Internet during work hours.
- Network resources and e-mail accounts are for business purposes. Incidental personal use may not involve any activity that would reflect badly on TDEA (e.g. spamming, harassment).
- Personal use should not include: installing personal software on project machines, joining personal machines to the project network, borrowing project machines for vacation use, or the use of any pirated software on project networks.
- Employees should cooperate with the IT organization in keeping their anti-virus software updated and refrain from activities that might infect TDEA computer with viruses.
- Unacceptable use includes any activity illegal under local or international law; violations of sexual harassment, hostile workplace, export, copyright, patent or other intellectual property laws (e.g. software piracy); using TDEA resources for personal gain or profit.

6.4. User Guidelines

Computer and network resources are essential for the work of TDEA and are purchased and installed for work purposes. As an employee or consultant of TDEA it is a privilege to use the resources in the offices and a responsibility to use them carefully. Here are guidelines that will help keep the network free of viruses and other problems.

- Log on and off the computer in a standard manner.Turnoff the computer at the end of the day.
- Learn to recognize viruses and hoax emails as they appear in your account. Do not open an
- Use a password and do not share it or let others use your account. Change the password every 6 months.
- Learn to recognize viruses and hoax emails as they appear in your account. Do not open an email from someone whose name you do not recognize, especially if there is an attachment on the email. Notify Information Systems department of suspected virus activity.
- Backup your work regularly by saving it to the correct network drives. If you are working in a non- networked environment, backup your data to a CD each week. Get guidance from Information System department in this regard as you will be the most affected party in the event data that you manage is lost.
- Do not install personal programs on a work computer without permission from the CEO through Information System department.
- Do not download unnecessary or illegal programs and files from the Internet including games, pictures, cracked programs, or pornography. Viruses and spyware that can be introduced into the office computer and network often accompany these files.

- Do not allow non-project employees to use computers. Lock your door or computer when you are away from your desk.
- Employees who use sensitive company data on their computers should limit access to such files via password protection. This type of information includes (but it not limited to) payroll, budgets, work plans, contracts, HR / employee data, Financial software files, etc. Passwords should be changed regularly.
- Ask for help if something goes wrong with the computer and follow the instructions of the MIS department when help is given.