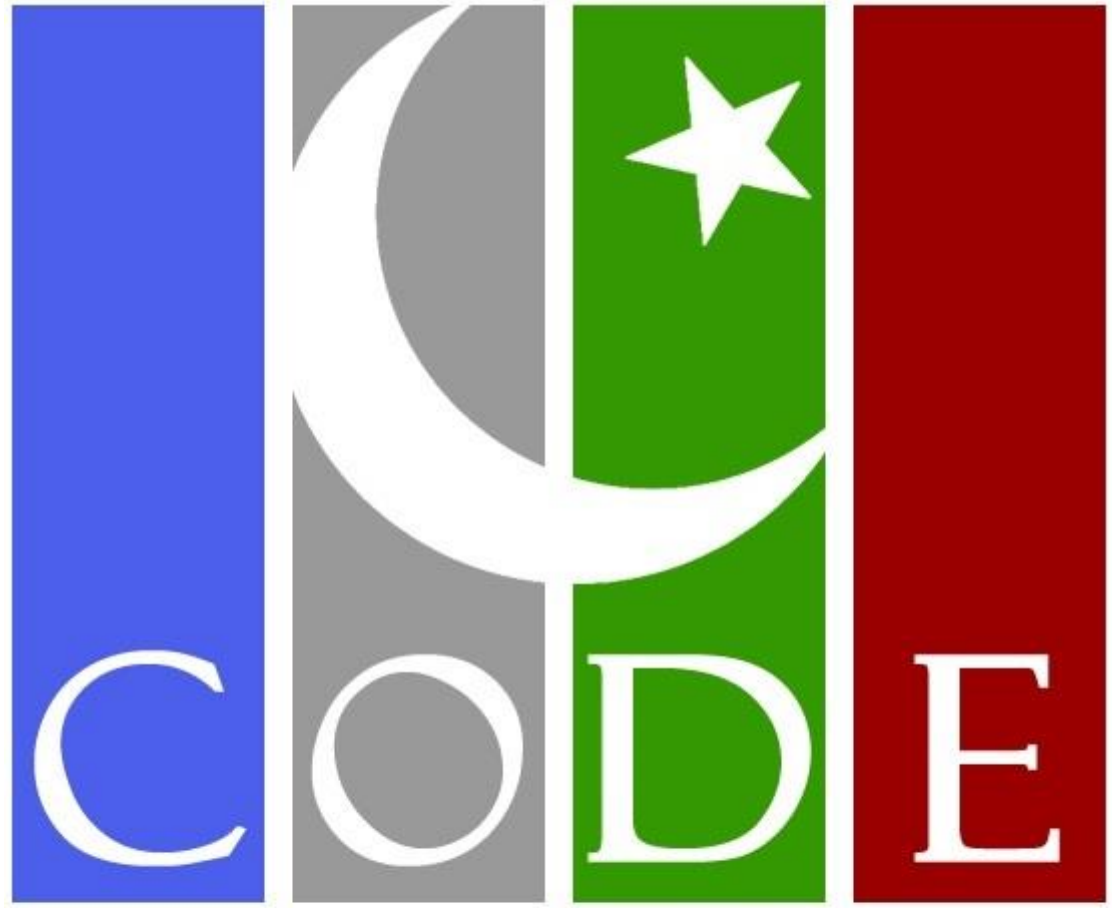
IT POLICY



CURSOR OF DEVELOPMENT
AND EDUCATION PAKISTAN

CODE PAKISTAN

2023

INFORMATION TECHNOLOGY POLICY

1.0. POLICY STATEMENT 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 business 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 business 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 an organization using any kind of IT services or equipment.

1.5. 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.)

1.6. 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.

1.7. 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.

1.8. 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.

- 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.

1.9. INTERNET AND 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.

1.9.1. 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.

1.9.2. 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.

1.9.3. 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.

1.9.4. EMAILS

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. As a common practice, it is recommended that login may comprise of first letter of first name and the last name in full for instance account for Faisal would be faisal@codepak.org
- 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.

1.9.5. 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.

1.10. 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.

1.11. IT POLICY IMPLEMENTATION

1.11.1 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.

1.11.2 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.

1.12. 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.
- 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.