Policy Guide and General Procedures

on

Network, Email, IT Usage & Security

PROVINCIAL DISASTER MANAGEMENT AUTHORITY (PDMA) and PROVINCIAL RECONSTRUCTION, REHABILITATION AND SETTLEMENT AUTHORITY (PaRRSA) KHYBER PAKHTUNKHWA

Draft Report

November 2012

DRAFT

Submitted By:

ASP-RSPN CB Team
PDMA-PaRRSA
Peshawar

Topics Covered

ASP-IT Team Work Plan Components:

6.4.1 Network Policy

6.4.2 Email Policy

6.4.3 IT Usage and Security Policy

DRAFT

Table of Contents

		Page #
Topics Covered		2
Table of Contents		3
List of Abbreviations		5
Section 1: Introduction		6
1.1	Organizational Background	6
	1.1.1 PDMA	6
	1.1.2 PaRRSA	6
	1.1.3 Administrative Setup	6
1.2	Purpose of the Document	7
Section 2: Network Policy (Network Resource Usage, Intranet and Internet)		9
2.1	Purpose	9
2.2	Aim	9
2.3	Applicability	9
2.4	Policy	9
2.5	Responsibilities	10
2.6	Guidelines	10
	2.6.1 General Usage and Ownership	10
	2.6.2 Security and Proprietary Information	10
	2.6.3 Unacceptable Use	11
	2.6.4 Encryption	12
2.7	Password Policy	12
	2.7.1 Password Guidelines	12
	2.7.2 Password Reuse, Password Lockout and Testing	13
2.8	Network Access Policy	13
	2.8.1 Network Access Guidelines	14
	2.8.2 Oversight of Network Resources	14
	2.8.3 Reporting and Investigating Violations	14
	2.8.4 Consequences of the Misuse of Network Resources	15
	2.8.5 Cognizant	15
2.9	Guidelines for Wireless Network	15
	2.9.1 Definitions	15
	2.9.2 Scope	16
	2.9.3 Policy	16
Section 3: Email Policy (Internet and Email Usage Policy)		18
3.1	Purpose	18
3.2	Aim	18
3.3	Permitted Use	18
3.4	Prohibited Use	18
3.5	Responsibilities	19
3.6	Violations	19
3.7	Confidentiality and Internet	20

DRAFT

3.8 Bad Judgment/Taste 20
3.9 Honest Disclosure 20
3.10 Excessive Resource Utilization 20
3.11 Public Forums 20
3.12 Chat and Instant Messaging 20
Section 4: IT Usage and Security Policy 21
4.1 Purpose 21
4.2 Leading Principles 21
4.3 Guidelines for Physical Security 22
4.3.1 Definitions 22
4.3.2 Purpose 22
4.3.3 Policy 22
4.3.4 Restricted Space 23
4.3.4.1 Server room 23
4.3.4.2 Electrical Circuits in the Server Room 23
4.3.4.3 Environmental Conditions 23
4.3.4.4 Backup Media 23
4.3.4.5 Communication Racks/Closets 23
4.3.4.6 Power Support 23
4.3.5 IT Storage Areas 23
4.3.5.1 Access Keys/Cards 24
4.3.5.2 Fire Precautions 24
4.3.6 Portable Systems 24
4.3.7 Inventory 24
4.3.8 Assigned Equipment 24
4.3.9 Shared Equipment 24
4.3.10 Annual Audits 24
4.3.11 Responsibilities 25
4.3.12 PDMA-PaRRSA Physical Security Guidelines 25
4.3.13 Related Procedures and Forms 25
4.3.14 IT Equipment Inventory Guidelines 25
4.3.15 Related Procedures and Forms 26
4.4 Technical Security Policies and Procedures 26
4.4.1 Responsibility 26
4.5 Operational Policies and Controls 26
4.5.1 Definitions 26
4.6 User Administration Policy 27
4.6.1 Responsibilities 27
4.6.2 Related Procedures and Guidelines 27
Glossary 29

DRAFT

List of Abbreviations

ASP	-	Assessment and Strengthening Program
CADR	-	Centrally Accessed Data Reservoir
DRM	-	Disaster Risk Management
FTP	-	File Transfer Protocol
GoP	-	Government of Pakistan
GoKP	-	Government of Khyber Pakhtunkhwa
ICT	-	Information and Communication Technology
IT	-	Information Technology
ITMNA	-	Information and Technology Management Need Assessment
MAC	-	Media Access Control
MIS	-	Management Information System
PC	-	Personal Computer
PDAs	-	Personal Digital Assistant
PDMA	-	Provincial Disaster Management Authority
PMU	-	Project Management Unit
RRSD	-	Relief, Rehabilitation and Settlement Department
RSPN	-	Rural Support Programmes Network
SOP	-	Standard Operating Procedures
US	-	United State
USAID	-	United States Agency for International Development
VLAN	-	Virtual Local Area Network
VPN	-	Virtual Private Network
WWW	-	World Wide Web

DRAFT

Section - I

Introduction

1.1 Organizational Background

1.1.1 PDMA

The Provincial Disaster Management Authority (PDMA) was initially established on 10 March 2007, with Home Secretary as its Director General. However, the PDMA was re-notified vide notification # SOR-III(E&AD)4-5/08-Home Dept. dated 27 October 2008 under the legal authority of Section 15 of the NDMO, 2006.

The stated mission of PDMA is to minimize disaster risks through formulation of comprehensive Disaster Risk Management (DRM) strategies and their effective and efficient implementation. PDMA's mission would entail an effective and efficient management and preparedness of disasters. PDMA is presently working as an authority of provincial Relief, Rehabilitation and Settlement Department (RRSD). Its responsibility, therefore, encapsulates every sphere of disaster management i.e. disaster risk reduction / mitigation, rescue, relief, recovery, reconstruction and rehabilitation.

1.1.2 PARSA

Provincial Relief, Rehabilitation and Settlement Authority (PaRRSA) has been established under PDMA as a separate body and as an administrative arrangement through Notification NO. SO (E-1)/E&AD/PaRRSA/2009 dated June 27, 2009 by GoKP.

PaRRSA was created as a dedicated body to coordinate, supervise and monitor reconstruction, rehabilitation and settlement of the conflict affected people in the five districts of Malakand and two Fata agencies i.e. Mohmand and Bajaur and is required to work within the overarching role of PDMA. The Authority will provide the requisite speed, ease, facilitation, coordination, supervision, and linkages to all the stakeholder and helping the provincial government in its endeavor to rehabilitate the affected areas. Its responsibility therefore encapsulates development of strategies and plans coordinate overall reconstruction, rehabilitation and resettlement, facilitation to national and international development partners, supervise and monitor implementing agencies and standardization and smooth application of processes through fast track methods. PaRRSA is the player on ground to conduct all reconstruction and rehabilitation activities.

1.1.3 Administrative Setup

Following are the different sections of PDMA-PaRRSA which will benefit from IT operations:

DRAFT

S. No.	Department
1	Program Management
2	Administration Cell
3	Planning Cell
4	Infrastructure Cell
5	Finance Wing
6	IT Section
7	Media & Communication
8	Donor Coordination
9	Monitoring & Evaluation
10	Internal Audit
11	Housing Section
12	Program Management Unit (PMU)
13	Relief
14	Reconstruction and Rehabilitation
15	Economic Growth

1.2 Purpose of the Document

It is an initiative which contributes to the organization's strategic objective of improving its governance through the deployment of long term policy making and designing IT Strategic Framework to improve monitoring and evaluation of PDMA-PaRRSA's IT systems including both hard and soft components. Policies, procedures and guidelines covered in this document would help to improve the efficiency and accuracy of these systems. Lucidity in defining roles, regulations and standard operating procedures will strengthen organizational protocols and smooth operations. Hierarchal explaination of policies will improve managerial SOPs and autonomy down to the level thus catalyzing overall performance. The Activity specifically contributes to Information Technology to establish, maintain and further develop a functioning IT Skeleton using modern information and technology systems at the provincial department.

The Government of Pakistan encourages its organizations and employees to use e-mail, Internet, organizational websites and other means of electronic media for conducting the official business, for communicating with other government employees and with the general public, for gathering information, and for developing expertise in using IT resources. The continued effort of the relevant departments is gradually shifting the functioning of the government offices to paperless environment.

Capacity Building is mandated by the USAID to help build capacity of PDMA-PaRRSA. In pursuit of its mandate to the CB Team started multiple Capacity building initiatives in the organization. Besides, automation and MIS development of a number of organization's functional sections and components, one of initiatives in Information

DRAFT

Technology Management area is the developing of its I.T Policy. An Information and Technology Management Need Assessment (ITMNA) study was conducted, and after consultation with various stakeholders, a comprehensive I.T. Policy was devised.

The following documents and general standards were used as guidelines for the formulation of IT Policy:

- National IT Policy and Guidelines (August 2000) - The National Telecommunication and Information Security Board's "Policy for Internet, Intranet, web-sites, and E-mail in Federal Government organizations,"
- US National Institute of Standards and Technology handbook
- International Information Technology best practices

While the IT tools and services have enormous potential in facilitating data operations centrally in an integrated environment. Conversely, it's wide application; possess great vulnerabilities to the data either through inadvertent or deliberate actions by organizations or individuals in disclosing classified information in an unauthorized manner or for unlawful activities. Thus it needs to lay down a policy framework that ensures the security of both information and network.

PDMA-PaRRSA is developing its information systems with the assistance of USAID Capacity Building Project. Besides, it needs some ground rules and guidelines for the safe and smooth functioning of its IT systems.

The policy addresses the key aspects of Information Technology. These are;

1. Network Resource Usage;
2. Internet and Email usage;
3. IT Usage and Security.

DRAFT

Section - 2

Network Policy

(Network Resource Usage, Intranet and Internet)

2.1 Purpose

The purpose of this policy is to outline the appropriate use of computer and network resources. The guidelines are meant to protect organization and its employees in digital realm. Inappropriate use of computer and network resources exposes organization to myriad risks like virus attacks, compromising of network systems and services, and legal complications. System usage occasionally results in such hazards.

2.2 Aim

The organizational vision is that all data, both quantitative and descriptive, should be captured at source and stored centrally. All paper forms for collecting data will be changed to intranet based web forms. Electronic work flow will be the prime vehicle for data transmission. The aim is to reduce paper based transactions organization.

The MIS Section of PDMA-PaRRSA is setting up a Centrally Accessed Data Reservoir (CADR) at the organizational Headquarter Peshawar. For its optimum performance the CADR needs to fulfill the following requirements:

- **Confidentiality:** Information security by the encryption of data transactions.
- **Integrity:** Prevent forgery and alteration of transactional data.
- **Authentication:** User identification for data transaction.
- **Non-repudiation:** Reliability enhancement for transactions by using electronic signature.
- **Access Control:** Permits only the selected users to access information.

This arrangement would enable authenticated and controlled access to the organization's Network/Internet and Intranet on security concerns.

2.3 Applicability

It applies to all the users who utilize its computer and communication network technologies for accessing, transmitting or storing organization's data.

2.4 Policy

Internet and intranet-related systems, like computer equipment, software, operating systems, storage media, network accounts (providing access to shared drives and electronic mail), World Wide Web browsing (WWW), File Transfer Protocol (FTP)

DRAFT

etc. are the property of the organization. These systems are to be used for the core purpose of serving the interests of the organization.

The following IT services will be provided to users after the approval of Controlling Authority i.e. head of MIS-Section:

- E-mail.
- Navigation -- WWW services as necessary for official purposes.
- Access to network shared drives for file storing and sharing.
- Access to shared printers/copiers, scanners, etc.
- Specific software applications that support day-to-day business operations (including departmental software applications, intranet applications, web applications, etc)
- IP telephony and fax services (if required by the organization).

2.5 Responsibilities

The Controlling Authority i.e. Head of MIS-Section is responsible for determining network resources usage policy on behalf of the Director General.

2.6 Guidelines

2.6.1 General Use and Ownership

Though a reasonable level of privacy is provided to the users, they however, should be aware that the data they create or store on the organization's systems is the official property. Because of the need to protect the network and its resources, the organization cannot guarantee the confidentiality of information stored on any of its network.

For the security and the network maintenance purposes, authorized system administrators may monitor equipment, systems and network traffic at any time. For ensuring compliance with this policy, the system may be audited on periodic bases.

2.6.2 Security and Proprietary Information

All files must be stored on a network drive, either in the user's network personal drive, or on one of the shared drives. All confidential information should be encrypted irrespective of the device used for its storage.

Passwords must be kept secure and should not be shared. Users are the responsible for the security of their passwords and accounts.

All equipment whether official or personal used by the organizational Internet/Intranet, shall:

- Always executing approved virus-scanning software with up-to-date virus definitions;

DRAFT

- Run an operating system firewall; and
- Have updated security patches for their operating system.

Users are not authorized to disable or re-configure anti-virus, firewall, and other security software installed on their organizational or personal computer systems. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. They shouldn't use and just delete such e-mails.

Dial-up connection is not allowed.

While leaving their computers un-attended, the users must lock their computer screens to avoid misuse of their PCs by unauthorized personnel.

The users must log off the network at the end of each day and power off their workstations.

2.6.3 **Unacceptable Use**

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by the organization.
- Accessing the Internet or downloading files for any unethical purpose, including, but not limited to, pornography, violence, gambling, racism, gender discrimination, harassment, religious or sectarian hatred or any other illegal activity.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which organization or the end user does not have an active license, is strictly prohibited.
- Introduction of malicious programs into the network or server, e.g., viruses, worms, Trojan horses, e-mail bombs, etc.
- Revealing staff account passwords to others, or allowing the use of user accounts by others. This includes family and other household members when work is being done from home.
- Covering security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the user is not authorized or logging into a server or account that the user is not expressly authorized to access. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing and denial of service.
- Port scanning or security scanning is absolutely prohibited.

DRAFT

- Unless it is his duty the user should refrain from network and monitoring.
- Circumventing user authentication or security of any host, network or account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
- Providing information about or lists of organizational staff to outsiders except during the course of normal business activities.
- Transferring of private data or data from user's previous employment, to organizational systems, including emails or any other type of electronic content.

2.6.4 **Encryption**

Computing devices, such as laptops, PDAs (Personal Digital Assistant), and smart phones, as well as storage media, such as CDs, DVDs, and USB (Universal Serial Bus) drives including thumb drives, flash drives, jump drives, etc. all have the potential of falling into the wrong hands, particularly when not placed in a secure location.

Encryption solutions that encrypt entire disks, file folders, or individual files can be used to protect information on such devices.

When sensitive or confidential information is stored in laptops or other mobile devices whose loss and theft may is a common occurrence.

The system administrator should be contacted by the users for setting up encryption on their devices.

2.7 **Password Policy**

All users should take responsible steps, as outlined below for selecting and securing their passwords. Delinquency may leads to disciplinary action.

2.7.1 **Password Guidelines**

All user-level passwords (e.g., email, web, desktop computer, etc.) must be at least 8 characters long and must be changed at least every 90 days.

All system-level passwords (e.g., root, server admin, application administration accounts, etc.) must be at least 12 characters long and must be changed every 60 days.

Passwords should be chosen which are not easy to guess. These should not be related to one's job or personal life. For example, a car license plate number, spouse's name, or fragments of an address should be avoided. Passwords should not be picked from the dictionary, parts of speech, proper names, places, technical terms, and slang words should not be used as passwords. Ideally, password control software may be used to prevent users from selecting easily guessed passwords.

DRAFT

Passwords must be complex and must contain characters from at least three of the following four character sets:

- Uppercase characters (A through Z).
- Lowercase characters (a through z).
- Base-10 digits (0 through 9).
- Non-alphanumeric (for example, !, $, #, %).

In order to maintain the password security, the following guidelines should be adhered to:

- Avoid sharing the passwords with anyone, including administrative assistants or secretaries.
- Treat passwords as sensitive and confidential information.
- Different accounts organizational and private should have different passwords.
- Passwords should not be conveyed through emails or other forms of electronic communication.
- Avoid the use of "Remember Password" features of applications (e.g., Outlook, FireFox, and Instant Messengers).
- Do not store passwords in a file on any computer system (including PDA's or similar devices) without encryption.

The user should immediately report to the system administrator, if the former suspects compromise of his password. The later latter should promptly change it.

User accounts that have system-level privileges granted through group memberships, e.g., domain administrator must have a unique password from all other accounts held by that user.

2.7.2 **Password Reuse, Password Lockout and Testing**

The system will keep track of the last 24 previously used passwords. Logon account will be locked after three consecutive failed logon attempts. Passwords that are locked will remain locked for 30 minutes (15 minutes for system-level passwords) or until the user makes a phone call to the system administrator from unlocking his account.

Lost and forgotten passwords cannot be recovered. Passwords are encrypted so that no one but the password owner can know it. User password can be reset by the system administrator with notifying him.

2.8 **Network Access Policy**

A network access policy is a set of usage rules, a set of parameters, to be used by a specific authorized user, or a set of system criteria that is used to precisely define the rules that must be complied with before the system is allowed to access the network.

DRAFT

2.8.1 **Network Access Guidelines**

Following are some prescribed procedures which must be followed for accessing the network:

- Any user can connect his computer to the network only during the business hours unless he is permitted for a specific period of time beyond regular office hours to work on late sitting official assignments. Late sitting network access privilege will be properly documented and a record will be maintained.
- A user can connect to the network only if he is running the latest version of anti-virus product.
- A laptop must run a personal firewall in order to access the network.
- On deployment of CADR, users in a relevant section will connect only to the specified VLAN.
- Guest users who have non-compliant but not malicious systems are allowed limited to the public internet.

2.8.2 **Oversight of Network Resources**

The head of MIS-Section (lead) is responsible for compliance with all the network policies.

The lead may officially designate another person (System Administrator) to manage and operate the system, but responsibility for information resources remains with the lead.

The system administrator is responsible for managing and operating network resources. The system administrator ensures compliance with policies, including accessing network resources necessary to maintain operation of the systems under the supervision of the system administrator (or lead).

a. **Responsibilities** — The system administrator would:
   - Take all appropriate actions to protect the security of network and information resources.
   - Take precautions against theft of or damage to data.
   - Faithfully execute all licensing agreements applicable to information resources.
   - Communicate this policy, and other applicable information, security and privacy policies and other related procedures to their information resource users.
   - Users should cooperate with head of the MIS-Section to diagnose and correct problems caused by the use of the system under their control.

b. **Suspension of Privileges** — System administrators may temporarily suspend access to information resources if they believe it necessary for the maintenance of the system.

2.8.3 **Reporting and Investigating Violations**

a. **Reporting Violations** — Supervisors will report violations to the head of MIS-Section. The lead will immediately address the defects through the system

DRAFT

account log. Any concerns with system security, or suspected unlawful or improper system activities would be conveyed to the competent authority.

b. **Investigating Violation** — Inspecting and monitoring network and network resources may be required for the enforcement of this policy. Conducting network investigations ensures the safety of an individual or the department. Only the head of MIS-Section may authorize this inspection and monitoring.

c. **Extending Cooperation** — Users will cooperate with any investigation of policy abuse. Failure to cooperate may lead to cancellation of access privileges, or other disciplinary action.

2.8.4 **Consequences of the Misuse of Network Resources**

A user found to have violated this policy may be understood a violator of organizational Code of Conduct and will be subject to appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. If necessary, the head of MIS-Section will refer violations to the higher ups.

2.8.5 **Cognizant**

Head of MIS-Section or other person designated by the Director General PDMA-PaRRSA, shall be the primary contact for the interpretation, monitoring and enforcement of this policy.

2.9 **Guidelines for Wireless Network**

A kind of network which has interconnection between nodes without using a wire is called wireless network. It is established with the help of electromagnetic waves, LAN connection etc.

The inherent nature of wireless communication, wireless networks require increased cooperation and coordination between interacting entities to maximize the technology's benefits to the users. The technology provides a roaming connection in different organizational sections independent of spatial constraints.

The wireless network guidelines sets forth guidelines for using wireless technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in a distributed network environment. This policy expands the MIS-Section Network Connection Policy by including specific directions regarding wireless communications and conflict resolution. This policy is, however, subject to change as the rise of new technologies and processes may entirely change the wireless landscape and warrant new regulations.

2.9.1 **Definitions**

- Access Point means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub

DRAFT

used to connect segments of a LAN, using transmits and receives antennas. Access Point is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. It strengthens wireless security and expands the physical range of service a wireless user has access to.

- Wireless infrastructure means wireless access points, antennas, cablings, power, and network hardware associated with the deployment of a wireless communications network.

- Coverage means the geographical area where a baseline level of wireless connection service quality is attainable.

- Interference means the degradation of a wireless communication signal caused by electromagnetic radiation from another source depending on the strength of the interfering signal.

- Privacy means the condition that provides for the confidentiality of personnel, employee and staff communications, and institutional data transmitted over a wireless network.

- Client hardware/software means the electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide a LAN interface to a wireless network.

2.9.2 **Scope**

This policy applies to all wireless network devices utilizing organizational IP space and all users of such devices, and governs all wireless connections to its network backbone, frequency allocation, network assignment, registration in the Domain Name System, and services provided over wireless connections.

2.9.3 **Policy**

- Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.

- Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.

- Wireless access points will require user authentication. These authentications and privileges assigned to specific supervisors must be registered with MIS-Section for record management.

- Physical security should be kept in view while planning the location of wireless access point and other wireless network components.

DRAFT

- Avoid some of the physical and logical interference between components of different network segments and other equipment and should be ensured while designing and deploying a wireless network.

- In the event that a wireless device interferes with other equipment, MIS-Section under the direction of Director General PDMA-PaRRSA shall resolve the interference. For conflict resolution an arbiter can be appointed by the mutual consensus the aggrieved parties.

- Disconnect Authorization

  Any wireless network, which poses a security threat, may be disconnected from the campus backbone network. If a serious security breach is in process, MIS-Section and Admin-Section may disconnect the LAN immediately. A Point of Contact will be nominated to reach, register and resolve security problems.

- MIS-Section has the authority to disconnect any wireless network from the network backbone whose traffic violates practices set forth in this policy or any network related policy. Anyhow, any conflict arise in this regard can be resolved through "Point of Contact".

DRAFT

Section - 3

Email Policy

(Internet and Email Usage Policy)

3.1 Purpose

The PDMA-PaRRSA has made substantial investments to make it possible for its employees to electronically communicate with fellow employees and other related personnel, organizations as well as to seek information from the worldwide web. These investments are meant to enhance the employee's productivity. Enabling such facilitation costs telecommunication, networking, additional software, and mass storage expenses. This policy, therefore, enforces and defines the acceptable use of these devices.

Internet facility at PDMA-PaRRSA is provided to users with understanding that they will use these resources for official purpose. Following is the list of appropriate usage:

a. Communicating with fellow employees and related organizations for official purposes.
b. Researching topics that are relevant to the user's specific job requirements.
c. Conducting any other official activities.

3.2 Aim

To lay down guidelines for the appropriate use of internet, email and allied communications.

3.3 Permitted Use

The Internet connections and e-mail system of PDMA-PaRRSA is primarily meant for official use. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of duties.

a. Users may use organizational internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct.
b. Users may send and receive e-mail attachments that do not exceed 5 MB in size. All attachments should be scanned before these are opened by the organizational chosen antivirus software.

3.4 Prohibited Use

Users shall not use official internet or e-mail services to view, download, save, receive, or send material related to or:

DRAFT

a. Offensive content of any kind, including pornographic material,
b. Promoting discrimination on the basis of gender, national origin, age, marital status, religion, sect, or disability.
c. Threatening or violent behavior.
d. Illegal activities & harassment.
e. Accessing Face book, YouTube, Twitter, LinkedIn and other social media.
f. Sending commercial messages for personal gains.
g. Gambling.
h. Forwarding e-mail chain letters of unofficial contact.
i. Spamming e-mail accounts from organizational e-mail services or other machines.
j. Violating copyrights.
k. Sending sensitive official information by e-mail or over the Internet.
l. Downloading & transmitting, songs and movies, games and other means of entertainment.
m. Using fake ID's or ID's theft.
n. Using/installing any spyware on personal or official.
o. Sending anti-state messages.
p. All other prohibitions defined by the GoP.

Note:- Please note that a, b, c, d, f & k are also covered under cyber crime law (Ministry of Interior) and if a complaint is registered by, the affectee, it can result in serious consequences for the offender.

3.5 Responsibilities

PDMA-PaRRSA users are responsible for:

a. Honoring the user policies of networks accessed through organizational Internet and e-mail services.
b. Abiding by all the existing federal and provincial networking laws and regulations.
c. Following copyright laws regarding protected commercial software and intellectual propriety.
d. Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of organizational network resources.
e. If any email is received which contrary to organizational policy it must be immediately forwarded to System Administrator for further action.

3.6 Violations

Violations will be reviewed on case-to-case basis. If it is determined that a user has violated one or more of the above usage regulations, then that user's account will be removed from the active list and he will be served with a warning. Management will initiate immediate corrective action upon the receipt of complaint regarding any violation.

DRAFT

3.7 Confidentiality and the Internet

The Internet enables to make statements for the organization. When an organizational employee sends a message or communicates through a public forum as an employee, it is natural for the recipient of that message or communication to understand it to be an official message.

Under no circumstances should any user disseminate confidential information over the Internet to any unauthorized person. Security and confidentiality of official documents should not be compromised under any circumstances. All attached files should be scanned using latest version of officially deployed anti-virus software. Confidential documents should be sent in encrypted form.

3.8 Bad Judgment/Taste

It is a violation of organizational policy to store, view, or print graphic files that are not directly related to an employee's job or to the official activities of the organization. Examples of such misuses include downloading games, jokes, audio/video files, animations etc.

3.9 Honest Disclosure

Users should honestly disclose their identity while making transactions over the web.

3.10 Excessive Resource Utilization

Users are reminded to make prudent use of the Internet in order to avoid degradation of the overall computing resources of the organization. Therefore, the users shall refrain from excessive downloads that might constrain computing resources.

3.11 Public Forums

All confidentiality matters apply to public forums.

3.12 Chat and Instant Messaging

Users are not permitted to use the official IT resources for chat or instant messaging, unless approved for an official purpose by the management.

DRAFT

Section - 4

IT Usage & Security Policy

4.1 Purpose

This policy provides assistance in securing computer-based resources (including hardware, software, information etc.) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, major techniques deployed for these controls, and other related considerations. It provides an overview of computer security to help MIS-Section understand its computer security needs and develop a sound approach for the selection of appropriate security controls. The section is also facilitated by providing a detailed implementation procedure for security control. Guidance for auditing the security of specific systems is also included.

4.2 Leading Principles

Framing of the PDMA-PaRRSA security policy is based on the following principles:

Accountability – Security arrangements and responsibilities among the providers and the users of the IT resources should be clearly defined.

Awareness – Awareness of the users of organizational IT resources so that they should readily be able, consistent with maintaining security, to gain appropriate knowledge of the existence and general extent of measures for the security of information systems. The users should be regularly updated on the security issues by the MIS-Section.

Ethics - The rights and the legitimate interest of others are respected.

Proportionality - Security levels, costs, measures, practices and procedures should be proportionate to the value of and degree of information systems. These should also be commensurate with the level of potential threats.

Integration – Integrated measures should be adopted for achieving an orderly and systematic security apparatus.

Timeliness – Well-timed troubleshooting for the IT resources.

Reassessment - The security of information systems should be reassessed periodically, as the IT security requirements morphs, reflecting the changes in the overall IT environment.

DRAFT

4.3 Guidelines for Physical Security

Physical and environmental security relates to measures adopted for the protection of systems, buildings, and related infrastructure against threats associated with their physical environment.

4.3.1 Definitions

The **physical facility** is usually a building, or other solid structure housing the system and network components. Systems can be both fixed and movable. Fixed systems are installed at permanent locations. Portable systems are moveable. They both or portable only may be operated in wide variety of locations, including buildings or vehicles, or in the open (such as laptop computers).

Threats can be both natural or man-made. Earthquakes, floods, landslides, fires, illegal interception of transmissions, electromagnetic interference, etc. or some of the major threats.

Supporting facilities and conditions are those services that support the system's operation. These include electric power, heating, air conditioning and telecommunications etc. Failure or substandard performance of these facilities may interrupt operation of the system and, may even cause physical damage to the hardware or stored data.

4.3.2 Purpose

The purpose of the physical security policy is to address security factors such as physical facility, physical threats, environmental and supporting conditions. Based on these factors, practices are developed for the physical protection of the IT resources.

4.3.3 Policy

All areas in the building where vital IT system components are situated must be identified as restricted space and physical access controls must be implemented. Vital system components include servers, telecommunication racks (closets) with active equipment, main electrical switch boards, telephone lines switchboards, internet connection devices, backup media and other components necessary to system operation. All of the essential components must have at the least a lock and a key. Keys should be entrusted only to authorized personnel.

DRAFT

4.3.4 **Restricted Space** (Server rooms, telecommunication closets or racks, IT storage rooms)

4.3.4.1 **Server room**

Server room should be locked at all times. Only authorized individuals should have access to the server room. Any unauthorized staff that may need temporary access to server room must be escorted and supervised while in the server room (like cleaning staff). The server room must not be used for storage of other hardware or any other flammable materials like cardboard boxes. No staff should be located in the server room. It would not be used by any employee as his permanent workplace.

4.3.4.2 **Electrical circuits in the server room**

Electrical circuits in the server room should be properly grounded/earthed.

4.3.4.3 **Environmental conditions**

Server room should be equipped with appropriate air-conditioning, and if necessary humidifiers, also. It should not be exposed to direct sunlight, windows and ventilators, and other openings should be sufficiently covered for blocking sunlight.

4.3.4.4 **Backup media**

Backup media should be kept in a locked place. Only authorized personnel should have access to the backup media. Media containing full weekly backup of server essential files and data should be kept off-site in a secure facility.

4.3.4.5 **Communication racks/closets**

Communication racks can be placed in the server room or they can be distributed over the different parts of the buildings. Each communication rack must be locked at all times. Only authorized personnel should have access to the communication racks.

4.3.4.6 **Power support**

All servers and communication equipment must be connected to Uninterruptible Power Supplies for surge protection, voltage fluctuation protection, and extended operation in case of power failures.

4.3.5 **IT Storage areas**

Boxed or spare equipment should be placed in a separate designated area with appropriate shelving for proper storage. Storage areas should be under lock and key. Only authorized personnel should have access to the storage areas.

DRAFT

4.3.5.1 **Access Keys/Cards**

Each users to whom access key/card has been assigned and issued will sign Receipt/Return of access keys form. The Return Form should be filled out when the access key/card is returned by assignee.

Safekeeping the access key/card is the user's responsibility. In case of damage or loss, the user will be required to fill out a damage/loss report.

4.3.5.2 **Fire precautions**

Server rooms and IT equipment storage areas should be fitted with smoke detectors. Fire extinguishers must be placed near the server and storage rooms. Directives of the civil defense departments should be followed in letter and spirit.

4.3.6 **Portable systems**

Laptops should be configured with security locks. While traveling, users must not leave laptops unattended at any time.

4.3.7 **Inventory**

Detailed and up-to-date inventory must be kept of all the IT hardware and software and issued portable devices.

4.3.8 **Assigned Equipment**

Each user to whom IT equipment has been assigned and issued will sign Equipment Receipt Form. The Equipment Return Form will be filled out when the equipment is returned.

User is responsible for safekeeping the equipment. In the event of damage or loss, user will be required to fill out a damage/loss report. User will be held accountable if negligence is proved on his part.

4.3.9 **Shared equipment**

Sign-out logs must be kept for the issuance of any shared or portable equipment (laptops, projectors, digital cameras, USB devices and any other shared portable equipment).

4.3.10 **Annual audits**

Annual review should be conducted to assess physical and environmental controls for IT systems. Annual review should be followed by a report and recommendations for improvement of physical security controls, preferably through a consultant.

DRAFT

4.3.11 **Responsibilities**

Head of the MIS-Section is responsible for determining and maintaining physical security policies, guidelines and controls. He may delegate some of his responsibilities but he cannot delegate his responsibilities.

4.3.12 **PDMA-PaRRSA Physical Security guidelines**

Both the server room and the storage room should have adequate protection against intrusion.

Only authorized users should be granted access through keys/access cards for entering the server room or the IT storage room. Administration, security, IT department employees and IT consultants may be given access in accordance with their positions and responsibilities.

4.3.13 **Related Procedures and forms**

- Issuance of access keys/access cards procedure
- Receipt/Return of access keys form
- Emergency procedures in case of fire
- Emergency procedures in case of natural disasters or physical damage to the facilities
- Loss/Damage report form

4.3.14 **I.T Equipment Inventory Guidelines**

An updated inventory of all the IT items shall be maintained.

Equipment inventory must contain

- equipment make model, and specifications
- Serial number
- MAC address (if applicable)
- Warranty information
- Date of purchase
- Donation date (if applicable)
- Assignee's name and location
- Working status of the different devices peripheral devices, along with maintenance history
- Goods stolen or purchased

The inventory must be updated whenever an event occurs which changes, the equipment specifications (memory upgrades, for example), the assignee, the location, or the status.

DRAFT

Each IT equipment item should have inventory sticker firmly attached to it for quick reference.

Relevant laws, regulations, and procedures, must be followed while disposing of redundant IT items.

All purchased software licenses must be kept in the inventory. The inventory should contain at least the following information about the software

- Name of the software developer
- Software name
- Number of licenses purchased
- Date of purchase transference date
- Documentary proof of purchase attached
- Maintenance information (software maintenance period, or software assurance period).

4.3.15 **Related Procedures and forms**

- Equipment issuance procedure
- Equipment return procedure (transfer to another assignee, equipment replacement or termination)
- Equipment Receipt form
- Equipment Return form
- Loss/Damage report form

4.4 Technical Security Policies and Procedures

4.4.1 **Responsibility**

Head of the MIS-Section has the Administrative Control over the IT systems established in his/her domain.

4.5 Operational Policies and Controls

Operational controls are security methods that focus on mechanisms that are primarily implemented and executed by people.

4.5.1 **Definitions**

The term **user** refers to any PDMA-PARRSA employee, contractor, or any other individual providing services to the PDMA-PARRSA, directly or indirectly. The user will be granted level of access commensurate with his position, and responsibilities.

DRAFT

System administrator, **developers**, and **IT support staff**, are employees or contractors who have elevated level of access to the IT system in order to maintain, develop, test the system, and provide user support.

The term **system owner** refers to section heads or other managers who are in charge of specific application, or infrastructure systems and are responsible for their overall functionality. Based on their responsibilities, the system owner may or may not have elevated access privileges to the IT systems. System owners usually work closely with the technical staff (system administrators, developers and IT support staff) to ensure system's functioning, and security.

The competent authority may designate the head of MIS- Section, or any other employee as the **controlling authority**. He is ultimately responsible for the implementation of the IT policies.

4.6 User Administration Policy

The user will be registered on the network for using shared network services, and system applications. He will be given an email account and access to the internet and/or intranet.

Access privileges will be revoked when an employee's contract terminates.

In the case of a change in job functions and/or transfer, the original access privileges will be discontinued and reissued only if necessary and a new request for access is approved.

External clients or non-organization personnel are not permitted access to organization internal network resources unless specifically approved in advance by the Controlling Authority.

4.6.1 Responsibilities

The concerned section head will request an appropriate level of access for his employee. The request for termination of service will also be initiated by him. On receiving such requests the system administrator will register or de-register the users.

The Controlling Authority is responsible for implementing the user administration policy.

4.6.2 Related Procedures and Guidelines

- Equipment issuance procedure
- Equipment return procedure (transfer to another assignee, equipment replacement or termination)
- Equipment Receipt form
- Equipment Return form

DRAFT

- Loss/Damage report form

DRAFT

Glossary

- **Antivirus** - **Antivirus** (or '**anti-virus**') **software** is a class of program that searches your computer or laptop hard drive and floppy disks/CDs/DVDs for any known or potential viruses.
- **CD-ROM** - (Compact disc read-only memory) - a pre-pressed compact disc that contains data accessible to a computer for data storage and music playback. It is read in an optical disc drive.
- **Memory** - In modern usage, a synonym for main memory, dating back from the time when the dominant main memory technology was magnetic core memory.
- **CPU** (Central processing unit) - the portion of a computer system that carries out the instructions of a computer program, and is the primary element carrying out the computer's functions.
- **Decryption** is the process of converting encrypted data back into its original form, so it can be understood.
- **Denial of Service** – A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.
- **Downloading** -The use of the terms uploading and downloading often imply that the data sent or received is to be stored permanently, or at least stored more than temporarily. In contrast, the term downloading is distinguished from the related concept of streaming, which indicates the receiving of data that is used near immediately as it is received, while the transmission is still in progress and which may not be stored long-term, whereas in a process described using the term downloading, this would imply that the data is only usable when it has been received in its entirety. Increasingly, websites that offer streaming media or media displayed in-browser, such as YouTube, and which place restrictions on the ability of users to save these materials to their computers after they have been received, say that downloading is not permitted. In this context, download implies specifically "receive and save" instead of simply "receive". However, it is also important to note that downloading is not the same as "transferring" (i.e., sending/receiving data between two storage devices would be a transferal of data, but receiving data from the Internet would be considered adownload).
- **DVD** (Digital Video Disc or Digital Versatile Disc) - an optical disc storage media format, and was invented and developed by Philips, Sony, TOSHIBA, and Time Warner in 1995. Its main uses are video and data storage. DVDs are of the same dimensions as compact discs (CDs), but store more than six times as much data.
- **E-Mail** – Is the mail sent electronically through the inter-connected digital devices on the Internet.
- **Encryption** - is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

- **File Transfer Protocol** – is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.
- **Firewall** - A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious locations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world. Firewalls can be either hardware or software. **Hardware firewalls** can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available. Software Firewall :individual home users, the most popular firewall choice is a software firewall. **Software firewalls** are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system. Additionally, software firewalls may also incorporate privacy controls, web filtering and more. The downside to software firewalls is that they will only protect the computer they are installed on, not a network, so each computer will need to have a software firewall installed on it.
- **Hard Disk Drive (HDD)** - a non-volatile storage device that stores digitally encoded data on rapidly rotating rigid (i.e. hard) platters with magnetic surfaces.
- **Hardware** - multiple physical components of a computer, upon which can be installed an operating system and a multitude of software to perform the operator's desired functions.
- **IT Skeleton** – The term used for a set of overall computer system comprising software applications running on server computers and accessed centrally through a wide deployment and use of terminal computers on LAN, WAN and ICT.
- **Input Device** - Any peripheral piece of computer hardware equipment) used to provide data and control signals to an information processing system.
- **Input/Output** - The communication between an information processing system (such as a computer), and the outside world possibly a human, or another information processing system.

- **Local Area Network** – A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users (for example, in an FDDI network).
- **Logon Account** - In general computer usage, logon is the procedure used to get access to an operating system or application, usually in a remote computer. Almost always a logon requires that the user have (1) a user ID and (2) a password. Often, the user ID must conform to a limited length such as eight characters and the password must contain at least one digit and not match a natural language word. The user ID can be freely known and is visible when entered at a keyboard or other input device. The password must be kept secret (and is not displayed as it is entered). Some Web sites require users to register in order to use the site; registered users can then enter the site by logging on.
- **Management Information System (MIS)** – Is a computer based application to manage information digitally so that it could be made available on click based environment.
- **MAC Address** - A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.
- **Network** – A collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users.
- **Operating system** - An operating system (OS) is a set of software that manages computer hardware resources and provide common services for computer programs.
- **Packet spoofing** - IP Spoofing is a security exploit where an Intruder attempts to send packets to a system which appear to originate from a source other than the Intruder's own. If the target system already has an authenticated TCP session with another system on the same IP network, and it mistakenly accepts a spoofed IP packet, then it may be induced to execute commands in that packet, as though they came from the authenticated connection. Improved reliability and routing filters in major Internet routers make this attack largely obsolete on the Internet in cases where theIntruder and target system are topologically distant.
- **Password** - A password is a secret word or string of characters that is used for user authentication to prove identity, or for access approval to gain access to a resource (example: an access code is a type of password).
- **Provincial Disaster Management Authority (PDMA)** -The stated mission of PDMA is to minimize disaster risks through formulation of comprehensive Disaster Risk Management (DRM) strategies and their effective and efficient implementation.

- **Provincial Relief, Rehabilitation and Settlement Authority (PaRRSA)** - PaRRSA was created as a dedicated body to coordinate, supervise and monitor reconstruction, rehabilitation and settlement of the conflict affected people in the five districts of Malakand and two Fata agencies i.e. Mohmand and Bajaur and is required to work within the overarching role of PDMA.
- **Peripheral** - A device attached to a host computer but not part of it, and is more or less dependent on the host. It expands the host's capabilities, but does not form part of the core computer architecture. Some computer peripheral include (Express Card, USB Drive, SD Card Memory Stick, router, external SSD & HDD Drives).
- **Personal Computer (PC)** - any general-purpose computer whose size, capabilities, and original sales price make it useful for individuals, and which is intended to be operated directly by an end user, with no intervening computer operator.
- **Pinged Floods** -A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most implementations of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.
- **Printer** - a peripheral which produces a text or graphics of documents stored in electronic form, usually on physical print media such as paper or transparencies.
- **Protocol** - In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate.
- **RAID (Redundant Array of Independent Disks)** - An umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives in order to increase reliability, allow faster access, or both.
- **RAM (Random-Access Memory)** - a form of computer data storage. Today, it takes the form of integrated circuits that allow stored data to be accessed in any order (i.e., at random).
- **ROM (Read-only Memory)** - a class of storage media used in computers and other electronic devices.
- **Routing** - Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (circuit switching),electronic data networks (such as the Internet), and transportation networks.
- **Server** - any combination of hardware or software designed to provide services to clients. When used alone, the term typically refers to a computer which may be running a server operating system, but is also used to refer to any software or dedicated hardware capable of providing services.

DRAFT

- **Software** - a general term primarily used for digitally stored data such as computer programs and other kinds of information read and written by computers. Today, this includes data that has not traditionally been associated with computers, such as film, tapes and records.
- **Spam** – Spam is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, social spam, television advertising and file sharing network spam. It is named for Spam, a luncheon meat, by way of a Monty Python sketch in which a spam hating restaurant patron is frustrated by a cafe in which the canned meat product is featured in seemingly every dish made.
- **Spyware** -Spyware is a type of malware (malicious software) installed on computers that collects information about users without their knowledge. The presence of spyware is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.
- **Tape Drive** - A peripheral device that allows only sequential access, typically using magnetic tape.
- **Terminal** - An electronic or electromechanical hardware device that is used for entering data into, and displaying data from, a computer or a computing system.
- **Trojan horse** - A Trojan horse, or Trojan, is a type of malware that masquerades as a legitimate file or helpful program but whose real purpose is, for example, to grant a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems.
- **USB (Universal Serial Bus)** - A specification to establish communication between devices and a host controller (usually a personal computers). USB is intended to replace many varieties of serial and parallel ports.
- **USB flash drive** - A flash memory data storage device integrated with a USB (Universal Serial Bus) 1.1, 2.0, or 3.0 interfaces. USB flash drives are typically removable and rewritable, and much smaller than a floppy disc.
- **VGA** - A Video Graphics Array (VGA) connector is a three-row 15-pin DE-15 connector. The 15-pin VGA connector is found on many video cards, computer monitors, and some high definition television sets. On laptop computers or other small devices, a mini-VGA port is sometimes used in place of the full-sized VGA connector.
- **Webcam** - A webcam is a video camera that feeds its images in real time to a computer or computer network, often via USB.
- **Workstation** - A workstation is a high-end microcomputer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems. The term workstation has also been used to refer to amainframe computer terminal or a PC connected to a network.

DRAFT

- **World Wide Web** – The World Wide Web (abbreviated as WWW, commonly known as the Web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks.
- **Worms** –Historical English-speaking cultures have used the terms *worm*, *Wurm*, or *wyrm* to describe carnivorous reptiles, and the related mythical beast's dragons. The term worm can also be used as an insult or pejorative term used towards people to describe a cowardly or weak individual or individual seen as pitiable. In IT this represents software which causes any weakness to the applied software.

DRAFT