HAPA IT Management and Control POLICY

August 2016.

The HAPA's main areas of interest:

- Advocacy & Civil Society (Human Rights, Child Protection, Seminars, Liaison with Government & local authorities & publications)
- Educational programs
- Health Education Programs (Preventive health behaviors, environmental and social health, drug abuse & rehabilitation, Mother & Child Health, Nutrition, Hygiene & Sanitation)
- Skill/ Human Development (vocational trainings, income generation& Community Development)
- Environment (Advocacy & Awareness on environment protection, forestation and safe water supply)
- Research & Development (Baseline Survey, Seminars & publications)
- Emergency relief
- Food Security

Stakeholders:

Community Development Councils (CDCs), Education Dep't, Economics Dep't, NSP/MRRD, Provincial Public Health Department (PHD), Department of Women Affair (DoWA), Provincial Department of Labor, Social Affair, Martyrs and Disables (DoLSAMD), UN family, PRT Kandahar & Helmand, local community members (men, women and children), government officials and donors.

Objective of IT Policy

The purpose of this policy is to define the protection and to the responsible use of computers and Information Systems and the use of all HAPA office equipment including, but not limited to

computers, scanners, printers, projectors, digital cameras, mobile phones and network devices and also the use of Internet and emails.

General

This policy shall apply to all employees of both HAPA main and sub offices using desktop computers, laptops, smart phones or any other device that may allow access to HAPA network.
To prevent unnecessary expenses, repairs and systems failures to HAPA equipment; also, to prevent misuse of equipment that may result in a slower internet and networking system, viruses to the HAPA network and exposure to web sites, photos and other materials not deemed appropriate for a work place.
The policies described below may at any time be subject to modification if the Board of Members of HAPA deems it necessary. In such cases, employees will be fully informed of the changes made.

Use of IT Systems and Equipment

Hardware and electronic communications systems at HAPA shall be used for the HAPA business and may not be used for personal needs, except on an incidental and occasional basis that does not interfere with an individual's job performance.
All systems are maintained by the HAPA IT Officer or the designee in main or sub offices.
Use of HAPA computing resources in a manner that creates a security risk is not permitted. This includes but is not limited to disclosing passwords, opening up illegal connections to the Internet.
Also the actions pointed below are prohibited.

- Attempting to add, remove or modify computer equipment, software, or peripherals without proper authorization.
- Accessing without proper authorization computers, software, information or networks that belong to HAPA.
- Unauthorized attempts to repair IT equipment. All repair needs are to be reported to the IT department or the designee in the office.
- Taking actions, without authorization, which interfere with the access of others to information systems.
- Reading other users files or information without permission.
- Installing games, playing/copying video songs or movies and installing pirated software.
- Using of software or downloading files which may degrade internet bandwidth.
- Using of IT systems for any unlawful or improper purposes including, but not limited to posting, copying, downloading, viewing or transmitting any material that violates the rights of others or is illegal, infringing, threatening, abusive, defamatory, sexually explicit or offensive, harassing or otherwise objectionable.

Failure to adhere to these policies will result in disciplinary actions. Disciplinary action may include counseling, restriction of computer access, written warning and/or termination.

Access to Computers

Employees and authorized users will not allow any person access, in any manner, to their assigned computer unless that person is from HAPA's IT department or supervisor/line manager.

Usage of Email

Individuals may be issued one email account based on the requirements or as requested by the line manager and approved by the HAPA senior Management.
The account holder is ultimately responsible for the use of his or her email account. If the account holder grants access to anyone else, such as delegating rights to an assistant, the account holder remains fully responsible for all messages sent from that account.

Workers must not use personal email accounts to conduct HAPA business. Only authorized HAPA email accounts and software should be used, except where there is an approved requirement.
Only IT devices that are owned by HAPA will be allowed to interface with the HAPA owned email system.

Email Security

The computers in HAPA are protected by licensed Kaspersky Antivirus software, so all internet-based email messages, both incoming and outgoing, are scanned for viruses. Also the email server has the capability of scanning the incoming emails for viruses, when a mailbox encounters a message that appears to be infected by a virus, the message will be marked versus or spam email.

IDs and Passwords

It is a prohibited to disclose login IDs or passwords to anyone, or allow anyone to utilize your credentials to access HAPA networks, computers or systems. It is also prohibited to have your login credentials written down in such a manner as to be seen by and/or visible to others. As examples; do not write your password(s) on a piece of paper and tape it to your screen, under your keyboard, inside your desk drawer, etc.

Internet

Browsing of the internet is restricted to HAPA use only, so browsing functions are not to be available on computers where access is not required. Heads of Departments and/or Project Managers may approve a request for internet access for an employee.
A record of all websites visited are routinely logged in the HAPA's proxy server and may be monitored, accessed, reviewed and disclosed.
The IT Administrator usually checks communications and IT systems in the normal process of work. This includes, visited web sites, system files etc.
Misuse of Communication and IT Systems as determined will result in disciplinary action. Disciplinary measures include written and verbal warnings.
The following actions are prohibited on HAPA Electronic Communications system.

- Downloading or installing any software or upgrades without proper authorization with the exception of Anti-Virus updates and security patches.
- Downloading and storing pictures, music or other entertainment.
- Accessing websites and media deemed inappropriate or offensive.
- Installing a private system to the HAPA network for internet access or otherwise without permission and approval from the line manager.
- If a private computer is to be used with HAPA network, the System Administrator has the right to monitor it the same way as a HAPA's computer.

Data Backup and Access

All work related data must be backed-up regularly on monthly basis's on the local computers and network drives then a monthly full backup will be performed on the network drivers or local computers by the IT administrator that a copy will be also stored on external hard disk or DVDs.

All data of work is considered the possession of HAPA and must be available for accesses by supervisors and senior management. Business records and correspondences are to be maintained neatly and well managed filing systems such that any single individual does not have control/access to this information. Whenever the employee become unavailable due to illness or other reasons or refuse to provide the information necessary, the IT Administrator may be required to access information.

Repair and Maintenance

All repairs and maintenance are to be conducted through the IT Administrator or designee in other HAPA offices. Under no circumstances are staff to attempt repairs at HAPA IT equipment personally or through unapproved vendor.

Users are required to maintain the IT equipment's assigned to them as described below:

- Equipment should to be cleaned regularly; especially from dust.
- Run "De-fragmentation" utility at least once a month on the computer to optimize your system's performance.
- Make sure to turn off electronic equipment's at your office including the power regulator and U.P.S. before you depart the office for the day.
- Users should back up HAPA business related data regularly or at least once a week.
- Users should scan Flash Memories or SD Cards from other staff or from filed officers, then copy or look at the data.

Use Safety

Use of cell phones and other handheld communication devices (whether belonging to HAPA or to the individual) is strongly discouraged while driving on HAPA business, except as required or prudent in particular conditions.

Software:

Employees are prohibited from downloading or installing software or programs onto the HAPA electronic communication systems or computers without authorization from IT Department. Do not copy software from HAPA's computer system for installation on home or other computers without prior authorization from HAPA's IT department. As may be required, HAPA will purchase additional copies or licenses. Any employee issued additional copies or licenses of software for home use acknowledge that such additional copies or licenses purchased for home use are the property of HAPA.

Returning of Property

Any property of HAPA that has been issued to an employee for use in connection with the Agency's work (including, but not limited to, keys, computers, credit cards, cell phones and all handheld portable electronic communication devices) must be returned to HAPA upon termination of employment.