CENTER FOR INTEGRATED HEALTH PROGRAMS (CIHP)

Standard Operating Procedures

Information Technology Policy

January, 2012

Centre for Integrated Health Programs (CIHP)
Plot 1129, Kikuyu Close (Off Nairobi Street)
Wuse II, Abuja

Information Technology Policy

This Information Technology policy articulates CIHP's strategy and principles as they relate to the use of information and information technology resources. IT policies interpret applicable laws and regulations and ensure that the policies are consistent with legal and contractual requirements. In addition, IT policies specify requirements and standards for the consistent use of IT resources across the organization.

This document develops and maintains IT policies that are in step with emerging technologies and align with the evolving role and philosophy of CIHP. The IT policy establishes a framework that will:

- Determine when to establish a policy, guideline or standard
- Determine the criteria for what should be in a policy, guideline or standards
- Create a collaborative methodology for the drafting, approving, updating, and expiration of policies, standards, and guidelines
- Document and communicate policies, standards, and guidelines
- Serve as an organizational resource to consistently interpret and arbitrate policies
- Measure policy effectiveness and level of adoption

These guidelines are also designed to alert CIHP staff of their responsibilities.

It is the responsibility of each CIHP staff to:

- Understand and follow the IT policies in this document.
- Use CIHP computer systems properly.
- Protect the integrity of the systems by treating equipment with care and adhere to IT security measures.
- Call the IT Help Desk when a problem occurs.

It is the obligation of CIHP's Information Technology staff to:

- Educate staff about any IT issues or concerns.
- Follow a process that addresses IT needs in a timely manner.
- Provide staff with basic functional equipment to facilitate their work duties.
- Respect staff's privacy for all information stored in the IT systems.
- Respond to Help Desk calls in a timely manner.

Scope

This Policy applies to all Users of IT Systems, including but not limited to full-time employees of CIHP, temporary hires and consultants. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by CIHP, as well as those administered by CIHP-supported facilities.

Use of IT Systems within CIHP premises, even when carried out on a privately owned computer that is not managed or maintained by CIHP, is governed by this Policy.

Policy Statement

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic mission of CIHP in pursuance of its goals and objectives. In particular, this Policy aims to promote the following goals:

- Ensure the integrity, reliability, availability, and superior performance of IT Systems;
- Ensure that use of IT Systems is consistent with the principles and values that govern use of organizational facilities and services;
- Ensure that IT Systems are used for their intended purposes; and
- Establish processes for addressing policy violations and sanctions for violators.

Reason for the Policy

Information technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of CIHP's, management, programmatic, administrative, and other roles. Users of CIHP's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as CIHP itself. This CIHP IT Policy provides guidelines for the appropriate use of CIHP's IT resources as well as for the organization's access to information about and oversight of these resources.

This CIHP policy is important in determining appropriate use of information technology. Using electronic mail ("email") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. CIHP policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant CIHP policies.

For statements of other applicable CIHP policies, please consult the CIHP Employee Manual, Procurement Policy, Property and Inventory Manual as well as policy manuals and statements issued from time to time.

Definitions

IT Systems: These are the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by CIHP. For example, IT Systems include institutional and

departmental information systems, desktop computers, the network, including systems and related equipment at field offices and those maintained by CIHP in supported facilities.

User: A “User” is an individual who has been authorized to make use of IT equipment to achieve CIHP business purposes. A "User" is thus any authorized person who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a CIHP computer cluster, or via an electronic network.

Systems Authority: CIHP has the legal title to all IT Systems. The default Systems Authority is the CEO or his/her designate.

Systems Administrator: System Authority may designate another person as "Systems Administrator" to manage the IT Systems. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

Certifying Authority: This is the Chief Executive Officer or his/her designate who certifies the appropriateness of an official CIHP document for electronic publication in the course of CIHP business.

Specific authorization: This means documented permission provided by the Systems Administrator to different levels of network resources.

Policy Sections

Appropriate use of IT Systems

Although this Policy sets forth the general parameters of appropriate use of IT Systems employees, temporary hires and consultants should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that CIHP considers appropriate in light of their varying roles within the organization. In the event of conflict between this IT policy and IT related clauses in other documents, this Appropriate Use Policy will prevail.

A. **Appropriate Use**.
IT Systems may be used only for their authorized purposes -- that is, to support the programmatic, financial, management, administrative, and other functions of CIHP. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

B. **Proper Authorization**.
Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

C. **Specific Proscriptions on Use**.
The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with CIHP's non-profit status**. CIHP is a non-profit, non-governmental organization and, as such, is subject to specific federal, state, and local laws including donor regulations regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-CIHP purposes is generally prohibited, except if specifically authorized and permitted under CIHP conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the CIHP's programmatic, administrative, financial, management, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. Use of IT Systems in a way that suggests CIHP endorsement of any political initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes CIHP involvement, except for authorized purposes in consultation with CIHP leadership.

4. **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another. This constitutes gross misconduct and appropriate sanctions will apply as defined in the employee manual.

5. **Use damaging the integrity of CIHP or other IT Systems**. This category includes, but is not limited to, the following six activities:

i) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, ITS or Systems Administrator from using security scan programs within the scope of their Systems Authority.) This constitutes gross misconduct and will result in immediate termination as outlined in the employee manual.

ii) **Unauthorized access or use**. CIHP recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-CIHP or individuals across the network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

iii) **Disguised use**. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

iv) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

v) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any CIHP-owned or administered equipment or data from IT Systems.

vi) **Use of unauthorized devices.** Without specific authorization, Users must not physically or remotely (wifi) attach any additional device (such as an external disk, printer, personal laptop or video system) to IT Systems except otherwise authorized by the Systems Administrator.

6. Use in violation of law. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; promoting prostitution or related activities; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not

automatically mean that the use is permitted without authorization. Violations under this provision constitute gross misconduct and will result in immediate termination as outlined in the employee manual.

7. **Use in violation of CIHP contracts**. All use of IT Systems must be consistent with the CIHP's contractual obligations, including limitations defined in software and other licensing agreements.

8. **Use in violation of CIHP policy**. Use in violation of other CIHP policies also violates this Appropriate Use Policy. Relevant CIHP policies include, but are not limited to, those regarding sexual harassment and ethnic harassment, as well as CIHP general administrative and departmental work-unit policies and guidelines regarding incidental personal use of IT Systems. (Wording of the paragraph to be rephrased)

9. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

D. **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts.

E. **Encryption of Data**. Users are encouraged to encrypt files, documents, and messages containing sensitive information for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. CIHP makes available software and protocols endorsed by the IT unit that provides robust encryption, as well as the capability for properly designated CIHP staff to decrypt the information, when required and authorized under this Policy. Users encrypting information are encouraged to use only the endorsed software and protocols. Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request. A staff member may only encrypt with the permission of his or her supervisor.

F. **Responsibility for Content**. Official CIHP information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.
CIHP will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private communication of an individual user.

G. **Personal Identification**. Upon request by a Systems Administrator or other authority, Users within the office premises must produce valid CIHP identification or authorization.

H. **Hardware and Software Requirements.** The CIHP standard hardware is Windows-based computers. Computers provided by CIHP are supplied with the following software called **BCE** (Basic Computer Environment).
• Windows 7/XP Professional
• MS Office Professional, which includes Word, Excel, Outlook, Access, PowerPoint, Excel, and Publisher
• ESET Antivirus
• Acrobat Reader
Any changes to these software packages shall be at the discretion of the Systems Administrator. Any additional software user requests must be ordered through the IT Manager.
Software is stored and cataloged by Information Technology Unit. Due to licensing restrictions and in order to limit CIHP's liability, software shall not be lent out except with explicit written permission of the Systems Administrator.

I. **Procurement of IT and IT-related Equipment.** Purchases of all equipment will be subject to CIHP procurement procedures as outlined in the CIHP Procurement Policy. All costs for computer equipment will include built-in warranty agreements that protect the purchased equipment for periods of up to 3 years.

Computer hardware and software that is of no further value to CIHP will be disposed of in a manner consistent with CIHP policy/procedures and according to the requirements of the awarding agency's regulations regarding asset disposal.

Conditions of CIHP Network Access

CIHP places a high value on privacy and recognizes its critical importance in an organizational setting. There are nonetheless circumstances in which, following carefully prescribed processes, CIHP may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant CIHP access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. **Conditions**. In accordance with applicable laws, CIHP may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or

2. When required by law or administrative rules; or

3. When such access to IT Systems is required to carry out essential business functions of CIHP; or

4. When required to preserve public health and safety; or

5. When there are reasonable grounds to believe that a violation of law or a significant breach of CIHP policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

6. For Users who are no longer in the employment of CIHP: When the User's employment contract has ended and there is a legitimate business reason to access the User's IT Systems.

B. **Process.** Consistent with the privacy interests of Users, CIHP access without the consent of the User pursuant to the above (through A1 – A5) will occur only with the approval of the Chief Executive Officer or his/her designate, except when an emergency entry is necessary to preserve the integrity of CIHP or to preserve public health and safety. CIHP, through the Systems Administrator, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the Director of Management Support Services, or other appropriate authority. A User will be notified of CIHP access to relevant IT Systems without consent. Depending on the circumstances, such notification will occur before, during, or after the access, at CIHP's discretion. In the case of a former staff member, access without consent pursuant must be approved by one of the former staff member's supervisors or their successors and no logging or notice is required.

C. **User access deactivations**. In addition to accessing the IT Systems, CIHP, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

D. **Use of security scanning systems**. By attaching privately owned personal computers or other IT resources to CIHP's network, Users consent to CIHP use of scanning programs for security purposes on those resources while attached to the network.

E. **Logs**. Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of User actions, including the extent of individually-identifiable data collection, data security, and data retention.

Operational Procedures

1.1 Equipment Provisioning and Assignment

CIHP staff are provided with a computer based on overall job function and as permitted by budgets and other circumstances. Computers provided to staff may either be a laptop or a desktop, depending on user needs and equipment availability. No user will be assigned more than one computer except where such determination is made by the Chief Executive Officer.

Computers supplied by and/or paid for with CIHP funds are CIHP property and are subject to all guidelines and policies set forth by CIHP.

1.2 Hardware and Software Requirements (Please refer to section H above)

1.3 Repair

Any physical or suspected problem found with equipment purchased by CIHP should be reported immediately to the IT department.

1.4 Network Access

The CIHP Network shall be made available for all CIHP staff with a unique naming convention and password. This allows users to access the CIHP network and resources. Each user will also be able to have access to mapped drives for collaboration evolving round departmental responsibility. Access to the shared U (Unit Resources) and O (General Resources) drives is possible.

1.5 Domain Accounts

A domain account (formerly referred to as a "NetID") is required for access to CIHP computer network and domain.

This includes access to the shared CIHP-departmental drive (U drive) on the U drive, which is open to all departmental members, and the O drive which is the general storage for all network users. Users would be granted access to a domain account. . IT will provide him/her with instructions on the proper use of the CIHP computer network and domain. All account requests require the approval of the IT Manager and Director, Management Support Services.

1.6 Safety & Security of IT Equipment

Users are responsible for the security and safety of the equipment that they are assigned by the IT Manager, as outlined in these standard operating procedures. Important measures must be taken by each user and each office to provide optimal security for CIHP's IT systems.

1.7 Back-ups

No matter how careful the users, computers will eventually fail. Having recent back-ups of important documents can avoid inefficiencies and delays in CIHP operations. Network drives (G & O) are directly located on central file server and are backed up on daily-incremental, weekly-full and monthly-full backup plans by the network administrator. These backup files are kept in the fireproof safe located in the IT office. An annual full backup is conducted once a year and kept offsite with a copy made for the CEO. Users are to ensure that only official documents are stored in these drives.

States offices are provided with external hard-drives to serve as backup device for sensitive official information. The operation and safe keeping of the drives is handled by Finance & Admin staff in each of the State offices. These drives are sent to the central office in Abuja when they have almost reached their full capacity (80% and above). The network administrator subsequently carries out the transfer of the data unto the fileserver and conducts a backup operation as appropriate.

All computers in the state and site offices are backed-up during scheduled visits by the central IT team. These backups are archived in the respective state and site folders on servers at the central office.

1.8 Maintenance

There shall be a quarterly maintenance for all IT equipments both in the central office and the State offices. This shall be coordinated by the IT Manager. A maintenance schedule shall be prepared on a quarterly basis to capture systems preventive maintenance with dates, location and users.

1.9 General Security

Passwords: Users are responsible for securing the passwords to their various CIHP-assigned accounts. Users must not share their passwords with third parties.
Computer Protection: Users are responsible for maintaining the overall functionality of their computers. IT unit will facilitate the installation of periodic security updates as distributed by the respective operating system vendor. In addition, users ***must*** utilize the antivirus and antispyware software installed on the computer to keep it free from malicious threats, which are on auto-download.

2.0 Security Policies

The following should be considered for every user as IT security policies:

Each employee when signing receipt of the CIHP standard operating procedures must understand that they have agreed to conform to CIHP's IT network and computer use policies, as described here and in CIHP's IT Policy codes of conduct.

In general, no personal identifiable information should be stored on CIHP computers. Personal identifiable information is defined as any information, including, credit card numbers, and bank account numbers, that can be used to uniquely identify a person. If the user must have personal identifiable information on an CIHP computer, these files should be on local drives/resources and not on the network.

Computers with stored medical or patient data that are no longer being used by designated technical staff must be turned over to the IT Manager. All data on the computer will be erased and the hard drive will be zeroed out and/or destroyed.

Hard drives that are suspected to be faulty must have all patient data and/or personally identifiable information on them removed. If the drive cannot be zeroed out, IT Manager will contact CIHP Chief Executive Officer for guidance *before* releasing the hard drive to third parties.

CIHP employees are not expected to erase their computer drives – or even portions of their files and programs – without prior review by and approval of their supervisor with the involvement of CIHP IT Manager. Mailboxes of disengaged staff to be kept secured on the server for a minimum period of two years

2.1 Communicating Protected Health Information (PHI)

CIHP is obliged to follow U.S. government regulations stipulated in HIPAA and other federal and state privacy laws. These regulations require that CIHP takes appropriate measures when communicating protected health information (PHI) via e-mail. *Protected health information* under HIPAA includes any individually identifiable health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual, but also to data that reasonably could be expected to allow individual identification.

As a general rule, e-mail should **not** be used to communicate protected health information.

E-mail is inherently less secure than other forms of communication. However, e-mail of protected health information will be permitted if certain safeguards are implemented. These include, but are not limited to:

- E-mail communications containing PHI must be transmitted only on a designated e-mail system and cannot be forwarded to an outside e-mail account. Such information must not be originated from a public mail account e.g. Yahoo, Gmail, hotmail etc.

- PHI must not be transmitted in the subject line of an e-mail message.

- The fact that the message or an attachment to the message contains PHI must be reflected in the subject line of the e-mail message.

- The e-mail message must include the following confidentiality notice at the bottom:
- *"This electronic message is intended to be for the use only of the named recipient, and may contain information that is confidential or privileged. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately by contacting the sender at the electronic mail address noted above, and delete and destroy all copies of this message. Thank you."*

- Note: This confidentiality notice can be added to the signature block of your email signature if you currently use an automated signature.

- Protected health information (e.g., HIV/AIDS information, substance abuse treatment information, and mental health information) must not be communicated via e-mail.
- If a document that contains PHI is attached to the message, the user must verify before transmitting the e-mail message that he/she has attached the proper attachment.

- Before transmitting the e-mail message, users must double-check the message and any attachments to verify that no unintended information is included.

2.2 Server and Networking Administration

CIHP IT department is responsible for maintaining servers and other networking infrastructure in order to better support the business operations of office staff.

2.3 Computer Inventory List

Computer equipment should be fully included in the CIHP property log and inventory performed as per the CIHP property management procedures . In addition, CIHP will request at least once per year that the IT Manager perform an audit of all software on CIHP purchased computer-related equipment.

2.4 Software Policy

Users are not to install any software or programs on CIHP computers or networks without the express permission of the IT Manager or the Chief Executive Officer.

Any suspect software that has been installed must be removed from office computers immediately and the corresponding suspect media destroyed. CIHP Information Technology Unit must be notified of such incidents.

Failure to remove non-CIHP approved software is considered a violation of CIHP codes of conduct. Penalties may include, but are not limited to, loss of access to computing facilities, loss of domain privileges, or other penalties, depending on the gravity of the offence or as outlined in the employee manual.

2.5 Internet-based Telephone Service (SKYPE)

Skype is an internet-based telephone service that enables callers to make free or low-cost telephone calls from *computer to computer* or *computer to telephone* using the Internet. It also provides a good mechanism for retrieval of data. To take advantage of Skype's features and this opportunity for cost savings, CIHP staff are encouraged to use Skype where possible for *international calls*. *Inter-computer* use of Skype is free and CIHP strongly encourages staff to use this feature as well.

To use Skype, a caller needs a computer, an Internet connection, a headset, and a Skype account. Skype is free software that may be downloaded from the internet with the assistance of the Systems Administrator

Conference phones and headsets for Skype will be provided by the IT unit.

VoiP (Voice over IP) are provided in the conference room for official usage. For additional technical assistance, staff should contact IT unit.

2.6 Network security and Privacy Policies

- Systems bought with CIHP funds are considered property of CIHP and can be considered CIHP systems. Network services provided and paid for by CIHP are governed by policy set forth by CIHP.
- An employee is not permitted unauthorized privileged access or access to any account or system not belonging to him/her on any CIHP system.
- Creation of any program, Web form, or other mechanism that asks for a CIHP user identity and password is prohibited except by permission of CIHP Information Technology Manager.
- Computer and network accounts assigned by CIHP provide access to personal and confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted.
- Each user is responsible for the proper use of his or her account(s) and any activity conducted with it. This includes choosing safe passwords, protecting them, and ensuring that file protections are set correctly.
- Each system owner is responsible for the security of any system he/she connects to the network. A system seen to be attacking other systems, e.g., having fallen victim to viruses/worms, will be taken off the network, generally without notice, until it has been made secure.
- No CIHP provided network may be used as a vehicle to gain unauthorized access to other systems.
- Any user who finds a possible security lapse on any CIHP system or network must report it to the IT Manager. To protect files and the system, employees must not attempt to

use a system under these conditions until the IT Manager has investigated the problem. Compromised systems of a severe nature must be reported as well to the CIHP IT Manager.

- All users should be aware that IT Manager or their designees will conduct periodic security checks of CIHP systems and networks, including password checks. Any user found to have an easily guessed password (e.g., a blank password or brand name of equipment on the user's desk) will be required to choose a secure password during his or her next log-in process.
- User files on centralized systems (servers) are to be kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The IT Manager who assigns access to files must not override file protections unless necessary in the course of his/her duties and must treat the contents of those files as private information at all times.

2.7 Network and Computing Usage Policies

- No CIHP-provided network may be used for any purpose or in a manner that violates these standard operating procedures, or local laws.
- Employees should keep in mind that many people use CIHP provided networks for daily work. Obstructing this work by consuming large amounts of system resources (disk space, network bandwidth) or by deliberately crashing the machine(s) will not be tolerated.
- Use of any CIHP system by outside individuals or organizations requires special permission from the Certifying Authority.
- Use of CIHP-provided networks for commercial purposes except where explicitly approved, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use, and preparation and presentation of advertising material.
- No CIHP-provided computing facility may be used for playing computer games.
- Copying, storing, displaying, or distributing copyrighted material using CIHP-provided networks without the express permission of the copyright owner, except as otherwise allowed under copyright law, is prohibited.

2.8 Email Usage Policies for @cihpng.org Accounts

- No e-mail message may be sent or forwarded through a CIHP provided networks for purposes that violate CIHP statutes or regulations or for an illegal or criminal purpose.
- Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness.
  CIHP IT administrators of central e-mail systems will not read mail unless necessary in the course of their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining computer networks and in carrying out other day-to-day activities. On central systems, e-mail messages that cannot be delivered to one

or more addressees are directed to the system administrators for purposes of assuring reliable e-mail service, in most cases as “headers-only.”

- Users should be aware that their “deletion” of electronic information will often not erase such information from the system's storage until it is overwritten with other data. It may, in any case, still reside in the CIHP's network either on various back-up systems or other forms, and even if erased, may still exist in the form of print-outs.
- Nuisance e-mail or other online messages such as chain letters and obscene, harassing, or other unwelcome messages are prohibited.
- Unsolicited e-mail messages to multiple users (“mass e-mails”) are prohibited unless explicitly approved by the appropriate leadership authority.
- All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.
- CIHP reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass, or commercial messages, or messages that appear to contain viruses to CIHP or other users, and to filter, refuse, or discard such messages.
- Violations of these CIHP policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to eventual revocation of access. Serious violations of the policy will be referred directly to the appropriate CIHP, or outside authorities; unauthorized use of CIHP computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from CIHP and/or criminal prosecution.

2.9 Additional CIHP Policy on Mass E-mails

CIHP maintains a variety of mailing lists for the benefit of distributing information quickly and widely through mass e-mails. Each mailing list is established for a particular purpose. It is urged that all users carefully review the content of their messages and ensure its content is appropriate ***before they post a message to a mailing list***. Utilizing CIHP established mailing lists for communication that is not directly related to the mission of each mailing list, or of the CIHP as a whole, may result in administrative action by the appropriate CIHP authorities. Should the need arise; e-mail lists may be disabled at the discretion of the IT Manager.

2.10 Internet Usage

CIHP acknowledges that the internet is an important information resource for staff and can improve the efficiency in the use of agency software. CIHP encourages staff to use the internet as a work resource, but also acknowledges that the internet is a recreational tool. The following are guidelines for use of internet within the CIHP office.

Surfing the internet should be done when looking for information relevant to official CIHP business. The internet can also be used for reading newspapers to catch up on

world events. All other recreational surfing should be done outside of office hours which are before 8am and after 5pm daily.

The IT Manager or designee will monitor the use of the internet and can produce reports detailing the amount of time spent on the internet and which sites are most frequently visited. These can be requested by the leadership at any time, and further policies can be based on previous usage history.

Surfing the internet to look at pornography or hate-based web sites is grounds for removal from the network and disciplinary action.

Intense personal net surfing will be considered a disciplinary issue, and a written warning given by offender's supervisor.

Surfing the internet to view film clips is prohibited. – viewing this material consumes server resources, bandwidth usage and clogs network activities. If there is a requirement to view a film clip, there will be need to request permission and guidance from the IT Manager.

2.11 Closed User Group (CUG) Accounts

CIHP maintains a Closed User Group with a telecoms company for all its employees. Closed User Group (CUG) allows persons within a predefined "user group" to make and receive unlimited calls within the same group. A monthly subscription fee applies for each member in the defined CUG. CIHP has established the CUG with Glo Mobile – One of the telecoms companies in Nigeria to provide services to its employees.

Once a CUG account is activated for a CIHP employee, he/she can place and receive calls to/from other employees and colleagues within the CUG without incurring call charges. However, discounted rates will apply for calls made to numbers outside the CUG.

This service enables CIHP to make significant savings on communication costs as employees have the ability to make unlimited calls and send text messages within the group. It also seeks to prevent abuse of the service for non-business calls.

CIHP provides a monthly credit allocation to various categories of employees to ensure their telephone lines are functional and reachable. Staff are encouraged to maintain the statutory minimum balance in their accounts for the service to remain active at all times. Staff who exceed their monthly credit allocation are responsible for offsetting their bills so that their accounts can remain active.

Enforcement Procedures

A. **Complaints of Alleged Violations**. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established CIHP Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment harassment). The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the Human Resources/Admin Unit, which must investigate the allegation and (if appropriate) refer the matter to CIHP leadership for disciplinary action.

B. **Reporting Observed Violations**. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the IT Unit, which must investigate the allegation and (if appropriate) refer the matter to CIHP leadership for disciplinary action.

C. **Disciplinary Procedures**. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for as outlined in the CIHP Employee Policy and Procedure Manual, and other applicable policies.
Systems Administrators may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators and the IT unit are authorized to investigate alleged violations.

D. **Penalties**. Individuals found to have violated this Policy may be subject to penalties provided for in the employee manual. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Chief Executive Officer.

E. **Legal Liability for Unlawful Use**. In addition to disciplinary measures by CIHP, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. **Appeals**. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

Policy Development
This Policy may be periodically reviewed and modified by the Chief Executive Officer for Board Chairperson's ratification; the **CEO** may consult with relevant staff in the IT unit.

Chairperson Board of Directors

09/05/2012
Date