Information Systems Security Policies and Procedures –V1.0

ARMAUER HANSEN RESEARCH INSTITUTE - AHRI

INFORMATION AND COMMUNICATION TECHNOLOGY

Addis Ababa, Ethiopia

Information Systems Security Policy and Procedure

ISSPP # V1.0 – IS Security Policies and Procedures

Armauer Hansen Research Institute - AHRI

Version: 1.0

Date: 2021/06/01

AHRI

Information Systems Security Policies and Procedures: ISSPP-V1.0

ISSPP #	V1.0
ISSPP title	ISS Policy and Procedure
Classification	Confidential
Executive Owner	IT Team
Custodian	Systems Engineer – Information Security
Version	1.0
Effective from	2021/06/01

Version Control

Version: 1.0	**Release Date: May 2021**
Title	Information Systems Security Policies and Procedures: ISSPP
Status	Final Draft
Version no.	1.0
Policy Author	Wondwossen Amanuel, Bamlaku Tilahun, Mulatu Biru (PhD)
Policy Owner	AHRI
Approved by (Name, title, date)	DDG/KMD of AHRI Alemseged Abdisa (PhD), Mulatu Biru (PhD)
Approval date	May 2021
Next review date	2022

Document Revision History

Version:	Release Date:	Author(s):	Revision Notes:

Contents

Preface

Armauer Hansen Research Institute (AHRI) was founded in 1970 through the Initiative of the Norwegian and Swedish Save the Children Organizations seconded by the Ministry of Health of Ethiopia. AHRI was established as a biomedical research institute located next to the all Africa Leprosy Rehabilitation and training Hospital (ALERT). Since 2016 February, the institute has been reestablished as the FMOH's biomedical research agency with the nationwide responsibility in research and innovations related to biomedical technology, biotechnology, clinical research, genetics, bioinformatics, systems epidemiology and medical technology. Further, the Institute should continue to play significant role in capacity building including in medical research training and strengthening research systems for clinical trials in the country.

As the institution expands its capacity and collaboration with both national and international institutions, it became essential to develop an Information Systems Security Policies and Procedures (ISSPP) document. This Information Systems Security Policies and Procedures (ISSPP) is a roadmap with specifications, standards, and best practices towards the adoption, use, maintenance, and value extraction at reasonable cost from ICT resources. Every action taken in the institution that uses or impacts ICTs must be guided by this Information Systems Security Policies and Procedures (ISSPP) document. The policy document comprises four chapters. First, the general use and practice of Information System Security Policy & Procedures; second, the email policy; third, the internet usage policy and finally the website and social media administration policy.

Introduction

To this end, the Ethiopian Government has given attention for the use of ICT to support socio-economic development as well as Ethiopia's on-going process of democratization and sound governance. In order to proactively meet this growing information security need, AHRI has decided to implement Information Systems Security Policies and Procedures (ISSPP) that would direct and guide the IS security practices at AHRI.

The current practices of the institute regarding Information System are not to the standard of the pace of the world. Starting with the purchase of any IT items, all workstations are not under Active Directory Domain Control and all software's which are being used for the institutional research purpose are not licensed. This are some of the existing gaps which makes the institute vulnerable for outside unauthorized access and the reason for the making of this policy.

AHRI being a research center with ground breaking outcomes providing Infrastructure deployment services, requires a solid – yet flexible information technology infrastructure in order to survive and to excel in this service provision. In order to achieve this, AHRI's IT infrastructure and IT operations must meet the needs of confidentiality, integrity, availability, efficiency, and effectiveness.

Armauer Hansen Research Institute (AHRI) set out this ISS policy & procedure as an underlying guideline for proper, efficient, and effective use of ICT to succeed in achieving its mission and objectives. The ISSPP articulated in this document provides guidelines and framework:

- as a program of actions for implementation and use of ICT
- it describes critical areas for the development and application of ICT in AHRI;
- It lays out a road map in terms of AHRI's overall vision and the corresponding mission and strategies for guiding and supporting AHRI's activities by using ICT as enabling tool.

This document is organized in to four chapters. The general use and practice of Information System Security Policy & Procedures are described in detail on the first chapter. Chapter Two discussion contains the Email policy. This policy applies to all email services provided by AHRI to all users and users of such services or information assets of AHRI, including but not limited to AHRI employees, employees of temporary employment agencies, vendors, research partners, contractors and all third parties.

Chapter Three outlines the Internet usage. This policy applies to all Internet services provided by AHRI to all employees of AHRI employees of such services or information assets, including but not limited to permanent full-time and part-time, contractual; AHRI employees, employees of temporary employment agencies, vendors, research partners, contractors and all third parties.

Finally, Website administration is briefly conferred on Chapter Four. AHRI's Web service supports official pages, and verified social media links.

All the Information System Security Policies and Procedures in the institution's presence must comply with the laws of Ethiopia.

Purpose

The purpose of this policy is to establish the framework governing Information System Security within AHRI, and to establish the Information System Security Management System (ISSMS) of AHRI's team. Every stakeholder, permanent and contractual employees, internal and external donors have responsibility to safeguard sensitive information kept with AHRI.

This ISSPP forms the foundation on which the information security system would be built at AHRI. These are directives and guidelines established by the senior management team of AHRI for all employees of AHRI and other users of the AHRI's Systems and IT infrastructure. The general purpose of this policy is to Institute Equipment Acquisition, Installation, and Maintenance procedures and guidance for the proper acquisition, installation, and maintenance of IS equipment/s.

The *email policy*, which is addressed under chapter 2, is to minimize risks associated with email services, reduce legal risk, and the delivery of best practice information to employees, to secure a greatly improved institute focus. Chapter 3 elaborates on the *Internet policy*, informs the employees of AHRI that the Internet services and their rights and responsibilities of AHRI's requirement that its Internet facilities are used in a legal, ethical and responsible manner to ensure that Internet facilities are used as an efficient mode of doing its research and/or administrative communications. The last chapter on this policy document is about the official *web platform* that applies to all the research and related content/s/ being published by AHRI on the web and social media portals.

For proper usage of any IT services, users are required to firmly adhere to this ISS policy.

Scope

This policy applies to **all users** of IT assets of AHRI, including AHRI employees (permanent & contractual), researchers, consultants, research partners, visitors, and vendors. The Information System Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Institute information and technologies, including external parties that provide information processing services to the Institute.

This policy applies to all information systems environments (IS Environments) operated and/ or used by AHRI, including those information systems accessed under formal or informal agreements with external parties and associated entities of AHRI.

It is important to acknowledge here the dual role of IT professional staff as both IT system administrators and as staff who are also "standard ICT users". This policy will apply to those staff while in their role as "standard ICT users".

However, in the course of their professional duties, IT staff may be required to undertake actions which are beyond those permitted in this policy. It is expected that they will do so in the spirit of both the AHRI's code of conduct and appropriate professional codes of ethics.

Pillars Information Systems Security Policies and Procedures (ISSPP)

This ISSPP is based on the following key pillars:

1. Proclamation No.1072/2018 Electronic Signature Proclamation
2. Proclamation No. 958 Computer Crime
3. Proclamation No. 808 Information Network Security Agency Re-establishment
4. The National Information and Communication Technology (ICT) Policy and Strategy

Structure

The Institute will implement an Information Security Management System based on the ISO27002/ISO27001 International Standard for Information Security. The Institute will also reference other standards as required, mindful of the approaches adopted by its stakeholders.

ICT Project Management

For any ICT related project/s task, request may come from within the IT Team, a researcher, or others, must be done in consultation with the IS team. The relevant shareholder/s and stockholder/s must come to common consent with clear terms, plans, and specifications/requirements before the start of a project. Preparing a project charter document, including costs, tasks, deliverables, and schedules is mandatory.

Regardless of the software development methodology used (waterfall or agile), all methodologies have similar activities associated with successful execution. The ICT Team leader shall be responsible for contracting or developing, maintaining, and managing a Software Development Life Cycle (SDLC).

All software developed in-house which runs on production systems shall be developed according to the established processes and procedures. At a minimum, SDLC activities and tasks should address the following ten activity areas:

- Project Initiation/Definition
- Risk Assessment
- Functional User Requirements
- Technical and Architectural Systems Design
- System Programming or Customized Off the Shelf (COTS) Software Development/Acquisition
- Quality Assurance
- Documentation and Training
- Systems Testing and Acceptance
- Installation
- Maintenance / Application Sunset

These projects can be new or modifying/scaling up of the existing infrastructure, but not limited to CCTV installation, Software development, Website design and development, Telephone system/Private automatic Branch Exchange (**PABX**), Enterprise Resource Planning (**ERP**), Changing of service provider, etc.

Any outsourced or inhouse project/task must abide to this ISS policy document.

Approval of Policy Document

This policy document was discussed and approved for productive use by the Armauer Hansen Research Institute

Director General in [Date].

Signed: _____

Chapter 1: ISSP

1. Information Security

Within the context of this policy, the term "security" in relation to information must mean the safeguard and principles of Confidentiality, Integrity, and Availability properties of the information, as per the definitions given under glossary.

2. Information Security System Governance

Information Security System-ISS services in AHRI is managed by ICT Case Team.

2.1. ICT Case Team

There is an ICT Case Team to oversee and advice on ISS development and use in AHRI. The case team must report to Knowledge Management Directorate-KMD.

The roles of the ICT Case Team are to:

- review and advise on ICT policies, plans, projects and activities
- support in the development and enforcement of ICT standards, policies and procedures in the Institute
- advise on the acquisition of major software and hardware resources
- installing, maintain, and troubleshoot security systems and infrastructures, with inhouse capacity or otherwise outsourced
- promote the harmonization of ISS development activities by all Institute Research and Administrative units
- identify and promote strategic partnership programs and areas of collaboration with other research institutions in deepening the use of IS and research
- provide quality assurance on the content, look and feel of the research's website, provide guidance to the Head of the ICT Office, and advise the Directorate on matters related to IS as and when required.
- there must be a shared responsibility among IT Staff and relevant system related information's must be kept in a hardcopy and soft copy formats. Such information's must be kept up-to-date.

3. ICT Equipment's

Information System (IS) equipment refers to computers, computer peripherals, printers, scanners, hubs, switches, routers, servers, networking cables, copier etc. The purpose of this Institute Equipment Acquisition, Installation, and Maintenance Policy is to provide procedures and guidance for the proper acquisition, installation, and maintenance of IS equipment.

Users must follow the ICT equipment acquisition, installation, and maintenance policy in this document.

3.1. Acquisition

Any ICT equipment purchase request must follow the institution procurement and purchase procedure with consultation of ICT office. Grants and donations, which are written on behalf of the Institute, which require the purchase of ICT equipment, must adhere to this policy.

3.2. Installation

ALL desktops, laptops, & tablet computers must be registered and connected to the domain server (ahri.gov.et)

- ICT Office must keep update of ICT inventory list of all ICT equipment's with relevant details.
- Only personnel authorized by the ICT Office must install and configure ICT equipment that belongs to the Institute after consulting the installation guide and manual of the respective equipment. Such personnel are responsible for the safety of the devices they install.
- All configured and installed ICT equipment must be fully and comprehensively tested and formally accepted by users before being transferred to live environment/end users.
- Computers, workstations, laptops, and smart phones or other removable storage devices such as USB drives or memory sticks may be connected to the Institute network subject to the regulations of acceptable use as set out by the ICT Office regularly.

3.3. Maintenance

For a regular preventive, and corrective maintenance of ICT equipment's, which can be performed by the IT team

- Adequate resources must be made available by the institute
- The Institute must put in place an elaborate program of refurbishment and replacement of obsolete and outdated computer equipment.
- All ICT equipment owned, leased or licensed by the Institute must be supported by appropriate maintenance facilities by qualified technicians.
- Deliberate or accidental damage to the Institute's ICT property must be reported to the officer in charge of ICT security as soon as it is noticed.
- Office machinery (copier, printer, fax ...) regular maintenance, based on their service period, can be outsourced to third party.

4. Software

Any purchase of software must follow the procurement and purchase process of the institution. With this if there are any new software development programs or project within the institution it must adhere to the same procurement and purchase policy. And all must go in consultation with the ICT office.

All software installed on Institute-owned equipment must have a valid license for use, from well-known vendors, because of continues security threats from outsiders (hackers, malicious files, using flash/USB drives, pirated software's). This is not only limited to application software's but also main operating systems of any desktop, laptop or tablet devices must also have a registered license.

All software installations should be performed by the Institute ICT staff, no user must have the right to install any kind of software's on their institute given devices unless authorized or having proper clearance by the director or senior management. Regular installation, update & maintenance of software's must be managed by the ICT office, users will download and install applicable software updates as they become available from software vendors.

ICT staff will maintain an inventory of software installed on Institute-owned equipment and the appropriate licenses for the installed software.

5. Physical and System Access Control

Information, data, and all electronics equipment's are to be make secured by applying a corresponding protective mechanism. And privacy of data, information, and materials need to be protected in consideration of Confidentiality, Integrity, and Availability. Ensure that materials and resources are only made available to those persons with a legitimate right of access. Deliberate attempts to degrade the performance of the Institute network or to deprive authorized personnel of resources or access to any AHRI network facilities is prohibited. Breach of security includes, but not limited to, the following: creating or propagating viruses, hacking, password grabbing, disc scavenging, social engineering, etc. The Institute must give high priority for preventing threats from being materialized and therefore users are required to adhere to this security and safety policy. The institute ICT team shall work to address network and computer software vulnerabilities and loopholes in the system.

This also means to invite outside firm to audit the institute network security infrastructure and report to the Directorate with mitigation plan.

5.1. Physical Security

The Institute, through the ICT Office, must set out procedures and operation manual with the consideration of preventing anticipated threats that may damage physical devices. AHRI ICT facilities must be adequately protected against fire, water and physical damage.

5.1.1. General

All Institute computer hardware must be marked, either by branding or etching with the name of the Institute unit and name of the office or computer laboratory where the equipment is normally located. All doors giving access to rooms or areas with computer equipment both from within and outside the building must, as a minimum, be fitted with metal grills.

1. In general, there should at least be one substantial physical security measure in place at all times to protect unattended information assets.
2. The Institute must identify and isolate secured areas (such as server rooms) from physical contact or access. Secured areas must be entered only by authorized personnel.
3. Rooms and buildings incorporating high-density computer equipment must have high-level physical security where applicable. At least 2 of the below lists in consideration of the industry best practices
    - ☐ Intruder detection (burglar alarms),

- ☐ Environmental monitoring and alerting systems,
- ☐ Strong rooms,
- ☐ Door and window locks,
- ☐ Systems to control and log access to sensitive areas,
- ☐ Out-of-hours security support,
- ☐ Specialized fire extinguishing systems (which may be automatic).
- ☐ Where applicable security personnel must also be used.

4. Staff must keep the doors and windows of unattended offices locked.
5. During non-working hours, secure areas must be protected against intrusion by appropriate access control, locks, and surveillance systems or by security personnel.
6. The Institute must put signs or sign board labeled as "Authorized Personnel Only" in areas where there is physical access restriction.
7. Construction and other civil works made around the Institute ICT infrastructure must be done in consultation with the responsible office and without damaging the surrounding infrastructure.
8. Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

5.1.2. Servers

All servers (Web server, File server, Database, Printer server, … etc.) must be kept securely under lock and key. Computer servers must be housed in a room built and secured for the purpose. Computer server rooms must contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

There must be a CCTV camera installed inside server room. Access to the system console and server disk or tape drives must be restricted to authorized personnel only.

Other related standard safety protocols must be put in place for security purpose.

Third parties authorized to support the institution in server infrastructure or provision of service must respect all the regulations set out in this policy.

5.1.3. Workstations

All workstation must have proper and standard naming (AHRI-Dep't-Office/Designation of the user)

- ➢ All workstations must be registered under the domain server
- ➢ All users of workstations, personal computers or laptops must ensure that their user account is logged out & their screens are locked when not being used and switched/turned off outside working hours.

5.1.4. Network Equipment's

LAN and WAN equipment such as switches, hubs, routers, and firewalls must be kept in secured rooms. Around office corridors, the equipment must be stored in lockable communication cabinets.

- ➢ All network switches must be manageable devices.

- All communication cabinets must be kept locked at all times and access must be restricted to authorized personnel only. Whenever legitimate access to communication cabinets is necessary, it must be done with physical supervision of the responsible personnel.

5.1.5. Wiring

- All network cabling must go through casing and in-built wiring where possible. After a wiring is complete, no cable must be left visible, uncovered, and directly exposed for damage.
- All internal or external network wiring must be fully documented using convenient means including positioning technologies like GPS.
- All network outlet must be labeled and documented properly
- All network cables must be periodically scanned and readings recorded for future reference.
- Users must not place or store any item on top of the network cabling/casing.
- Redundant cabling schemes must be used where possible.

5.1.6. Monitoring Software

The use of monitoring tools, such as network analyzers or similar software, must be implemented and restricted to authorized personnel who are responsible for network management and security purpose only except when explicit permission is given for administration and research purposes by an authorized person. Network monitoring tools must be securely locked when not in use.

Purposefully scanning internal or external machines in an attempt to discover or exploit known computer software or network vulnerabilities is prohibited.

5.1.7. Electrical Security

Power feeds to servers and workstations must be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure. All switches, routers, firewalls and critical network equipment must be fitted with UPS. Generator power with auto-restart function must be provided to help protect computer systems in the case of power failure.

5.1.8. Inventory Management

The Institute must keep a standard complete and updated inventory of all ICT infrastructure equipment's and software's in use. Computer hardware, software, network infrastructure, and maintenance tool kits audit must be carried out periodically, at least twice a year, to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

5.2. System Access Control

The Institute, through the ICT Office, must set out procedures and operation manual with the consideration of preventing anticipated system security threats. System security scrutiny to asses for vulnerability and penetration test can be done both with the internal IT Team capacity and outsourced for checking any susceptible areas and loopholes.

5.2.1. Antivirus

The Institute must install standard and licensed antivirus software to ensure that all servers, workstations, and notebooks owned by the Institute are protected against computer virus infection. Antivirus software(s) must be updated on a regular basis.

5.3. Logical Access Control/ Identity Management

Appropriate domain control mechanism must be put in place for the same purpose. Access to network facilities must be through user IDs and passwords. All users must have user account and access rights and privileges that must be set accordingly. When a user is accessing AHRI' resources they must provide his/her own personal credentials for authentication, to identify the user.

- AHRI facilities must not be used for anything that may bring the name of AHRI into disrepute or expose AHRI to the risk of civil action.
- Intentional creation, execution, forwarding or introduction of any viruses, worms, Trojan horses or software code designed to damage, self-replicate or hinder the performance of AHRI network is prohibited.
- Accounts on all systems must be audited quarterly-four times a year for validity.
- The institute does not export or bulk transfer identities, passwords, or personal information to third parties for authentication or any other purpose.

5.3.1. Network Control

Connecting any computer device to AHRI network unless it meets the security standards established by the Institute is prohibited. The setup of network monitoring/detection, control/prevention, and security infrastructure for network access must be done by the ICT Office or under its direction.

- Next-generation firewall-NGFW, Intrusion Detection System-IDS and Intrusion Prevention System-IPS must be put in order to secure the institute network
- Involving in pervasive computation for financial gain without the knowledge and explicit permission of the Institute is prohibited.
- Permission must be sought from the ICT Office for any third-party network connections to the Internet or any external networks.
- The Institute network infrastructure must be secured against email spam, intruders or hackers, break-ins, viruses, Trojan horses, worms and other disruptive software.

5.4. Remote Access

Any remote access to AHRI servers is generally prohibited. Remote access permission can be granted under special circumstances like support vendors, file transfer to partners and so on. In the occurrence of such event, requests and approval procedures must be followed.

Remote access mechanism must be through secured Virtual private network-VPN.

Clear procedure on situations and scenarios of asking a remote access must be prepared and refereed when the need arises.

5.4.1. Remote Access Requirements

- Secure remote access must be strictly controlled with encryption (using secured VPN)
- Authorized users must protect their login user name and password.
- Remote machines that are connected to AHRI servers via remote access must use the most up-to-date anti-virus software.

5.4.2. Requesting Remote Access and Authorization Procedures

- The directorate who want to have or be grant remote access for themselves or others must initiate the request and submit to ICT team, at least ten working days prior the activity, using the appropriate format.
- The ICT team should evaluate the request according to the procedures and forward it to top management for approval.
- If the top management approves the request, the ICT team will authorize and provide the appropriate credential to access the remote machine for a limited period through a safe and secured mechanism.
- Access will be granted with a limited time frame or by giving a unique username and password with expiration date.
- The server will be monitored with audit log, during or after, for any activity and transaction done using the permitted server/computer.

6. Transfer and Disposal of Computer and Software

The Institute unit must work with the ICT Office to ensure that procedures consistent with security best practices are followed for the reliable removal of licensed software and confidential data before equipment transfer or disposal takes place. ICT equipment owned by the Institute may only be disposed of by authorized personnel who have ensured that the relevant security risks have been mitigated.

- Disposal of devices must not entail environmental damage or abuse and must follow the disposal instruction manual of the respective hardware.
- All computers must be fully formatted and restored to factory default before they are transferred to new staff user
- Any computer hard disk must be removed from the device and kept in safe location before disposal or transfer of the computer to outside organization, as donation or other purpose.

6.1. User Responsibilities

Only eligible users must be allowed to use the Institute's ICT facilities. The user as a whole must not use the facilities, software, services and systems in any illegal or otherwise unauthorized manner. Using computing resources (CPU time, disk space, bandwidth) in such a way that causes excessive strain on the computer systems or disrupts, denies or creates problems for other users must not be exercised.

- The deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users is prohibited.

- The Institute reserves the right to monitor and record all activities within the Institute when users access the facilities, software, services and systems. Users must take all reasonable steps to ensure that computer equipment in their possession or under their control is protected at all times against theft and accidental or deliberate damage.
- For any damage of ICT equipment under the care of the user, the user is accountable for any improper use and/or unauthorized access. And must be responsible upon the human resource and finance policy and procedure of the institute.
- Personal laptops and other computers connected to AHRI Net must adhere to the following.
    - Their operating system and any installed software must be fully licensed and kept up-to-date.
    - The owner of a private system (e.g., a desktop computer system in an institute member's office) that is connected to AHRI network is responsible for ensuring that unauthorized individuals do not use the system.

7. Applicability and Use

The main objectives of this section of the Institute's Information Systems Security Policies and Procedures are the presentation of the detailed specifications of who the target users are and the terms and conditions for the use of the ICT resources to ensure that the resources are used in an effective, efficient, ethical and lawful manner. The policies set out in this section have two components: the specification of the target users and the unacceptable activities in the use of ICT resources.

7.1. Applicability

The following must apply to and govern use of ICT resources

- All AHRI offices and hosted societies or research offices that make use of the ICT resources within AHRI.
- All ICT systems, equipment, connected locally or remotely to the AHRI ICT infrastructure.
- All AHRI owned and administered ICT infrastructures including, but not limited to, servers, network devices (such as routers, switches, backup power supplies, cablings both fiber and copper), personal computers, network equipment, operating systems and application software.
- All connections made to external networks through the Institute network.
- All ICT related data, report and reports derived from the ICT facilities within the Institute. ICT projects, planned or in progress.
- The public other than users of the Institute may access information as set by the Institute via the official Website.

7.2. Users

Users of AHRI ICT infrastructure, facilities, and resources include Research and Administrative staff (permanent as well as contractual employees), currently enrolled MSC and PhD students, collaborating/ visiting researchers, guests, and other affiliated individuals or organizations authorized by the Director or his/her designate. A user may be given access to all or a particular part of ICT facilities, depending on the individual work or study requirements, same access as approved by the Director.

7.3. Rights

Users have the right to use ICT facilities to carry out legitimate activities. Users have also the right to privacy while engaged in legitimate activity. This right may on occasions be superseded as indicated in Section 7.4 below (Privacy).

7.4. Privacy

Users have legitimate expectation to privacy in carrying out their activities. In general, the Institute does not monitor or restrict the content of material transported across AHRI Net. The Institute, however, has a legitimate right to inspect any data on a computer system on AHRI Net (regardless of data ownership), to prevent, detect or minimize unacceptable behavior on that computer system. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved. This section formalizes these principles.

- The Institute, through the ICT Office or other authorized agents, may monitor any device or terminal without notice.
- In the course of carrying out computer system auditing operations, the Institute may access and copy any file on any computer system owned by the Institute. Subject to all other conditions of this policy, the Institute is obliged to maintain confidentiality of the data it acquired as a result of such access.
- The Institute has the right to give to any appropriate member of the Institute community, or law enforcement bodies, any information it possesses regarding the use of the Institute's resources.
- The Institute may authorize specified personnel whose duties include monitoring the use of AHRI Net facilities to investigate the suspected security breaches or unauthorized access.

7.5. Violation

The consequences or penalty to follow as a result of non-compliance to the Policy or other regulation set forth in the Procedure Manual must be adequately detailed in an unambiguous and concise manner in subsequent document(s) that may be produced during the implementation of this Policy.

Furthermore, any offence committed against this policy is subjected to penalty in accordance with the Institute's legislation and/or by the respective law of the Federal Democratic Republic of Ethiopia.

8. Password policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts, computer login &/or email. It is the responsibility of the user to secure their devices, personal or company given, hence follow the below bullets

- A user company given device's must be registered under the institute domain and governed by group domain policy rules
- Users must change their passwords after their first login and on regular basis
- All passwords must consist solely on combinations of Numeric, uppercase and lowercase Alphabetic characters with a minimum length of 8 characters and maximum of 20

- Use must not have a password that is the same as the username, recycled or previous passwords or a name which is associated with the user
- Password expires with in a maximum of 90 days, with an advanced prior reminder for the user
- Passwords must not be stored by a system in any other form than that using non-reversible encryption, and passwords should not be transmitted unencrypted
- Use of user accounts or credentials without the consent of the legal holder of the credential is prohibited
- Furthermore, users of systems will not divulge passwords, pins, private keys or similar elements to anyone else, and they will not exploit sessions left open or otherwise steal the "identity" of another user
- During resignation or termination, employee must handover their credentials to the IT team leader. The IT Team leader must change the departure employees' passwords on his/her first-time login.

Any employee found to have violated this policy may be subject to disciplinary action.

9. Administration

Administration of the ICT resources and services at central, local, and personal level is one of the core functions of the ICT Office. The central level relates to managing primarily the backbone network platform that includes AHRI data center, network server farms at central, cables and active network devices between Departments and between buildings. The departmental computer and resources, including specialized software and equipment, are considered to be local and AHRI controls their respective access to the network and supports their proper administration. Staff members who have their own desktop or laptop computers are responsible for their equipment.

9.1. Information Security Incident Management

1. Guidance will be available on what constitutes an Information Security incident and how this should be reported.

1.1. General Data Privacy Regulation (GDPR): Any data breach MUST be reported to the directorate within 72 hours of notification after the incident.

2. Actual or suspected breaches of information security must be reported and will be investigated.
3. Appropriate corrective action will be taken, and any learning built into controls.

9.2. Server Administration

- The administrator of a server connected to the Institute network is responsible for the security of that system.
- The System Administrator monitors logs accesses, and keeps other system logs that could be useful in establishing the identities and actions of people, programs and processes that use the system.
- Units that operate publicly accessible computers (i.e., computer lab/s) connected to the Institute network must implement safeguards against network abuse.

- Data that are considered confidential must not be publicly accessible. Administrators of servers containing confidential data are responsible to reasonably secure these systems so as to reduce the threat to the Institute as a whole.
- All servers that provide access to the Institute network or Internet services must require user authentication for authorized access.

10. System and Configuration Change Management

AHRI keeps a detailed recording and updating of information that describes its computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied and locations and network addresses of hardware devices.

The Institute must ensure that all system configurations and changes are introduced in a controlled and coordinated manner. All system and configuration changes made to major system units and infrastructures must be recorded on the change management log.

11. Strategy of Implementation

In order to achieve the goals and objectives of the Information Systems Security Policies and Procedures, the ICT office must steadfastly pursue the following broad strategies.

- Design state-of-the-art service network infrastructure & communication systems that allow all users to communicate to each other easily.
- Set up organizational structures for the ICT Office and define duties and responsibilities of
    - the director of the ICT Office,
    - each service under the director, and
    - each team under each service.
- Adopt methods and procedures to ensure that required ICT system(s) is/are developed, deployed, and configured for serving the various components of the Institute' s governance structure; and follow-up and coordinate the proper and efficient utilization of ICT resources.
- Promote and facilitate the participation of users and communities in ICT development.
- Support the development of ICT systems and programs that enhance the participation of women and the physically challenged.
- Conduct awareness creation and capacity building through specialized and result-oriented training.
- Establish public information gateways or portals to harness, develop, and integrate public information resources.
- Promote bilateral and multilateral cooperation with organizations involved in the development and promotion of ICT.

12. Policy Statement

It is the policy of AHRI to ensure the security of all information owned by or kept in the custody of AHRI. The security provided to information must be commensurate with the value of the information assets to AHRI and the risks associated with such information assets.

13. Business continuity plan

Business as usual for the institute is doing research projects without or very limited down time. And any related office/ administrative activities. This is to address Disaster Recovery (DR) plan integration for countermeasure actions to be placed for security threats which might or might not occur. This may befall from nature or man-made causes.

While these instances may occur unplanned and without any prior warnings yet we MUST plan and prepare for such conditions. To mitigate such instances the institute MUST put a business continuity plan and prepare such guidance.

1. The Institute will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs.
2. This will include appropriate backup routines and built-in resilience.
3. Business continuity plans must be maintained and tested in support of this policy.
4. Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

Questions to be answered

- *Is there a requirement to keep the institute running in an event of power outage?*
  - ✓ *If so how long is the minimum/maximum tolerable/acceptable duration?*
  - ✓ *What is "Plan B"?*
    - *Plan B: Disaster Recovery back up site with a different geographic location that has **Cold/Warm/Hot** synchronization automation? (**Cold** is a dead site updated once or twice a year; **Warm** is regularly update site within weeks of backup interval; **Hot** is an active backup site with frequent update)*
- *Who are the decision makers that can provide the necessary information to move to Plan B?*
- *Is the institute willing to pay for a system not being used "Plan B"?*
- *Is the insurance policy? Does it cover such costs?*

Chapter 2: Email

Email service is one of the major services on the AHRI Net. The Institute must provide email services on its network to support its Research and Administrative functions to all users. In order to enable users share information, improve communication, exchange ideas and improve productivity, the Institute encourages the use of email.

For proper usage of the email service, users are required to firmly follow this email policy.

Use of email services to create, send, forward, reply, copy, store, print, or possess Email messages are captured in this policy.

1. Policy Statement

1.1. Ensure Email communication is secure and efficient

The service provider must ensure that Email and related services to AHRI, remains secure, and efficient and Email communication within the AHRI network facilities is reliable to an acceptable level of quality. The service provider is expected to provide an effective access control mechanism as per the conditions agreed in the Service Level Agreement (SLA) forged between AHRI and the relevant service providing entity.

1.2. Provision of Email accounts to the eligible

AHRI need to provide Email accounts to the eligible personal to perform their work.

1.3. Messages sent and received are property of AHRI

All messages sent and received by employees via the institute Email are considered as records and property of AHRI.

2. Use of Email Services

a) A user must send their email account request to their respective director for approval then submit the approved document to ICT Office.
b) Email and related services must be used primarily for research communication and admin purposes, unless management has specifically approved non-research usage.
c) Each Email account user is responsible for management and housekeeping of their Email account and for the maintenance of the confidentiality of its contents.
d) All Email account holders must choose “strong” passwords (a “strong” password is one that is hard for others to guess - it should contain a mixture of letters and numbers and should not be as simple as a birth-date or similar to the user’s name).
e) Blanket forwarding of Email messages with large attachments, including but not limited to, high resolution graphics, images, audio and video files, are prohibited.
f) No individual may use or access an Email account assigned to another individual to either send, receive or read messages.

g) An Email account, login credentials and rights are non-transferable and must not be left unattended and accessible.
h) Sending bulk unsolicited Emails (commonly known as SPAM) and/ or knowingly propagating malicious code (commonly known as virus) are strictly prohibited.
i) Create / send Email under another's name (forgery): and create / send / forward obscene, abusive, fraudulent, threatening or repetitive messages are strictly prohibited.
j) Users must not send confidential or sensitive information (e.g., any type of corporate data) via Email to external parties.

2.1. Security and Confidentiality

a) The contents of email messages sent or received are generally intended to be confidential.
b) A user's email address may be included in the Institute's Phone Book Database
c) A user's email received/sent through AHRI is considered private. The Institute must not read the content of an email unless there is a court order.
d) The Institute reserves the right to refuse email from outside hosts that send unsolicited (bulk), mass or commercial messages, or messages that are considered as threats, or messages that appear to contain viruses, and to filter, refuse or discard such messages.

2.2. Closure of an email Account

a) A user's account of a staff member that is dismissed, resigned, or deceased must be closed/ deactivated as soon as the event is officially notified to the ICT Office by the immediate supervisor or director and HR admin.
   Before deactivating and/or deleting the user email account proper backup must be taken by the email admin.
b) A retired staff shall be able to use his/her Institute email account for 12 more months after retirement date.
c) Backup log of deleted account will be kept for a maximum of 12 months.

2.3. User Naming

a) This must be done as per the Institute's rules and procedures which must be formulated by the ICT Office.

2.4. Disk Space Quotas

Disk space quota for email users must be set to users by the ICT Office based on availability of resources.

Chapter 3: Internet

The purpose of this policy is to minimize risks associated with Internet services and define controls against associated threats such as unauthorized access, theft of information, theft of services, and malicious disruption of services. AHRI provides Internet communication facilities to the staff for the purpose of supporting the research, administration and all other relevant requirements to carryout job functions. For proper usage of Internet services, users are required to firmly adhere to this Internet policy. All users must follow the institute principles regarding resource usage and exercise good judgment, use the internet as if your family member or coworker is sitting with you, when using the Internet. AHRI MUST use a standard bandwidth and network management tool.

1. Policy Statements

a) Internet use on AHRI Net is for the purpose of conducting the Institute's Research and Administrative works.
b) A firewall must be used on AHRI Net to control all data packets and connection requests; only explicitly permitted traffic is allowed through the firewall, all other traffic must be rejected; all traffic passing through the firewall must be capable of being logged and audited; packet filtering must be used with rules, which keep the risk to a minimum. Users will be warned of excessive bandwidth use.
c) At any time and without prior notice, the management reserves the right to examine and inspect Internet access accounts and browsing histories without the consent of the user when required for auditing purposes as well as to help investigations conducted by internal and/ or law enforcement agencies.
d) The Internet is to be used only when necessary for the execution of a user's job responsibilities.
e) Separate set of devices and controlled privileges must be made available for scientific research with special permission from an authorized body i.e. the Directorates.
f) If high bandwidth applications for recreational use of the Institute network are identified, they will be restricted or blocked.
g) Internet users may not operate a peer-to-peer (P2P) file sharing protocol on your computer. This includes the systems (among others): Kazaa, Morpheus, Direct Connect, LimeWire, Gnutella, eDonkey netwrok, FastTrack, BitTorrent, etc.

2. Resource usage

a) Internet service must be used primarily for research and institutional purposes, unless management has specifically approved other usage. Do not waste resources.
b) Users of AHRI's computers, on discovering that they have connected to a web site that contains potentially offensive material, must be immediately disconnect from that site.
c) Users require being aware that AHRI accepts no liability for their exposure to illegal, immoral, unethical and offensive material that they may access via the Internet.
d) The ability to connect with a specific web site does not in itself imply that users of AHRI's systems are permitted to visit that site.

e) Users accessing the Internet using computers of AHRI are not permitted to connect to the Internet through sources other than AHRI's Internet communication facilities (Central Proxy server).

f) Users must not place AHRI's or Group's information or material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP -File Transfer Protocol or similar services, unless the Department Heads and the IT-Director have first approved the posting of these materials.

g) All users of AHRI Internet services need to strictly refrain from committing or attempting to initiate unethical or "inappropriate" activities using AHRI's Internet facilities or equipment.

h) Abusive, unethical or "inappropriate" use of the Internet is considered grounds for disciplinary, legal and/ or punitive actions, including termination of employment. Examples of prohibited employee Internet use include, but are not limited to, the following,

- Introduce material considered indecent, offensive, or related to the production, use, storage, or transmission of sexually explicit or offensive items on AHRI's network or systems, using the Internet.
- Conduct illegal activities, including but not limited to gambling, and access to or the downloading of pornographic material.
- Solicit for any purpose which is not expressly approved by the AHRI management.
- Use AHRI's logos or materials in any web page or Internet posting unless it has been approved, in advance, by AHRI senior management.
- Reveal or publicize proprietary or confidential information of AHRI.
- Represent and publicize personal opinions as those of AHRI to mislead the public or for personal gain.
- Upload or download commercial software in violation of its copyright.
- The use of the Institute's Internet services to engage in hacking other sites and accessing unauthorized information within and outside the Institutes are not allowed.
- The creation, dissemination, storage and display of obscene or pornographic materials, indecent images of children, hate literature, defamatory materials or materials likely to cause offence to others is prohibited.
- Institute facilities may under no circumstances be used to obtain, view, or reach any pornographic, or otherwise immoral or unethical Internet sites.
- Make or post indecent remarks e.g., wage of smear campaigns, malicious written attacks directed at any individual or some organization or similar written attacks.
- Attempt to gain illegal access to remote systems on the Internet.
- Establish Internet or other external network connections that could allow non- AHRI users to gain access into AHRI's systems and information assets.
- Spoofing and phishing the identity of another user on the Internet or on any of AHRI's communications systems.

3. Allowed Usage

Questions can be addressed to the Directorate for any special requirements which might demand added bandwidth usage for specific user to have more upload and download speed based on priority. And on some cases, such privilege can be scheduled for a specific time/duration.

User Internet access requirements will be reviewed periodically by the institute to ensure that continuing needs exist.

All users of internet should be aware that the institute network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Chapter 4: Website and Social media

AHRI provides Web publishing services to support its Research and Administrative functions. Armauer Hansen Research Institute Website is an official publication of the Institute. Its mission is to promote the Institute and provide a usable, informative, consistent, and up-to-date information in an accessible and attractive manner to audiences inside and outside of the Institute. It is an all-encompassing site and a virtual reflection of the Institute community, value, mission, and its heritage.

Official pages are those for Institute offices such as, Research and Administrative units. They represent the Institute potential researchers, employees, donors, and visitors. Official pages must conform to the design styles adopted by the responsible office to give the site unity, coherence, functionality, and readability.

The Web Policy applies to the web and online presence of any department, directorate, center, or other organizational unit that is a part of, or owned, managed, and staffed by the Institute.

1. Policy Statements

The Website is an invaluable tool that offers new opportunities for communicating Information about AHRI to a worldwide audience. It is expected to represent AHRI's mission and its character, just as other AHRI's publications strive to do.

Because of its importance in building the Institute's future and a means for communicating with the public, this Web publishing policy is set to govern the nature, content, format, maintenance, timeliness and ownership of information contained on the official and unofficial pages of the Institute Website.

1.1. Official Institute Web Pages

a) The official website of the institute is: https://ahri.gov.et/
b) The official website must consist the Institutes logo at the header, the copyright, the developer and privacy policy at the footer.
c) Related research project webpages must be a sub-domain/under the official webpage domain.
d) The contents of all pages-parent or child website link- must reside on the AHRI's Web server.
e) All pages must be built using template pages supplied through the Web Administrator and must be maintained and regularly updated by the responsible Institute offices or research units.
f) The institute pages within the AHRI's Website must be readily identifiable as a part of its site by the use of the Institute, name, logo or logotype, a specific palette of colors and specific typefaces.
g) Official pages must be accurate, well-written, concise, and free of spelling and grammatical errors.
h) Research departments must carry navigational links to each of its unit member's home pages or to the email addresses and telephone numbers of those unit members who choose not to have a home page.
i) All official pages must be regularly monitored by the Web Administrator to ascertain that the material is current. Those with outdated materials will be notified to update their page or remove the outdated material.
j) Graphic elements and photographs on official pages must be governed by the Institute's rules and procedures.

k) Interactive features must not be used on the Website's official pages without prior approval from the ICT Team leader and a plan for periodically updating the material contained in them.

1.2. Web Authoring

a) The ICT/Web professional is responsible for the pages pertaining to it.
   - This person will help build, add to, maintain and/or update the Web pages. He/she must also be responsible for checking materials for their accuracy and conformance with Web standards and for working with the Web Administrator of the ICT Office prior to the publication of the site.

b) All Web authoring tools must follow the Content Management System used by the Institute.

c) Web developers must be provided with consultation and training, appropriate software, hardware, as well as individual assistance in the use of content management systems, mastering software and style for the Website.

d) Web developers may choose from a selection of official Institute templates, colors and photos for composing pages representing their office(s) or department(s). These must be stored in a Website library maintained by the ICT Office.

1.3. Social media

For the purpose of creating awareness, sharing information and establishing the institute image, the institute may use verified social media platform to create even a more engaging experience for the employees and its donors.

Social media content posting and updating must be managed by Public Relation department. And will be regularly monitored.

Legal risks

Staff and PHD/Maters students using social media should be mindful of the following legal risks and acts in particular:

- Defamation: posting untrue content adversely affecting a person's or organization's reputation, which has caused, or is likely to cause harm,
- Malicious falsehood: posting untrue and damaging content with an improper motive resulting in financial loss for the subject,
- Harassment: subjecting someone to a course of conduct that causes them distress or alarm, including stalking, trolling and cyber-bullying,
- Intellectual property infringement: posting content which copies a substantial part of a work protected by copyright,
- Breach of confidence or trust: posting confidential information.

2. Website Security

A system of permissions must be adopted and used to protect the security of the Institute's Website. Those with full permissions to administer the Webpages will be limited and will be designated by the ICT Office as necessary to maintain Web pages.

a) Permissions for Web developers will be limited to their areas of responsibility on the Website. Permissions to author on the site will be given by the Web Administrator.

b) All employees with full or limited permissions to the Institute Website are responsible for taking all reasonable precautions to protect both the public and developmental Website areas from vandalism, hacking and accidental alteration.

This includes not sharing computer account information or passwords with others and carefully monitoring access to personal computers in shared work areas.

3. Acceptable Use

3.1. Staff Requirements of Social Media Use

- **Public Interest Disclosure (whistleblowing)**

1. Any disclosure of serious malpractice, corruption, wrongdoing, or impropriety should be made to the Director General. Where an employee releases such information through social media, the Institute's *Public Interest Disclosure Policy (or any similar policy applicable for the institute)* will be initiated before any further action is taken.

- **Social Media Account Creation and Maintenance Procedure**

1. Before creating a new company social media account, it is vital that staff considers whether there is a different audience or set of objectives which cannot be met through an existing account.
2. Before opening a new account, an activity plan should be created which considers: the target audience and their information needs; the content to be shared; how producing content and monitoring the account will be resourced; and how this account sits together with those already established across the Institution.
3. The Department of ICT Services will maintain an asset register of all corporate social media accounts for the Institution.
4. All corporate social media accounts must adhere to the Institution's web and brand guidelines. It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions should be responded promptly within operating hours.

- **Social media posts guidelines**

1. All posts from institution social media accounts represent the Institution. It is vital that messages posted are carefully considered, appropriate and do not damage the reputation of the Institution or otherwise bring it into disrepute.

- **Account Security**

1. Social media accounts are at risk of hacking and this can cause significant reputational damage and potentially serious misinformation for stakeholders. There are also considerable resource implications following on from any breach in security such as a compromised social media account.
2. Staff should also secure accounts with 2-factor authentication.

- **Escalating concerns and issues Institution.**

a) If a social media account has been hacked or a post from a corporate account attracts a number of negative comments and it is not clear how best to respond, staff should flag this with the Institution management and IT department and seek guidance.

Users are responsible for the Webpages that they publish under applicable Institute rules and regulations. Complaints alleging misuse of the Web service must be directed to bodies responsible for taking

appropriate disciplinary action. This may include the withdrawal of access to Web service and other computing facilities.

Without specific authorization by concerned bodies, the Web service may not be used for the following:

- Commercial advertising – this does not include advertisements related to or supporting the research, or service mission of the Institute, such as departmental conferences, or listing of sponsors for a performance or special event.
- Publishing of Web pages of non-authorized users (such as non-Institute persons, organizations, etc.).
- Activities that would provide non-Institute-related personal financial/monetary gain.
- Alteration of pages of other users.
- Posting harmful, threatening, abusive, harassing, hateful or objectionable pages, or pages that violate any applicable regional, federal or international laws.

Web pages are subject to periodic review and approval by the concerned Web master(s). The Institute reserves the right to remove any page that is in violation of rules and regulations, is in conflict with the Institute's interests or is detrimental to the performance of its computing or network services.

3.2. Server-Side Scripts and Domain Names

This must be done as per the Institute's rules and procedures which must be formulated by the ICT Office.

3.3. Supervision, coordination, development, and maintenance of pages

This must be done as per the Institute's rules and procedures which must be formulated by the ICT Office. And it must always keep the institution interest in all the publications on the institute web portal.

14. Cloud Computing Policy

Cloud computing is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, the Institute for services such as, but not limited to, social networking applications (i.e., blogs and wikis), file storage (assignment drop box, buckets), and content hosting (publishers textbook add-ons). This policy pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.

14.1 Staffs must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

14.2 Use of cloud computing services for Institute purposes must be formally authorized by the senior management and the Director General of the Institute.

14.3 Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans.

15.User Support Policy

This policy contains guidelines for providing any service; hardware, software, Internet, application, or any troubleshooting, how to receive the service request, record it, and then provide the solution.

The purpose of the ICT support is to minimize number of fails and provide solutions to have business continuity by defining a guidelines process regime for all the staff and guests.

Responsibility

It is the responsibility of the ICT Directorate' to take relevant steps for ensuring solving any ICT problem.

15.1. The Service Desk Process

1. **Request Capture:** Requests are gathered and verified the right to service based on the Directorate ID or affiliation of the requester.
2. **Trouble Tracking:** A trouble ticket will be opened in Tracks with the user's name, email, and problem description.
3. **Problem Resolution:** An ICT Team leader will attempt forward problems and requests for IT team with their respective responsibilities to supported network, operating systems, computer hardware, applications, and peripheral devices. If call volume prohibits the specialist from spending any more time on the call, or the problem remains unsolved, the ticket will be escalated.
4. **Escalate the Request, if necessary:** The ticket will be updated and escalated to the second level within the Service Desk or to third level support outside of the Service Desk.
5. **Log Resolution into Ticket:** The Specialist who resolves the problem is responsible for appropriately updating the ticket with the action taken.

6. **Ticket Closure:** All Service Desk tickets will be closed when a resolution has been offered, with the status of the ticket set to "Resolved'. Tickets will be set to "Closed" through a 2 day auto-closure process that will generate emails upon status change and closure.
7. **Customer Satisfaction Surveys:** Tracks will randomly send customer surveys to gauge satisfaction with the ICT Service Desk. Based on survey results, users may receive a follow-up call.

16.Video Conferencing Use Policy

The institute shall use various means for the administration and research work of the daily business works as needs to accomplish the task. These are any collaborative team-work platforms.

a) The video conference at the Institute will be used for educational, administration, and/or research purpose only.
b) The recordings of the lectures during the video conferences are subjected to copyright law
c) The video conferencing service is available to staffs and students
d) Video conference services will not be used for personal calls.
e) ICT team provides the technical support for video conferencing equipment and ensure that they are in functioning order,
f) Video conferencing services will only be available through booking the services using a video conferencing request form.

17.Policy Violations

a) Any violation of the Email access policy may be subject to disciplinary action against the individuals and may lead to, counselling, dismissal and/ or may be referred to relevant law enforcement agencies in accordance with the policies, and research code of conduct of AHRI.
b) All users of AHRI Email services are required to do so ethically and in a legally responsible manner at all time.
c) While AHRI upholds the principles of privacy, it will not condone deliberate breach of either AHRI policies or external legislative requirements and will cooperate fully with the authorities in any investigations resulting from a breach. Consequences of a breach may include the removal of access rights to AHRI's ICT resources, disciplinary proceedings and in the case of serious and deliberate breach, may result in civil or criminal proceedings.
d) By using an Email account, the staff member agrees to be bound by the AHRI Email policy.
e) Any violation of the Internet security policy may be subject to disciplinary action against the individual and may lead to, counselling, dismissal or exclusion and/ or may be referred to relevant law enforcement agencies in accordance with the policies, and research code of conduct of AHRI.
f) All Internet account holders must do so ethically and in a legally responsible manner at all times.
g) By using an Internet account, the staff member agrees to be bound by AHRI's Internet security policy.
h) Any violation of the Web policy may be subject to disciplinary action against the individual and may lead to, counselling, dismissal or exclusion and/ or may be referred to relevant law enforcement agencies in accordance with the policies, and research code of conduct of AHRI.
i) All web account holders must do so ethically and in a legally responsible manner at all times.

j) Any violation of government laws or legislations may carry the additional consequence of prosecution under the law, where judicial action may result in specific fines or imprisonment, or both: plus, the costs of litigation or the payment of damages or both: or all.

18.Availability of the IS Security Policy

It is intended that this ISSPP be accessible to the institute staff via the institute's Intranet. It is a requirement that all institute staffs be familiar with relevant sections of this policy. The infrastructure team will periodically conduct workshops and/ or communicate to employees the relevant parts or the entirety of the ISSPP. All new employees will have to be informed and explained the contents of the ISSPP by the IT team when new access rights are granted to the new employees. IT team will take part in institute's new employee induction programs to spell out the ISSPP document.

19.Period Content Review of the IS Security Policy

This is a living document to be modified, updated and changed based on the current internal and/or external circumstances, institutional administrative changes.

It is customizable based on system and functional areas.

This Information Systems Security Policies and Procedures must, in general, be reviewed at least every two years. However, the office in charge of executing the policy may, from time to time, propose amendments that are necessary to enhance the objectives of this policy. Before the enactment of such amendments, the executing office must provide opportunities to its Institute community to comment on the proposal.

a) The IS security policy is a "living" document that will be altered and amended as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.
b) Major changes (addition of new clauses, policies and procedures to the existing ISSPP) will be made in consultation with the Director of AHRI, IT team, Admin office, and other relevant parties as decided by Directors.
c) Minor changes (modification of existing clauses, policies and procedures of the ISSPP) will be approved by the IT team and KMD Directorate.

20.Recommendation

Here are listed some of the main recommendation as observed from the current practices and organization structure of the institute.

Organization structure

As currently ICT is under KMD, good things are being done and much in progress. The daily activities, efficiencies and all communications of the institute are much dependent & supported by the ICT infrastructure & systems. As the growth of any organization/ institution is much dependent with the parallel growth of its Information System environment, as it will also help to operate in the fast-paced competitive world. If ICT service in AHRI is self-managed by its own IS Directorate Office, it will help to advance and grow the institution with the state-of-the-art technology and systems.

Integrate the ISSPP into institution's ethical document. This will insure the implementation process to be effective.

For website content management

An editorial must be assigned from the public relation or other department to review contents to be posted in short period of time (hours).

Supportive manual/document

This policy documents states the use of IT equipment (computers, tablet, printers, etc.) disposal instruction manual. So better for relevant parties to prepare and/or update such manual. Also related guidelines and policies shall be developed for Mobile device and BYOD Policy.

Infrastructure

As a technology prime institute, it is highly advised that the institute must have a *Log* and *Application* servers for same purpose. This is addition to the *Backup* sever.

Users' awareness

Published ICT guideline shall be prepared out of this policy document.

Procurement process

With the current practice, the procurement process takes quite a very long time after getting the purchase requirements, which directly affects the deliverables and outputs of the IT Team. There must be designed some kind of work in/around to address and resolve such kind of issues.

21.Glossary

Availability - Authorized users are granted timely and uninterrupted access to information. Availability will be based on the institutional requirement of the user.

Bring Your Own Device (BYOD)- is a concept in which staffs utilize their personal equipment to conduct Institution business.

Confidentiality - Information should not be made available or be disclosed to unauthorized entities (e.g., persons, organizations, and systems).

A **data center** is the physical infrastructure, including the building, electricity, cooling, and networking.

Email User means Legitimate AHRI Email account holder.

Email address/ Email account refers an officially recognized AHRI Email address.

ICT - Information and Communication Technology, or (technologies) refers to technology that is used for the creation, processing, and distribution of data and information using any computing equipment and software, telecommunications, and digital electronics. ICT has become an enablement tool for any activity and research process of the institute.

Information System (**IS**) means an electronic system that manages information and data related to the ICT Asset.

IT - Information technology can be defined as the study, design, implementation, support or management of computer-based information systems. IT typically includes hardware, software, databases and networks. Information technology falls under the IS umbrella but deals with the technology involved in the systems themselves.

Information Security, sometimes abbreviated to ***infosec,*** is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another.

ICT Environment defines the total environment within which information is processed, stored, and transmitted, and includes, but are not limited to, all documentation, physical and logical controls, personnel, hardware (e.g., servers, desktops, network devices, and wireless devices), software, information, media and services hosted in the cloud such as google driver, etc.

Integrity - Reliability of information will be maintained through protection from unauthorized, unintended modifications during transmission, storage, and retrieval.

Service-level agreement (SLA) is a commitment between a service provider and a client in this case AHRI. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user/AHRI.

Social media are websites and applications that enable users to create and share content or to participate in social networking. Examples of popular social media sites include, but are not limited to LinkedIn, Twitter, Facebook, YouTube, Instagram, Snapchat, Flickr, Yammer, Yahoo/MSN messenger, Wikis and blogs, Weibo, WeChat, and WhatsApp.

Standard ICT User is a user of ICT infrastructure and components that enable modern computing, a user without any escalated administrator privileges.

User Account reference assigned to an individual to enable a computer system to identify that individual.

User Password secret string of characters (letters, numbers, special symbols) that is used to prove identity.