

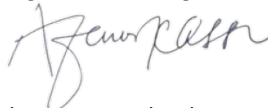
DOCUMENT PROFILE				
Version 1.0	Type of Document: Policy	Date: Apr. 01, 2024	Owner: Knowledge Management Directorate	Responsible Unit: Finance and Procurement Executive Office
Title:	Data Backup Policy			
Area <sup>1</sup>	Governance			

## 1. INTRODUCTION

### 1.1. PREAMBLE

Armauer Hansen Research Institute (AHRI) is a biomedical, clinical, vaccine, modern and traditional medicine research and development and pharmaceutical industry support Institute based in Addis Ababa, Ethiopia. It focuses on infectious and noninfectious diseases medical research, vaccine, pharmaceuticals & diagnostics research and development as well as nationwide pharmaceutical industry support. The Institute was founded in 1970 as part of the All-Africa Leprosy and Rehabilitation Training Center (ALERT), with the support of two Save the Children organizations of Norway and Sweden, and the Ethiopian government. The Institute was named after Gerhard Armauer Hansen, a Norwegian physician who discovered the leprosy bacillus in 1873. In 1999, the Institute was restructured and renamed as AHRI, under the Ministry of Health of Ethiopia. AHRI's mission is to Improve public health and well-being by generating and presenting scientific evidence, enriching and developing new/improved products, equipment and methods, providing pharmaceutical industry support and advisory services and to be a center for technology transfer and capacity building, enhancing the country's sustainable economic, social and environmental benefit. On 14th April 2023, The Council of Ministers of the Federal Democratic Republic of Ethiopia (FDRE) re-established AHRI under Regulation No. 530/2023 with further expanded mandates.

As a research institution, AHRI generates and manages a large volume of data ranging from research findings, medical records, experimental data, and administrative documents. These data are critical to the functioning and continued success of AHRI and must be protected from loss or damage. AHRI is acquainted with the importance of safeguarding its data and has therefore developed policies and procedures aimed at mitigating the risk of data loss or damage. One area of focus for AHRI is the development of Data Backup Policy to ensure that critical data is always available. The backup policy is a set of guidelines and processes that guide the regular backup and recovery of critical data.

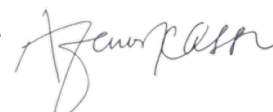


<sup>1</sup> Area refers to which comprehensive functional categories the document belongs to: Research and Development, Research Training, Innovation, Production/Manufacturing, and Governance.

The importance of having a backup policy enables the institution to restore lost or damaged data within the shortest possible time, minimizing disruptions to operations. In a fast-paced research environment where data is generated regularly, having a backup policy is particularly critical as it ensures that all data is secured in case of unforeseen events such as natural disasters, cyber-attacks, hardware failure, or even human error. And hence, data backups are a critical aspect of data management, and AHRI must develop a strategic Data Backup Policy that aligns with its operations and objectives.

## **1.2. DEFINITIONS OF TERMS**

- 1.2.1. The backup policy is a set of rules and procedures that define how backups of important data will be taken, and how they will be stored and protected, emphasizing on identifying which data should be backed up, how frequently backups should be taken, where and how long backup copies should be retained.
- 1.2.2. Backup: A copy of electronic data created for the purpose of recovery in case of data loss.
- 1.2.3. Full back up: A complete copy of all data within a designated scope.
- 1.2.4. Incremental backup: A backup capturing only the changes in data since the last backup.
- 1.2.5. Research data: is the raw information collected or generated during scientific studies, or experiments, forming the basis for analysis and conclusions.
- 1.2.6. Operational data: information used in daily organizational activities aiding in decision-making and performance monitoring.
- 1.2.7. System configurations: refer to the specific settings and arrangements defining the behavior and functionality of computer systems, software, and networks, ensuring optimal performance, security, and compatibility with AHRI needs.
- 1.2.8. Encryption: The process of transforming data into a scrambled format that requires a key for decryption.
- 1.2.9. Access Controls: Security measures that restrict access to data and functionalities based on authorized roles.
- 1.2.10. Critical data: refers to information that is essential for the functioning, operation, or continuity of an organization, system, process, or project
- 1.2.11. Data retention: refers to the length of time data is stored and kept accessible for operational or compliance purposes.
- 1.2.12. Cyber-Security: It's unauthorized and deliberate exploitation of computer system or networks to disrupt, steal or manipulate data or cause other harmful effects.
- 1.2.13. System failure: unexpected and significant disruption or malfunctioning of computer system, networks or hardware that renders them unable to perform their intended function.
- 1.2.14. Data loss: unintentional or accidental deletion, corruption or destruction of digital information rendering it inaccessible or unusable.



## **1.3. PURPOSE AND OBJECTIVES**

### **1.3.1. Purpose:**

The purpose of this backup policy is to ensure the protection, availability, and integrity of critical data and systems of AHRI in the incident of a disaster, system failure, data corruption, cyber-attacks, accidental deletion or data loss.

### **1.3.2. Objectives:**

1. To establish a regular backup mechanism for critical data and systems,
2. To identify the critical data and systems that require backup, and prioritize them based on their importance to the institute's operations.
3. To ensure that all backup processes are properly documented, including backup procedures, frequency, and storage locations.

## **2. SCOPE AND POLICY STATEMENT**

### **2.1. SCOPE**

This policy applies to all critical data, applications and systems owned, processed, or stored by AHRI, including but not limited to: research data, operational data and system configurations

### **2.2. POLICY STATEMENT**

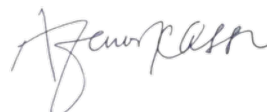
The backup policy for Armauer Hansen Research Institute is designed to ensure the protection and availability of critical data and systems in the event of a disruption or disaster. This policy includes regular backups of all data and systems, with three or four copies stored both locally and offsite. Backups are performed daily and tested regularly to ensure their integrity and ability to restore data in the event of a failure. The retention period of backups is determined by the type of data and its importance to the organization. All backup procedures are documented and reviewed periodically to ensure they comply with changing needs and standards.

### **2.3. BACKUP PROCEDURES**

Backup procedures include identifying the critical data to be backed up, specifying backup methods, and frequency, ensuring backup integrity, applying backup retention, and carrying out recovery processes. Furthermore, constant testing of backup and restore operations is required to ensure reliability and preparedness.

## **3. BACKUP FREQUENCY**

- 3.1. All critical data, including research data, patient records, system configurations, and operational data, shall be backed up daily or weekly to ensure minimal data loss.
- 3.2. Incremental backups shall be performed daily to capture only the changes made since the last backup, reducing backup time and storage requirements.
- 3.3. Full backups shall be conducted every week to capture any changes made during the week and to maintain a comprehensive backup history.



- 3.4. Monthly backups should be performed to create archival copies of the data for long-term storage and compliance purposes.

#### **4. BACKUP LOCATIONS**

- 4.1. Data backups shall be stored on-site in secure and fireproof storage facilities to ensure quick access in the incidence of data loss or system failure.
- 4.2. Ensure the on-premises backup server is located in a controlled environment with adequate security measures.
- 4.3. Backups shall be replicated to an off-site location, such as a secure cloud storage service or a separate physical location, to protect against physical disasters like fire, theft, or natural calamities.

#### **5. BACKUP RETENTION**

A data retention schedule will be implemented to match the necessity for data accessibility with the optimization of storage resources.

- 5.1. Daily backups shall be retained for one week.
  - 5.1.1. Retain at least 7 daily backup sets for short-term data recovery needs.
  - 5.1.2. Automatically overwrite the oldest daily backup set after one week.
- 5.2. Weekly backups shall be retained for one month.
  - 5.2.1. Maintain a minimum of 4 weekly backup sets for long-term recovery and compliance purposes. Monthly backups will be retained for one year.
- 5.3. Critical historical data will be archived according to research project requirements and relevant data retention regulations

#### **6. SECURITY AND COMPLIANCE**

- 6.1. Enforce encryption of backup data both in transit and during storage to protect sensitive information from unauthorized access.
- 6.2. Implement strict access controls and authentication mechanisms to restrict unauthorized access to backup systems and data.
- 6.3. Ensure backup procedures adhere to relevant data protection and privacy regulations applicable to the institute.

#### **7. BACKUP TESTING AND MONITORING**

- 7.1. There should be regular test backup procedures and restore processes to validate data recoverability (effectiveness of the backup system) and to ensure integrity.
- 7.2. Monitoring tools should be implemented to track backup job statuses, storage capacity, and trends.
- 7.3. Configure alerts for backup failures or issues requiring immediate attention.



## **8. DOCUMENTATION**

Backup procedures, schedules, and responsibilities in a centralized repository should be documented for reference.

## **9. DUTY TO COOPERATE**

The concerned bodies shall have the duty to cooperate with a view to facilitating to effectively discharge its duties under this policy.

## **10. INAPPLICABLE POLICIES**

No policies or practices or circular letter shall, in so far as it is inconsistent with this policy, be applicable with respect to matters provided by this policy.

## **11. IMPLEMENTATION**

This policy shall take effect from the date of approval by the relevant body. The members of medical research directorates shall establish a system for monitoring and evaluating the policy's implementation. Additionally, the policy will have guidelines for data backup and archiving to facilitate the implementation process.



Prof. Afewok Kassu  
Director General  
April 01, 2024