FAWE
Ethiopia Chapter

DATA SECURITY POLICY

January 2025

Contents

JANUARY 2024 I

APPROVAL FOR THIS DOCUMENT 3

1. INTRODUCTION 4

1.1. PREFACE 4
1.2. DEFINITIONS AND ACRONYMS 4
1.3. SHORT TITLE 5
1.4. OBJECTIVES 5
1.5. SCOPE OF APPLICATION 5
1.6. PURPOSE 5
1.7. OTHER GOVERNING RULES 6

2. AUTHORITY AND RESPONSIBILITY 6

2.1. THE BOARD 6
2.2. THE EXECUTIVE DIRECTOR 6
2.3. MONITORING AND EVALUATION OFFICER 6
2.5. ALL PROGRAM AND FIELD OFFICERS 7
2.6. THE INFORMATION TECHNOLOGY UNIT 7
2.7. ALL STAKEHOLDERS AND PARTNERS 8

3. DATA SECURITY POLICY STATEMENTS 8

3.1. ACCESS CONTROL AND AUTHORIZATION POLICY TO THE DATA 8
3.2. DATA PROTECTION AND IMPACT STATEMENT(DPIA) 8
3.3. DATA PROTECTION AND CLASSIFICATION POLICY 9
3.4. DATABASE SECURITY 10
3.5. PERSONNEL SECURITY POLICY 10
3.6. MEDIA PROTECTION POLICY 10
3.7. RESEARCH EXEMPTION 11
3.8. TRAINING, EDUCATION, AND AWARENESS POLICY 11

4. EXCEPTION HANDLING AND POLICY MANAGEMENT 12

4.1. EXCEPTION HANDLING TO THIS POLICY 12
4.2. POLICY ENFORCEMENT 12
4.3. REVISION 12
4.4. EFFECTIVE DATE 12

Approval for this document

Role	Name	Role	Signature	Date
Proposer				
1	Eden Fesseha	IT Officer		
Reviewers and Validators				
Approver				



1. INTRODUCTION

1.1. Preface

FAWE Ethiopia Chapter has been striving to advance its information system and support its vision and mission by acquiring different technologies related to data storage, mining, and computing. These technologies require a separate issue-specific security policy.

Efforts have been made to safeguard the existing data assets to prove the FAWE Ethiopia's ability to meet its objectives and obligations.

Since IT related technology is evolving faster, it is essential to have a fast-changing issue-specific policy to preserve confidentiality, integrity, and availability of FAWE Ethiopia assets.

Hence, a Data security policy has been devised to cater to distinct data protection prerequisites that necessitate frequent updates. It also comprises a declaration on the FAWE Ethiopia Chapter's positions on specific issues.

1.2. Definitions and Acronyms

a) **Third-party service providers/ Remote service providers:** A paid organization for its service. Example: The cloud

b) **Archive**: The process of moving data that are no longer actively used, in a separate data storage device for long-term retention

c) **Authentication**: Provision of assurance that a claimed characteristic of an entity is correct.

d) **Availability**: The state of being accessible and usable upon demand by an authorized entity;

e) **Automation**: Means The use of computer or system of computers to enter, store, retrieve, transmit or manipulate data to increase reliability and efficiency, often through a limited number of employees.

f) **Backup**: Saving of files onto storage devices like magnetic tape or other offline mass storage media.

g) **Confidentiality**: Ensuring that information is made available or disclosed only to those individuals, entities, or processes authorized to have access.

h) **Data owner:** The individual, who has responsibility for the integrity, accurate reporting and use of computerized data; In case of FAWE Ethiopia it includes, but not limited to: Executive Director, Program Coordinator, Program Coordinator, communication Officer

i) **Data custodians:** Means the individual(s) and/or department(s) responsible for the storage and safeguarding of computerized data
In case of FAWE Ethiopia: Executive Director, Communication officer, IT officer

j) **Workforce:** All staffs of FAWE Ethiopia.

k) **Information:** Means data that is accurate and timely, specific and organized for the purpose, presented within a context that gives it meaning and relevance.

l) **Integrity**: Means the safeguarding of the accuracy and completeness of assets.

m) **Data Protection Impact Assessment (DPIA):** Means minimize the data protection risks involved in projects, processes and activities involving the processing of personal data.

n) **Stakeholders:** All parties who have individual interest on FAWE Ethiopia

In case of FAWE Ethiopia.

o) **Data Subject**: identified or identifiable natural person" from whom or about whom information is collected

1.3. Short Title

This policy can be sited as "Data Security Policy of FAWE Ethiopia Chapter".

1.4. Objectives

objectives of this Data Security Policy are:

a. To ensure the availability of FAWE Ethiopia data, information and information processing facilities.
b. To ensure the confidentiality of FAWE Ethiopia data, information and information processing facilities.
c. Ascertain the integrity of data, information and processing operation.

1.5. Scope of Application

This Data Security Policy applies to FAWE Ethiopia system assets which consist of data, information, employees, and information processing facilities. All entities that have access and interest to the FAWE Ethiopia Chapter data are covered by the policy.

1.6. Purpose

Purpose of this Data Security Policy is to:

a. Guarantying the collection and processing of data is based on the consent of the data subject.
b. To give Direction for all stakeholders on the protection of personal data starting from collection to processing and public release.
c. Minimize the risk of disclosure of confidential information to unauthorized persons.
d. Abiding all FAWE Ethiopia stakeholders and partners

e. State the extent and provide a clear set of rules of disclosure of confidential data to external parties, that does not place FAWE Ethiopia or the data user at risk.

1.7. Other governing rules

Data security policy shall comply with closely connected parts of data security related laws, regulations, and standards of ISO 27001, Data Security Policy of the Federal Democratic Republic of Ethiopia, Data protection and privacy policy of FAWE.

2. AUTHORITY AND RESPONSIBILITY

2.1. The Board

The Board shall:

a. Assure that an appropriate Data Security Policy is established to collect, accumulate, and produce accurate, complete, relevant and timely information from the data.
b. Review and Approve the FAWE Ethiopia Data Security Policy.

2.2. The Executive Director

a. Monitor and ensure the approval of this policy by the Board before implementation.
b. Oversee the proper implementation of this policy and its alignment with the organization objectives.
c. Approve standards, procedures, and guidelines concurrent with this policy.
d. Decides on the appropriate data and computing resource requirements of the organization.

2.3 The Program Coordinator

The program coordinator shall;

a. Ensure the proper implementation of the Data Security Policy across all programs starting from the date of approval.
b. Ensure that appropriate controls are in place to all labeled data.

2.3. Monitoring and Evaluation Officer

The M&E officer shall;

a. Ensure the proper implementation of the Data Security Policy across the organization.
b. Oversee and evaluate the implementation of this policy document.
c. Ensure that appropriate controls are in place to all mission critical data.
d. Ensure that the data users are provided with the proper policy related support as part of policy implementation.

e. Oversee, evaluate and approve the proper selection and labeling of data before passing it to the data digitizer.
f. Ensure the prevalence of appropriate controls in data collection and delivery required for reporting, and management decision according to this policy.
g. Oversee the development, organization and evaluate the effectiveness of data security training and awareness programs.
h. Ensure training to data and computing resources are given according to training, education and awareness policy.

2.4. Safeguarding Officer

a. Oversee the development, implementation and maintenance data security policies, standards, procedures, and guidelines.
b. Oversee the effectiveness and efficiency of data security risk assessments, vulnerability discovery mechanisms of the overall FAWE Ethiopia data assets.
c. Organizes a response to actual or suspected breaches in the confidentiality, integrity or availability of information and assets.
d. Oversee and evaluate the proper implementation and functioning of the security incident and monitoring operation.
e. Shall give induction to this policy, upon the arrival of new staff.
f. Make sure a consent is provided by the data subject for any collection and processing of data.

2.5. All Program and Field Officers

All officers in a program shall:

a. Ensure the proper implementation of the data security Policy in the day-to-day operation.
b. Ensure the completeness and accurate reporting of all collected data before the processes following it.
c. Develop and/or implement processes and procedures that is aligned to this Policy.
d. Commence amendments on the data security Policy as deemed appropriate.

2.6. The Information Technology unit

The Information Technology shall;

a. Develop and submit the "Data Security policy" and submit for approval.
b. Establish a structure to the development, implementation and storage of data provided by the Monitoring and Evaluation officer.
c. Monitor the appropriate data protection and safeguarding mechanisms are implemented to the stored data according to the FAWE Ethiopia IT Strategy and Policy.
d. Ensure the integrity of the Organizations' data.

e. The IT unit, in collaboration with the communication officer, shall ensure a specific consent is obtained for data to be processed for a digital use.
f. If a data subject removed his/ her consent to the processed data, the IT unit shall remove it from storage and digital platforms as soon as its reported.
g. Audit the archived data with the data owner for the disposing of data that are no longer in use within FAWE Ethiopia.
h. Ensure the fast retrieval of data when needed by the data custodian.
a. Disposal of archived data based FAWE Ethiopia IT Strategy and Policy the archive data which is no longer in use as directed by the IT officer

2.7. All Stakeholders and Partners

All Stakeholders and Partners shall:

a. Shall read and adhere with this policy before agreement of a contract. An exception to this policy will be handled according to the Exception handling article of this policy.
b. Contribute to the identification, monitoring, and reporting of actual and/or suspected data security breaches and/or policy violations by taking the appropriate measures and promptly informing the appropriate authorities.

3. Data security policy statements

3.1. Access Control and Authorization Policy to the Data

All FAWE Ethiopia Chapter data is covered by the following statements.

3.1.1. All requests must be documented using the appropriate forms, processes and follow the guidance established by the organization data security policy and IT Strategy Policy document.
3.1.2. Use of any cloud or third-party system which should be used to store, process, or interact with restricted information must be formally approved in accordance with FAWE Ethiopia IT Strategy and Policy.
3.1.3. Data owners shall define which workforce members are authorized to access each information asset and should maintain a list of such workforce members along with the IT and HR unit. Both should work together to ensure that only authorized workforce members have access to such resources and manage user accounts based on the organization IT Strategy and Policy document.
3.1.4. The exceptions to this policy shall be handled by the exception handling article of this policy.

3.2. Data Protection and Impact Statement(DPIA)

In practice, FAWE will require a DPIA for any projects involving the use of personal data, including new systems, solutions, and some research studies. describe the nature, scope, context, and purposes of the processing

a. Assess necessity, proportionality, and compliance measures
b. Identify and assess risks to individuals

c. Identify any additional measures to mitigate those risks.

3.3. Data Protection and Classification Policy

3.3.1. Data protection involves defining and protecting all information assets. Information assets is an all-inclusive term that includes the 'data', 'knowledge', and 'data sets' and should be referred to collectively as "data".

3.3.2. All workforce have a security role and personal responsibility to protect the information he or she has been entrusted to use.

3.3.3. The safeguarding and IT unit should maintain an up-to-date inventory of all sensitive and restricted information assets.

3.3.4. FAWE Ethiopia should encrypt all restricted information in accordance with the organization IT Strategy and Policy.

3.3.5. **Public Data** includes information that receives widespread disclosure and does not require controls to limit access to the information. While public information does not have high sensitivity or confidentiality requirements, care should be taken to protect the integrity of the information.

3.3.6. **Sensitive Data** includes information that is intended for use by FAWE Ethiopia workforce members who have contact or potentially may have contact with this information, such as: (a) Project Officers (b) Human Resource information such as salary ranges, policies, and benefits; and (c) Personal information of beneficiaries. FAWE Ethiopia shall apply appropriate controls to this information to limit the chance of inadvertent exposure.

3.3.7. **Restricted Data** includes both sensitive personal data as well as sensitive organization information. FAWE Ethiopia shall restrict unauthorized access to beneficiaries and workforce members data.

3.3.8. Any and all data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

3.3.9. All workforce members who suspect that restricted data may have been misplaced, lost, stolen, or altered in a suspicious way, must immediately report the incident to the HR and IT unit.

3.3.10. The data custodian is the individual or group who is responsible for the maintenance and protection of data assets. (a) The data custodian of electronic information may be the data owner and/or the Information Systems Division. (b) For electronic information, the data custodian's duties may include information backups, implementing technical security protocols and controls as directed by this policy, restoring information from backups, and fulfilling requirements set in the other policies. (c) The data custodian of non-electronic information is usually the data owner.

3.3.11. FAWE Ethiopia shall not store information labeled as restricted at a third-party location unless authorization is provided by the HR and Safeguarding unit. Exceptions should be managed in accordance with exceptions handling article of this policy.

3.3.12. In virtual meetings and telephone calls where restricted information is to be discussed, a determination must be made in accordance with FAWE Ethiopia IT Strategy and Policy document.

3.4. Database Security

3.4.1. Each database and its underlying operating system should adhere to the general security requirements as defined in the IT Strategy and Policy document.

3.4.2. All system administrators should use named accounts in accordance with Access control and Authorization Policy

3.4.3. The data on a database shall be decommissioned once the IT and safeguarding unit working jointly with the management team determines that the existing data is no longer necessary.

3.4.4. All system administrators shall be properly trained and educated on safeguarding of data and security of the database systems they administer in accordance with the Safeguarding Policy and Training, Education, and Awareness Policy.

3.4.5. The exceptions to this policy shall be handled by the exception handling article of this policy.

3.5. Personnel Security Policy

3.5.1. All workforce members have a responsibility to protect FAWE Ethiopia data and computing resources and this security role is considered a part of every person's job responsibility.

3.5.2. Personal data shall only be processed to improve the data subjects life condition.

3.5.3. FAWE Ethiopia shall ensure appropriate safeguarding measures are applied while data processing.

3.5.4. Workforce members in the Information Technology Division have a greater responsibility to protect the integrity and confidentiality of data.

3.5.5. The Human Resources Department should coordinate with the Information System division to ensure that all workforce members should have defined security roles and responsibilities included in their job descriptions.

3.5.6. Workforce members are assigned security roles based on their need to access and manipulate certain types of data as described in FAWE Ethiopia Data Protection and Classification Policy.

3.5.7. Upon contract termination with an employee, the Human Resources Department should communicate with IT division to confirm that all company-owned equipment, data, and anything security related has been disabled, access revoked and returned to FAWE Ethiopia.

3.5.8. All FAWE Ethiopia computer users shall be educated on proper methods for accessing data and computing resources in accordance with FAWE Ethiopia Training, Education, and Awareness Policy.

3.5.9. The exceptions to this policy shall be handled by the exception handling article of this policy.

3.6. Media Protection Policy

3.6.1. FAWE Ethiopia has made a commitment to implement both security and safeguard the data under its custody.

3.6.2. On the use of data for marketing for purposes of fundraising and awareness campaigns by email, SMS, social media, websites, telephone etc. FAWE must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honored such requests promptly.

3.6.3. All stakeholders and of FAWE Ethiopia, must ensure that it understands or consults with the designated persons within the organization on FAWE's legal obligations in relation to direct marketing before embarking upon any direct marketing campaign.

3.6.4. Workforce members must get authorization from safeguarding unit before commenting about FAWE Ethiopia restricted and sensitive data on media. If authorization is given, the workforce member must disclose his or her employment relationship with when posting a comment regarding the labeled data.

3.6.5. Any workforce member who discusses while using personal social networking sites must include a disclaimer that specifically states the opinions and attitudes expressed are those of the workforce member alone and may not be attributed to FAWE Ethiopia. Unless that workforce member shared a post directly from FAWE Ethiopia social media, it must be clear that he or she is speaking for himself or herself.

3.6.6. A workforce member who suspect that restricted data may have been misplaced, lost, stolen, or altered, must immediately report the incident to the Safeguarding Officer.

3.6.7. Information, not previously publicly released by FAWE Ethiopia should not be posted on personal social networking sites.

3.6.8. Using Logos and trademarks on social networking sites without tangible permission from Communication Officer is restricted.

3.6.9. Workforce members should not maintain any expectation of privacy with respect to information posted on social networking sites.

3.6.10. This article is not intended to restrict a workforce member's right to discuss working conditions with coworkers or in any way limit workforce members' rights.

3.6.11. Correct mistakes: If a workforce makes a mistake in the content of his/her post, correct it as soon as possible. If the workforce make a major mistake, inform the Communication Officer as soon as possible.

3.6.12. If the workforce do not have exact knowledge about the data to be projected, then do not comment on any of it.

3.6.13. The exceptions to this policy shall be handled by the exception handling article of this policy.

3.7. Research Exemption

3.7.1. Some of the rules outlined above do not apply when personal data is being used for research purposes due to an exemption contained in the GDPR and DPA 2019. This exemption applies if the following conditions are met:

3.7.2. Appropriate technical and organizational safeguards exist to protect personal data e.g. data minimization, pseudonymization, or access controls.

3.7.3. There is no likelihood of substantial damage or distress to the data subjects from the data processing.

3.8. Training, Education, and Awareness Policy

3.8.1. FAWE Ethiopia should implement an information Data security awareness program intended to motivate and remind workforce members to help protect data and computing resources.

3.8.2. FAWE Ethiopia should provide training to workforce members that include the importance of secure authentication, social engineering, data protection measures

3.8.3. FAWE Ethiopia should facilitate training that teaches its workforce members to identify strange or unusual behavior and data at risk of safeguarding based on FAWE Ethiopia Safeguarding policy.

3.8.4. The IT and safeguarding unit should identify data security needs and privacy training needs through knowledge and skill assessments of workforce members.

3.8.5. The IT and safeguarding unit shall design the content of the training based on the skill assessment made and deliver it to the workforce.

3.8.6. FAWE Ethiopia should prioritize the use of training resources based on the needs of the organization.

3.8.7. The exceptions to this policy shall be handled by the exception handling article of this policy.

4. EXCEPTION HANDLING AND POLICY MANAGEMENT

4.1. Exception handling to this policy

This section handles all exceptions thrown by this policy.

4.1.1. A request for an exception must be completed and sent to the Executive Director, if a work force is unaware of their security non-compliance.

4.1.2. There is a need for a written request describing the risk analysis and asking for an exception if a particular team feels the risk is reasonable.

4.1.3. The written exception request should also include mitigating actions.

4.1.4. The Executive Director or a formal representative assigned by the Executive Director, will approve or deny the request for an exception request and maintain documentation for each request. The requester shall be notified of the approval, denial or for any adjustment.

4.1.5. The approved exception should only apply to that particular instance and for a specified time frame, as estimated by the Executive director. The validity period should be stated clearly on the approval notification.

4.2. Policy Enforcement

Violation of this policy may result in disciplinary measures and ministrative sanctions.

4.3. Revision

This policy shall be reviewed and updated every ..... years or as deemed necessary, depending on changes in technology or regulatory requirements.

4.4. Effective Date

a. This Data security Policy shall be implemented as soon as its approved.

b. The approved policy shall be communicated by the FAWE Ethiopia to all concerned stakeholders.