VISION INITIATIVE FOR TRANSFORMATION
(VITRA)
"Restoring Hopes & Transforming Communities"
Rock City, Jebel – Munuki, Juba | Central Equatoria State, South Sudan
Tel: +211 920 699 912 | +211 928 889 912 Email: vitrasouthsudan@gmail.com
Website: http://www.vitra.simdif.com

# VISION INITIATIVE FOR TRANSFORMATION

# (VITRA)

# DATA PROTECTION POLICY

## 1. Scope

This principles outlined in this policy apply to the processing of personal data. The policy does not apply to anonymous information that cannot be linked to an identified or identifiable natural person**.**

Compliance with this policy is mandatory for any person in the service of Vision Initiative for Transformation (VITRA), including but not limited to employees, intern, volunteers, and consultants. Where appropriate, interns, volunteers, and consultants are expected to adhere to the principles and practices outlined in the policy. Although this policy is primary aimed at the protection of personal data related to Vision Initiative for Transformation (VITRA) programs and operation.

## 2. Purpose of the Data Protection policy

Vision Initiative for Transformation (VITRA) acknowledges that information technology should be at the service of every citizen. Information technology development shall take place in the context of international co-operation. Information technology shall not violate human identity, human rights, privacy, or individual or public liberties. VITRA is committed to international compliance with Data protection Laws, particularly while working in humanitarian context of South Sudan. The data protection policies applies worldwide to VITRA operations in South Sudan and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy relationships and the reputation of VITRA as a credible organization. The data protection policy ensures the adequate level of data protection as prescribed by relevant international legal framework as per international law and ethical standards, including in South Sudan that does not yet have adequate data protection laws. VITRA data protection policy is meant to be a practical and easy to understand document to which all VITRA departments, its staff and responsible staff for implementation and monitoring of this policy for its abidance by its staff and associates, can refer to.

## 3. Scope

This policy applies to all Vision Initiative For Transformation (VITRA)’s employees, contractors, consultants, and any third parties who have access to Vision Initiative For Transformation (VITRA)'s data and systems, both digital and physical, including but not limited to:

- Personal identifiable information (PII)
- Financial data
- Health records (if applicable)
- Confidential business information
- Intellectual property
- Email addresses
- Telephone numbers

- Identity card and passport
- Fingerprints

**4. Data Classification**

Data should be classified into the following categories based on sensitivity:

- **Confidential**: Includes sensitive information that must be protected (e.g., PII, financial records).
- **Internal Use**: Information that is not classified as confidential but still requires limited access (e.g., internal reports).
- **Public**: Information that can be shared with the public without harm.

**5. Data Access Control**

- **Access Rights**: Access to data is granted based on the principle of least privilege. Employees and contractors should only be granted access to the data necessary for their role.
- **Authentication**: Strong authentication methods, such as multi-factor authentication (MFA), must be implemented for accessing sensitive data.
- **Authorization**: Access to data must be regularly reviewed and updated based on job role and responsibilities.

**6. Data Protection**

- **Encryption**: Sensitive data must be encrypted both in transit (e.g., via SSL/TLS) and at rest (e.g., using AES-256 encryption).
- **Backup**: Regular backups of all critical data must be made, and backup systems should be secured and tested periodically to ensure data integrity and availability.
- **Data Masking and Tokenization**: Where possible, sensitive data should be masked or tokenized to reduce exposure.

**7. Data Handling Procedures**

- **Data Collection**: Only the minimum necessary data should be collected and processed, in line with the purpose for which it was collected.
- **Data Retention**: Data must be retained only for the duration required to fulfill the business purpose or to comply with legal obligations. Retention schedules should be established, and unnecessary data must be securely deleted.
- **Data Disposal**: When data is no longer needed, it must be disposed of in a secure manner (e.g., shredding physical documents, securely erasing digital files).

- **Third-Party Access**: Any third party with access to [Company Name] data must comply with the organization's data security standards and sign appropriate confidentiality agreements.

**8. Incident Response and Reporting**

- **Incident Response**: In the event of a data breach or security incident, the organization will follow the established incident response plan. This includes immediate containment, investigation, notification to affected parties, and mitigation measures.
- **Reporting**: Employees are required to report any suspected data breaches or security vulnerabilities to the designated security officer immediately.

**9. Employee and Third-Party Requirements**

- **Employee Training**: All employees and contractors must undergo regular training on data security practices and procedures.

**10. Compliance and Legal Requirements**

- Vision Initiative For Transformation(VITRA) will comply with all relevant data protection laws and regulations, including but not limited to:
    - The General Data Protection Regulation (GDPR) for EU residents
    - The California Consumer Privacy Act (CCPA)
    - Health Insurance Portability and Accountability Act (HIPAA), if applicable
    - Any local or international data protection laws relevant to the business

**11. Security Monitoring**

- Continuous monitoring of systems and networks will be carried out to detect any unauthorized access attempts or anomalies in data access patterns.
- Logs of data access will be maintained and regularly reviewed to ensure compliance with security policies.

- Failure to comply with this Data Security Policy will result in disciplinary action, which may include termination of employment or contractual agreements.

**12. Principle of processing Data**

1. **Fairness and Lawfulness**

When processing personal data, the individual rights of the data subject must be protected. Personal data must be collected and processed in a legal and fair manner.

- Collected data shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing.

- Individual data can be processed upon voluntary consent of the person concerned.

Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

2. **Restriction to a specific purpose**

    - Personal data can be processed only for the purpose that was defined before the data was collected.

    - Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. • Subsequent changes to the purpose are only possible to a limited extent and require justification.

    - However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to take decisions with respect to the data subjects.

3. **Transparency**

    The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of, or informed of:

    • The purpose of data processing; -

    • Categories of third parties to whom the data might be transmitted.

    Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal and ethical obligation to which VITRA is subject; the protection of the data subject's life; the performance of a public service mission entrusted to VITRA.

4. **Confidentiality and Data Security**

- Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

5. **Deletion**
    - Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. **Factual accuracy and up to datedness of data**
    - Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

## 13. Data Processing

### 1. Consent to Data Processing

• Individual data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. In certain exceptional circumstances, consent may be given verbally.

### 2. Data processing Pursuant to Legitimate Interest

• Personal data can also be processed if it is necessary to enforce a legitimate and ethical interest of Vision Initiative For Transformation (VITRA). Legitimate interests are generally of a legal (such as filing, enforcing or defending against legal claims), audit or financial nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the individual merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of personal data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the organisation in performing the control measure (e.g. compliance with legal provisions and internal rules of the organisation) must be weighed against any interests meriting protection that the individual affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

## 3. Telecommunications and Internet

• Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by Vision Initiative For Transformation (VITRA) primarily for work related assignments. They are a tool and an organizational resource. They can be used within the applicable legal regulations and internal Vision initiative For Transformation (VITRA) communication policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

• There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by Vision Initiative for Transformation (VITRA) that block technically harmful content or that analyze the attack patterns.

• For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of Vision initiative For Transformation (VITRA). The relevant South Sudanese national laws must be observed in the same manner as the Vision Initiative For Transformation (VITRA) regulations and ethical standards.

## 4. Rights of the Data Subject

• All individuals who are the subject of personal data held by Vision Initiative For Transformation (VITRA) are entitled:

• To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. If personal data is transmitted to third parties, individuals should be informed of such a possibility. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

• To request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

• To object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

**Transmission of Personal Data**

Transmission of personal data to recipients outside or inside VITRA is subject to the authorisation requirements for processing personal data and requires the consent of the data subject. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside VITRA, this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.

The processing of personal data is also permitted if national legislation requests, requires or authorises this. The type and extent of data processing must be necessary for the legally authorised data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the individual that merit protection must be taken into consideration.

In certain circumstances, the VITRA Data Protection Policy allows personal data to be disclosed, based on a legal obligation, to law enforcement, without the consent of the data subject. Only VITRA's Executive Director can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to Vision Initiative For Transformation(VITRA). Before approving such disclosure, VITRA's Executive Director will check that the recipient of the data uses the data for the defined purposes only, and that it demonstrates the capacity and will to abide by such an obligation. Where necessary, Vision Initiative For Transformation(VITRA)'s Executive Director will refer to legal advisers for advice, and to VITRA's respective managers for written validation, notably but not only in cases involving direct security threats and implications or global organisational risks including reputation.

14. **Subject access and modification requests to personal data**

All Vision Initiative For Transformation(VITRA) staff and external individuals to the NGO can contact VITRA to request rights. Rights of the Data Subject to be applied. Individual subject access requests from individuals should be addressed by email or in writing. If not in writing, the request should be taken and handled by a duly authorised VITRA staff and registered in a log for
reference and follow up. Any individual subject access request received by Vision Initiative For Transformation(VITRA) will be duly verified before being handled, with the verification of the identity of anyone making a subject access request, before handing over any information. A responsibility holder is VITRA Executive Director. VITRA will ensure to respond to individual requests in a timely manner in a written form. VITRA

will ensure that any data subject, including but not only personnel, individual donors and sympathisers, and beneficiaries, have the means to contact VITRA to verify the data VITRA holds about them, and can have authorised (written notice) VITRA personnel update and correct personal information. Such an obligation entails the following:

• VITRA staff should have access to their personal files and to any information held by VITRA on them, by simple request to Human Resources department, to be presented and corrected by a duly authorised staff only. The consultation of any information on any other staff is strictly prohibited.

• Individual donors, partners in alliances/networks membership and sympathisers listed by VITRA can reach out to VITRA to check the data held by VITRA and have it corrected as well as deleted. Information on this right and on how to reach out to VITRA for such a purpose should be clearly indicated on VITRA Official Website, VITRA's organizational page on Facebook as well as on the main media of communication to Individual donors and sympathisers, including donation receipts and donor documentation, and upon request when calling VITRA Coordination Office in Juba. Such a responsibility lies at the primary level with the VITRA Executive Director.

• VITRA current direct and indirect beneficiaries (including survey interviewees) shall have access to VITRA to check any data VITRA holds on them, to ensure its correctness, fairness, and to have it modified and updated upon request by duly authorised VITRA managers – with prime responsibility of VITRA Executive Director. For such a purpose, VITRA teams at Juba coordination office level should set up and maintain complaints response mechanism that is both open and accessible to individuals, with limited constraints, while ensuring that any request by individuals is duly followed by appropriate corrective measures and communications. Contact information to uphold this right and reach out to VITRA for such a purpose should be clearly indicated on VITRA Official Website as well as on other means of public information at VITRA Coordination Office in Juba level. Such a responsibility lies with the VITRA Executive Director at country level and with TITI FOUNDATION's Head of Programmes.

• VITRA contractors and suppliers can reach out to VITRA at coordination office in Juba to check data held by VITRA and have it corrected. Such a responsibility lies with the VITRA Operations Manager in charge of data

• VITRA partners shall have access to VITRA to check any data IMPACT holds on them, to ensure its correctness, fairness, and to have it modified and updated upon request by duly authorized VITRA personnel – Executive Director and /or Operations Manager. Such a responsibility lies with the above two senior responsibilities – holders in office level in Juba. Article 9 - Providing information VITRA aims to ensure that individuals are aware that their data is being processed, and that they understand:

• How the data is being used;
• How to exercise their rights;

To these ends, the current policy is shared with all VITRA staff and available on request by individuals. A version of this Policy is also available upon request to VITRA Office in Juba. Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by VITRA, except if already previously informed, regarding: the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device; the means vailable to them to object to such action.

15. **Confidentiality of Processing Personal data is subject to data secrecy.**

Any unauthorised collection, processing, or use of such data by employees is prohibited. carry out as part of his/her legitimate duties is unauthorised. The "need to know" principle applies. Duly-authorised employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

16. **Processing Security**

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). The technical and organisational measures for protecting personal data are part of VITRA's ITC management (IT) and must be adjusted continuously to the technical developments and organisational changes.

**17. Data Protection Control**

Compliance with the Data Protection Policy and the applicable data protection and ethical standards practiced in humanitarian, peace and development nexus is checked regularly by

VITRA Operations Manager and Head of Programs. The performance of these controls is the responsibility of VITRA's Executive Director or appointed representative. The results of the data protection controls performed by appointed representative must be reported to the Executive Director.

## 18. Violation, sanction and reporting

Any failure to comply with the current policy or to deliberately violate the rules set in the policy will result in the launch of an appropriate investigation by VITRA. Depending on the gravity of the suspicion or accusations, VITRA may suspend staff or relations with other stakeholder during the investigation. This will not be subject to challenge. Depending on the outcome of the independent investigation, if it comes to light that anyone associated with VITRA has deliberately violated the rules set in the policy for its personal profit or any other usage of personal data, or has systematically and deliberately contravened with the principles and standards contained in this document, VITRA will take immediate disciplinary action and any other action which may be appropriate to the circumstances.

This may mean, for example, for:

• Employees - disciplinary action/dismissal;

• Trustees, officers and interns - ending the relationship with the organisation;

• Partners - withdrawal of funding/support;

• Contractors and consultants - termination of contract. Depending on the nature, circumstances and location of the case and violation, VITRA will also consider involving authorities such as the police to ensure the protection of personal data and victims. The reporting of suspected or actual violations to this policy is a professional and legal obligation of all staff and partners.

Failure to report information can lead to disciplinary action. VITRA encourages its staff and stakeholders to report suspected cases which involve any VITRA staff, consultants, board members, guests or staff of VITRA's partner organisations, their board members, staff and or suppliers. VITRA encourages its staff and stakeholders to report suspected cases through the following means:

• Staff and interns can report contacting standard lines of hierarchy (contained in staff Terms of Reference); the Head of Human Resources.

• Beneficiaries and their representatives can report using the Complaints and Response Mechanism (CRM) and /or Code of Conduct Reporting Mechanism. • Suppliers and contractors can use the confidential email address (Executive Director is to be contacted). The email address will be copied too by posting on VITRA official website too.

• Individual donors and sympathisers can refer to the confidential email address (Executive Director is to be contacted). The email address will be copied too by posting on VITRA official

website too. All reports will be treated as confidential in line with VITRA's Code of Conduct and VITRA's Human Resources guidelines. VITRA will not tolerate false accusations which are designed to damage a member of staff's reputation. Anyone found making false accusations will be subject to investigation and disciplinary action. Responsibilities VITRA's Executive Director and Operations Manager is responsible to ensure that the legal

Personal data protection of VITRA's primary and secondary beneficiaries.

Scope:

• This Policy applies to all personal data held by TITI FOUNDATION in relation to persons of concern to VITRA the processing of other data, e.g. aggregated or anonymized, does not fall within the scope of this Policy.

• This Policy applies whether processing takes place within one VITRA office, between different TITI FOUNDATION offices (offices and coordination office in Juba), or whether personal data is transferred to partners or third parties. The Policy continues to apply even after persons are no longer of concern to VITRA.

• Compliance with this Policy is mandatory for all VITRA

Basic principles:

Basic principles of personal data processing: VITRA staff and other associates need to respect and apply the following basic principles when processing personal data:

• Legitimate and fair processing

• Purpose specification

• Necessity and proportionality

• Respect for the rights of the data subject

• Confidentiality

• Security
• Accountability and supervision Legitimate and fair processing Processing of personal data may only be carried out on

## Transfer of personal data to third parties:

GENERAL CONDITIONS

VITRA may transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy

Given the potential data protection risks involved in transfers to third parties, VITRA needs to pay particular attention to the following basic principles of this Policy: 1

i.Transfer is based on one or more legitimate bases;

ii. Transfer is for one or more specific and legitimate purpose(s);

iii. The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;

iv. The data subject has been informed, either at the time of collection or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions apply;

v. The third party respects the confidentiality of personal data transferred to them by VITRA. Whether or not a data transfer agreement has been signed between VITRA and the third party, VITRA must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication;

vi. The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure

## 19. Policy Enforcement

- The policy will be reviewed and updated regularly to ensure continued compliance with evolving security practices and legal requirements.

**20. Policy Review**

This policy shall be reviewed at least annually or in response to significant changes in business operations, legal requirements, or technological advancements.

**21. Acknowledgment**

All employees and third parties must acknowledge receipt and understanding of this Data Security Policy upon hire or engagement with Vision Initiative For Transformation(VITRA) and periodically thereafter.

---

**Acknowledged by:**
Signature: _____
Name: _____
Position: _____
Date: _____