منظمة أشرعة الأمل
SAILS OF HOPE ORGANIZATION

# Data Security Management Policy

## 1. Introduction

SHO is committed to ensuring the confidentiality, integrity, and availability of the data we collect, process, and store in the course of our operations. This Data Security Management Policy outlines our commitment to implementing robust data security measures to protect against unauthorized access, disclosure, alteration, or destruction of data, in compliance with relevant international, national, and local laws and regulations, including the General Data Protection Regulation (GDPR) and applicable Sudanese legislation.

## 2. Scope

This policy applies to all data collected, processed, or stored by SHO, including personal data, financial data, program data, and any other sensitive or confidential information, regardless of format or storage medium. It applies to all staff, volunteers, partners, and third parties who have access to SHO's data systems or information assets.

## 3. Principles

a) Confidentiality: SHO will protect the confidentiality of data by ensuring that only authorized individuals have access to it and by implementing appropriate access controls and encryption mechanisms.
b) Integrity: SHO will maintain the integrity of data by ensuring that it is accurate, complete, and reliable, and by implementing measures to detect and prevent unauthorized alterations.
c) Availability: SHO will ensure the availability of data by implementing appropriate backup and disaster recovery procedures to minimize the risk of data loss or unavailability.
d) **Compliance: SHO will comply with all relevant data protection laws, regulations, and industry standards, and will regularly review and update our data security practices to ensure ongoing compliance.

## 4. Data Classification

SHO will classify data based on its sensitivity, importance, and regulatory requirements, and will implement appropriate security measures based on the classification level. Data may be classified as:

- Public: Information that can be freely disclosed to the public without risk of harm to SHO or individuals.
- Internal: Information that is intended for internal use within SHO and should be protected from unauthorized access or disclosure.
- Confidential: Sensitive information that requires the highest level of protection due to legal, ethical, or privacy considerations.

**5. Access Control**

a) Access to data will be granted on a need-to-know basis, with permissions assigned based on job roles, responsibilities, and business requirements.
b) User accounts will be created for authorized individuals only, with strong passwords and multi-factor authentication where possible.
c) Access to sensitive data will be restricted and monitored, with regular reviews and audits of user permissions and access logs.

**6. Data Encryption**

a) SHO will implement encryption mechanisms to protect data both in transit and at rest, using industry-standard encryption algorithms and protocols.
b) Encryption will be applied to sensitive data stored on servers, databases, mobile devices, and removable media to prevent unauthorized access or interception.

**7. Network Security**

a) SHO will implement firewalls, intrusion detection systems (IDS), and other network security measures to protect against unauthorized access, malware, and cyber threats.
b) Remote access to SHO's network and systems will be secured through virtual private networks (VPNs) and secure authentication mechanisms.

**8. Physical Security**

a) Physical access to data storage facilities, server rooms, and data centers will be restricted to authorized personnel only, with access controls, surveillance cameras, and alarm systems in place.
b) Portable devices containing sensitive data will be encrypted and protected with physical security measures to prevent loss or theft.

**9. Data Backup and Recovery**

a) SHO will implement regular backup procedures to create copies of critical data and information systems, with off-site storage and redundancy to ensure data availability in the event of a disaster or system failure.
b) Data backup and recovery processes will be tested regularly to verify their effectiveness and reliability.

**10. Incident Response and Reporting**

a) SHO will establish an incident response team responsible for detecting, responding to, and mitigating data security incidents, including breaches, unauthorized access, or data loss.
b) All data security incidents will be promptly reported to management, documented, and investigated, with appropriate corrective actions taken to prevent recurrence.

**11. Training and Awareness**

a. SHO will provide regular training and awareness programs for staff, volunteers, and partners on data security best practices, policies, and procedures.
b. Employees will be educated on the importance of data security, their roles and responsibilities in safeguarding data, and the potential risks associated with data breaches.

**12. Compliance and Monitoring**

a. SHO will conduct regular assessments and audits of our data security practices to ensure compliance with this policy and applicable laws and regulations.
b. Any deficiencies or non-compliance issues identified will be addressed promptly, with corrective actions implemented to mitigate risks and improve data security posture.

**13. Review and Revision**

- This Data Security Management Policy will be reviewed and updated as necessary to reflect changes in SHO's operations, technology environment, regulatory requirements, and emerging threats to data security.
- This Data Security Management Policy is designed to meet UN standards, international law, and local regulations in Sudan, ensuring the protection of data collected and processed by SHO. Adjustments may be necessary based on specific organizational needs, legal advice, and stakeholder input.