Volunteers National Organization for Development and Humanitarian Services

Cybersecurity and Password Policy Standard Operating Procedure (SOP)

Organizations Background:

Volunteers National Organization for Development and Humanitarian Services is a Sudanese women lead NGO registered as a national voluntary charitable humanitarian non-governmental organization founded by group of women and youth volunteers, whom work in humanitarian and development domain. The creation of this organization is inspired by a feeling among this group that something must be done to mitigate the sufferings of women's, girls and youth in Darfur in particularly and in Sudan in general.

Volunteers National Organization for Development and Humanitarian Services was established in 2014, and was officially registered with the humanitarian aid commission (HAC) as a local, non-governmental organization to provide relief, and advocate for the promotion of human rights principles.

Volunteers National Organization for Development and Humanitarian Services is a non-religious non-political, non-profitable and non-commercial organization; it is basically a humanitarian organization whose vision is to promote "Peace, Unity Development, women rights and women Empowerment for All" among the different communities, ethnic groups and tribes in Darfur and Sudan in general. National Volunteers has been able to acquire sufficient community goodwill that will enable it to implement future activities smoothly

Introduction:

Cybersecurity and Password Policy Standard Operating Procedure (SOP) document it is customize for Volunteers National organization. It outlines best practices, responsibilities, and policy enforcement.

Cybersecurity and Password Policy Standard Operating Procedure (SOP)

Document Title: Cybersecurity and Password Policy SOP
Version: 1.0
Date: July 9, 2025
Approved By: [Name / Title]
Next Review Date: [e.g., July 9, 2026]
Confidentiality Level: Internal Use Only

1. Purpose

This SOP outlines the organization's policies, roles, and procedures to ensure the security of digital systems, safeguard sensitive information, and enforce strong password management across all systems.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and third-party vendors who access or manage information systems and data assets of [Organization Name].

3. Roles and Responsibilities

Role	Responsibility
IT Security Officer	Oversee implementation and compliance with cybersecurity protocols
System Administrators	Implement and monitor technical controls
End Users	Comply with password and cybersecurity requirements

Role	Responsibility
HR Department	Ensure staff are trained and policy is acknowledged during onboarding

4. Cybersecurity Policy

4.1 Acceptable Use

- Users shall access IT resources only for legitimate business or academic purposes.
- Personal use of company systems must be minimal and not interfere with job responsibilities.

4.2 Data Classification

- **Public**: Approved for open access (e.g., marketing brochures).
- **Internal**: Limited to internal employees.
- **Confidential**: Sensitive data requiring strict access control (e.g., financial records).
- **Restricted**: Highly sensitive data, e.g., PII, PHI, IP, trade secrets.

4.3 Device Security

- All endpoints (desktops, laptops, mobile devices) must have:
  - Antivirus software
  - Device encryption
  - Screen lock after 10 minutes of inactivity

4.4 Email Security

- Do not open suspicious links or attachments.
- Use spam filters and report phishing attempts to IT security.

4.5 Network Security

- Secure VPNs must be used for remote access.
- All Wi-Fi networks must be encrypted (WPA3 or enterprise-level WPA2 minimum).
- Firewalls and IDS/IPS systems must be maintained and monitored.

4.6 Software and Patch Management

- Only authorized software may be installed.
- Systems must be patched regularly and monitored for vulnerabilities.

4.7 Incident Response

- All incidents must be reported within 1 hour of discovery to vnodhs@volunteersno.org].
- The IT Security Officer will initiate the Incident Response Plan (IRP) and maintain a record of all incidents.

5. Password Policy

5.1 Password Creation

- Minimum length: **12 characters**
- Must include at least one:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special character (e.g., @, #, %, ^)

5.2 Password Management

- Passwords must **not** be reused across systems.
- Must be changed every **90 days**
- Cannot reuse the **last 5 passwords**
- Use of password managers (approved by IT) is strongly encouraged.
- Multi-factor authentication (MFA) is **mandatory** for:
  - Email
  - VPN
  - Cloud services
  - Admin access

5.3 Password Protection

- Never share passwords.
- Do not write down or store plaintext passwords.
- If a password is suspected to be compromised, change it immediately and notify IT.

5.4 Service Accounts

- Must use complex passwords (16+ characters).
- Passwords must be rotated at least every **180 days** or when staff changes occur.

6. Enforcement and Compliance

- Violations of this policy may result in disciplinary action, including suspension or termination.
- Regular audits will be performed.
- Periodic phishing simulations and cybersecurity awareness training will be conducted at least **quarterly**.

7. Training and Awareness

- Mandatory cybersecurity training for all new hires within the first **7 days**.
- Annual refresher training for all employees.
- Training topics include phishing, safe browsing, data handling, and secure password practices.

8. Review and Revision

- This policy will be reviewed **annually** or after a major security incident.
- Revisions will be approved by IT Security and senior leadership.

Last review for this policy is January, 2025