Volunteers National Organization for Development and Humanitarian Services

Standard Operating Procedure (SOP): Security Assessment

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:

Security Assessment Standard Operating Procedure (SOP) designed for organizations to evaluate the effectiveness of their physical, digital, and operational security controls.

Standard Operating Procedure (SOP): Comprehensive Security Assessment

1. Purpose

To establish a standardized process for conducting comprehensive security assessments that evaluate an organization's physical, cyber, and personnel security to identify vulnerabilities, ensure compliance, and mitigate risks.

2. Scope

This SOP applies to all departments, facilities, IT systems, personnel, and third-party services within the organization's operational domain.

3. Definitions

- **Security Assessment:** A systematic evaluation of an organization's security controls.
- **Vulnerability:** A weakness in security procedures, system design, implementation, or internal controls.
- **Threat:** A potential cause of an unwanted incident.
- **Risk:** The potential for loss or damage when a threat exploits a vulnerability.

4. Roles and Responsibilities

Role	Responsibility
Chief Security Officer (CSO)	Overall oversight, approval of findings and remediation plan.
Assessment Team Lead	Coordination and execution of the assessment process.
IT Security Analyst	Conducting cyber assessments, penetration testing, and vulnerability scans.
Physical Security Officer	Evaluating physical access control, surveillance, and safety systems.
HR/Personnel Security Officer	Reviewing employee security policies, training, and background checks.
Internal Audit	Validating assessment integrity and compliance.

5. Assessment Frequency

- **Comprehensive Assessment:** Annually
- **Targeted or Ad-hoc Assessments:** As required after major changes, breaches, or incidents

6. Assessment Process

6.1. Planning Phase

1. **Define Objectives and Scope**
   - Identify business units, systems, and assets to assess.
   - Establish legal/regulatory requirements.
2. **Form the Assessment Team**
   - Include representatives from IT, HR, Physical Security, and Legal as needed.
3. **Develop Assessment Plan**
   - Include tools, techniques, timeline, and documentation templates.

6.2. Information Gathering

- Review past incident reports, policies, and configurations.
- Interview key stakeholders.
- Inventory assets and data flows.

6.3. Security Controls Evaluation

A. Cybersecurity Evaluation

- Vulnerability scanning (internal and external)
- Penetration testing
- Configuration reviews (firewalls, routers, servers)
- Patch management assessment
- User access reviews
- Data encryption and backup checks

B. Physical Security Evaluation

- Perimeter security (fencing, gates)
- Surveillance system review (CCTV, alarms)
- Access control systems (badges, biometric)
- Visitor management
- Emergency response readiness

C. Personnel Security Evaluation

- Background checks and onboarding processes
- Security awareness training
- Policy compliance (acceptable use, remote work)
- Insider threat programs

6.4. Risk Analysis and Reporting

1. **Identify Risks**
    - Based on threat likelihood and impact.
2. **Risk Prioritization**
    - Use a risk matrix or heat map.
3. **Draft the Security Assessment Report**
    - Executive summary
    - Detailed findings and evidence
    - Risk ratings
    - Recommended mitigation strategies
4. **Presentation to Management**
    - Deliver findings and remediation options.

6.5. Remediation and Follow-Up

- Assign ownership of remediation actions.
- Set timelines and track implementation.
- Perform validation checks or retesting.
- Update documentation and risk registers.

7. Documentation and Records

Maintain secure records of:

- Assessment plans and scope
- Evidence collected
- Final report and approvals
- Remediation actions and status

8. Tools and Resources

- Vulnerability scanners (e.g., Nessus, Qualys)
- Penetration testing frameworks (e.g., Metasploit, Burp Suite)

- Physical security audit checklists
- HR policy templates
- Compliance frameworks (ISO 27001, NIST, CIS)

9. Compliance and Standards

Ensure alignment with:

- GDPR, HIPAA, or other relevant regulations
- Organization's internal policies

10. Review and Updates

- This SOP must be reviewed annually or after a significant security event.
- All updates require approval from the CSO.



