*Volunteers National Organization for Development and Humanitarian Services*

# *Digital Asset Protection Policy*

***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

Below is an extensive list of security measures that can be deployed to ensure your digital asset protection. However, not everyone will be suitable for your business. Your business is unique and your security measures should reflect that.

## 1. Comprehensive Security Implementation

- Endpoint security deployment across all devices accessing digital assets, including workstations, mobile devices, and remote access points
- Advanced managed firewalls with real-time monitoring and threat detection capabilities

- Phishing-resistant Multi-Factor Authentication (MFA) implementation across all critical systems
- Systematic patch management protocols with automated updates and compliance tracking
- Strategic network segmentation to isolate sensitive client data and intellectual property from general business operations
- Regular security assessments by experienced IT risk experts to identify and address potential vulnerabilities – particularly important given that only **31%** of businesses conducted cyber security risk assessments in the past year

## 2. Strategic Access Management

Strong authentication methods and access control form the foundation of protecting digital assets:

- Role-based access control
- Continuous verification of users and devices through zero-trust architecture
- Comprehensive monitoring and logging of all system access attempts
- Detailed audit trails with automated alerts for suspicious activities
- Regular access review and adjustment based on role changes
- Secure remote access protocols supported by 24/7 IT expertise

## 3. Data Security Protocols

To protect digital assets effectively:

- End-to-end encryption for all sensitive data during storage and transmission
- Secure file-sharing platforms with built-in encryption and access controls
- Advanced Data Loss Prevention (DLP) solutions with content analysis capabilities
- Clear data handling procedures aligned with industry standards
- Regular data classification reviews and updates
- Secure data disposal protocols for obsolete information

## 4. Robust Backup Solutions

Secure your digital content through:

- Automated backup systems with multiple redundancy levels
- Regular restoration testing to ensure data integrity
- Comprehensive business continuity planning with defined recovery objectives
- Encrypted backup storage with strict access controls
- Clear documentation of backup and recovery procedures maintained by dedicated IT professionals

## 5. Employee Security Training

Most data breaches happen because of human error – often, hackers do not 'break in' to a system, they log in.



Strengthen your security measures through:

- Comprehensive cybersecurity awareness programmes
- Specific training for handling sensitive files and intellectual property
- Regular updates on emerging threats and phishing attack methods
- Documented security procedures with clear guidelines
- Recognition programmes for security-conscious behaviour

## 6. Collaboration Security

For professional service businesses or engineering firms working with external partners:

- Secure collaboration platforms with encrypted communications
- Strict access controls for external users
- Real-time monitoring of collaborative activities
- Intellectual property protection through digital rights management
- Clear policies for external information sharing
- Regular review of collaboration security measures by IT security experts

## 7. Standards Compliance

Meet industry requirements through:

- Implementation of recognised security frameworks such as Cyber Essentials, Cyber Assurance and ISO 27001 if required for your industry
- Regular internal and external security assessments
- Maintenance of relevant certifications including Cyber Essentials – organisations holding Cyber Essentials certification are **92%** less likely to claim on cyber insurance policies
- Comprehensive documentation of compliance measures
- Regular updates to meet evolving standards
- Clear assignment of compliance responsibilities

## 8. Professional IT Support

Partner with experienced IT professionals who can:

- Provide 24/7 security monitoring and threat detection
- Respond rapidly to potential security incidents
- Maintain and update security infrastructure
- Offer strategic guidance on security improvements
- Conduct regular security assessments
- Provide ongoing technical support and training with a personal touch

## 9. Physical Security Integration

Protect your digital assets through:

- Secure onsite server locations with controlled access (if applicable)



- Regular security audits of physical locations (if servers are kept onsite)
- Integration of physical and digital security measures
- Clear protocols for physical access to areas where sensitive information is stored
- Documentation of physical security procedures

### 10. Incident Response Planning

Prepare for security incidents with:

- Detailed response protocols for various scenarios
- Clearly defined team responsibilities and escalation procedures
- Comprehensive incident documentation procedures
- Post-incident analysis and improvement processes
- Regular updates to response strategies

## Taking Action on Digital Asset Protection

For all businesses – whether in engineering, law, or consultancy – **protecting digital assets requires a balanced approach** combining technical controls, employee awareness, and professional IT support.

The key lies in finding an IT partner who understands the specific needs of small and medium-sized businesses and can provide personalised attention to each user while maintaining enterprise-level security standards.

Success in digital asset protection depends on implementing comprehensive security measures while maintaining operational efficiency. While 75% of businesses report that cybersecurity is a high priority for their senior management, only 22% have formal incident response plans in place.

This balance is particularly crucial for professional service businesses and engineering firms where rapid access to digital resources directly impacts productivity and client service delivery.

### Getting Started with Enhanced Protection

1. Conduct a thorough assessment of your current digital assets
2. Identify critical resources requiring enhanced protection
3. Evaluate existing security measures against industry standards
4. Develop a prioritised implementation plan
5. Establish clear metrics for security effectiveness
6. Create a timeline for security improvements

## Digital Asset Protection Policy

### 1. Purpose



The purpose of this policy is to define the procedures and responsibilities for the protection of digital assets owned or managed by [Organization Name]. Digital assets include all forms of data, media, and content stored digitally that have value to the organization.

## 2. Scope

This policy applies to all employees, contractors, third-party partners, and anyone with access to the organization's digital assets. It covers all systems, networks, cloud services, and storage devices.

## 3. Definitions

- **Digital Assets:** Includes data, documents, intellectual property, digital content, system configurations, databases, source code, and digital credentials.
- **Asset Owner:** The individual or department responsible for a digital asset.
- **Sensitive Data:** Any information that must be protected due to confidentiality, legal, or regulatory requirements.

---

## 4. Policy

### 4.1. Asset Inventory

- Maintain an up-to-date inventory of all digital assets.
- Assign ownership and classification to each asset (e.g., confidential, internal, public).

### 4.2. Access Control

- Implement role-based access control (RBAC) to restrict access based on job function.
- Enforce strong authentication methods (e.g., MFA).
- Review access permissions quarterly.

### 4.3. Data Security

- Encrypt sensitive data at rest and in transit.
- Store digital assets only in approved, secure locations (e.g., company cloud storage).
- Prohibit the use of personal storage services for company data.

### 4.4. Backup and Recovery

- Regularly back up all critical digital assets.
- Test recovery procedures semi-annually to ensure data integrity and availability.

### 4.5. Monitoring and Auditing



- Implement continuous monitoring of access and usage of digital assets.
- Log access and changes to sensitive digital assets for audit purposes.

### 4.6. Third-Party Management

- Ensure third-party vendors comply with this policy or have equivalent standards.
- Use NDAs and data processing agreements where applicable.

### 4.7. Incident Response

- Report any suspected compromise or loss of digital assets immediately to the IT Security team.
- Investigate and document incidents in accordance with the organization's incident response plan.

### 4.8. Training and Awareness

- Conduct annual training on data protection and cybersecurity best practices.
- Provide role-specific guidance on secure digital asset handling.

## 5. Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination, as well as potential legal consequences.

## 6. Review and Updates

This policy will be reviewed annually and updated as needed to reflect changes in technology, regulatory requirements, or business operations.

