Site 99 UG LTD | Information Security Policy

Document owner: Data Protection Officer, Site 99 UG LTD
Version: 1.0.0
Effective date: 1st July, 2026
Next review date: 1st July, 2027
Approved by: Board of Directors

1. Purpose

This policy defines how Site 99 UG LTD ("Site 99") protects the confidentiality, integrity and availability of its information, systems and the personal data entrusted to it by staff, clients and the public. It supports our Data Protection Policy and our obligations under the Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations, 2021, which require appropriate technical and organisational security measures.

2. Scope

This policy applies to all directors, employees, interns, contractors and partners, and to all information assets: laptops, phones and other devices, cloud platforms and hosting, source code repositories, databases, client portals and systems we build or host, email and messaging, shared drives, paper records and physical premises.

3. Security objectives

- **Confidentiality:** information is accessible only to those authorised.
- **Integrity:** information is accurate and protected from unauthorised change.
- **Availability:** systems and data are available when needed.
- **Compliance:** we meet legal, contractual and client security requirements.

4. Roles and responsibilities

- **Management:** approves this policy, funds security controls, accepts residual risk.
- **Technical Lead / Security Lead:** Bwanika Christian Ryan. Owns technical controls, monitors systems, manages incidents and access reviews.
- **Data Protection Officer:** Rwihura Eineamaani. Oversees personal data protection, breach notification and regulator liaison.
- **Project leads:** apply secure development and access practices on every client project.
- **Everyone:** follows this policy, protects credentials and devices, completes training and reports incidents immediately.

5. Information classification and handling

Class	Description	Examples	Handling
Confidential	Personal data, special personal data, credentials, contracts, financial records, client system data	Client end-user records, staff files, API keys, bank details	Encrypted, access on need-to-know, no sharing via personal accounts, logged access
Internal	Business information not for public release	Project plans, proposals, internal docs	Shared only within Site 99 and authorised partners
Public	Approved for release	Website content, published portfolio work	No restriction after approval

Staff must label or treat unlabelled data as confidential unless told otherwise.

6. Access control

1. **Least privilege:** access is granted only to what a person needs for their role and project.
2. **Unique accounts:** every user has an individual account; shared accounts are prohibited except where unavoidable and then documented and controlled by a password manager.
3. **Multi-factor authentication (MFA):** mandatory on email, cloud platforms, code repositories, hosting and admin panels.
4. **Onboarding and offboarding:** access is requested through the Technical Lead, approved by management, and removed on the day a person leaves or a project ends. Devices and credentials are returned or reset.
5. **Access reviews:** admin and production access is reviewed at least every quarter, and all access at least twice a year.
6. **Role-based access in systems we build:** every client system has defined roles, with administrative functions restricted and actions logged.

7. Passwords and authentication

- Passwords must be at least 12 characters, unique per service, and stored in an approved password manager.
- Default and shared passwords must be changed immediately.
- Passwords are never sent by email or messaging apps in plain text, or written on paper or screens.
- Credentials are reset immediately if compromise is suspected.

8. Device and endpoint security

- Work devices use full-disk encryption, screen lock (maximum 5 minutes), up-to-date operating systems and security patches, and active anti-malware protection.
- Only approved software is installed; pirated software is prohibited.
- Personal devices used for work (BYOD) must meet the same standards, have a screen lock, be free of jailbreaks or root access, and must not store confidential data locally unless encrypted.
- Lost or stolen devices must be reported within 1 hour so that access can be revoked and, if required, a remote wipe performed.
- Removable media (USB drives) are not used for confidential data unless encrypted and approved.

9. Network security

- Office Wi-Fi uses WPA2/WPA3 with a strong passphrase; guest access is separated from work access.
- Staff avoid public or untrusted Wi-Fi for work; where unavoidable they use a VPN.
- Administrative access to servers and hosting is restricted by MFA and, where possible, by IP allow-listing.
- Firewalls and platform security groups follow a deny-by-default approach.

10. Data protection controls

- **Encryption in transit:** all websites, portals and APIs we build or operate use HTTPS/TLS.
- **Encryption at rest:** databases, storage and backups holding Confidential data use encryption provided by the hosting platform or equivalent.
- **Data minimisation and masking:** sensitive fields (IDs, health, financial) are collected only where needed and masked or restricted in interfaces.
- **Separation:** each client's data is logically separated; production data is not used for testing unless anonymised.

- **Secure disposal:** data and devices are securely wiped or destroyed when no longer required; paper records are shredded.

11. Secure development and change management

1. Security and privacy requirements are considered at the start of every project, including a short data protection impact assessment for systems that handle personal data.
2. Source code is stored in access-controlled repositories with MFA, and secrets (API keys, database credentials, tokens) are never committed to code; they are kept in environment variables or a secrets manager.
3. Code changes to production are reviewed, tested in a non-production environment where practical, and recorded.
4. Dependencies and platforms are kept updated, and known vulnerabilities are fixed in a timely way based on severity.
5. Systems are tested for common vulnerabilities (such as broken access control, injection, insecure uploads and exposed secrets) before launch and after major changes.
6. Input validation, authenticated sessions, role checks on every protected action, rate limiting on sign-in and audit logging are standard requirements for the systems we build.
7. Where we use AI tools or automation, confidential or personal data is not entered into tools without an approved agreement and appropriate settings, and outputs are reviewed by a person before use.

12. Logging and monitoring

- Authentication events, administrative actions, data exports and deletions in production systems are logged.
- Logs are protected from alteration, retained for 12 months and reviewed on suspicion of an incident and during periodic checks.
- Hosting and platform alerts are enabled and sent to the Technical Lead.

13. Backup and business continuity

- Production databases and critical files are backed up automatically at least daily, with backups encrypted and stored separately from the primary system.
- Restores are tested at least twice a year.
- A basic continuity plan identifies critical systems, who restores them and the target recovery times agreed with clients.
- Key staff have a documented deputy so that critical access and knowledge do

not rest on one person.

14. Third-party and supplier security

- Suppliers who process personal data or host systems (cloud, hosting, email, payment, analytics, AI and automation services) are assessed before use for security and privacy practices and location of data.
- Written agreements require confidentiality, security measures, breach notification and deletion or return of data at the end of service.
- Approved suppliers are listed in the register of processors maintained by the DPO and reviewed annually.
- Freelancers and contractors sign confidentiality undertakings and receive only the access their task requires.

15. Physical security

- Offices and workspaces are locked when unattended; visitors are supervised.
- Screens are locked when leaving a desk, and paper containing confidential data is stored in locked storage and not left unattended.
- Equipment is recorded in an asset register and securely stored.

16. Email, messaging and remote work

- Staff use company-approved email and collaboration tools for work. Confidential data is not shared through personal email or unapproved messaging apps.
- Staff verify unexpected requests for money, credentials or data (phishing and impersonation) through a second channel before acting.
- Remote workers apply the same standards at home or elsewhere, in a place where screens cannot be viewed by others.

17. Security awareness and training

All staff and contractors complete security and data protection induction before getting access, and refresher training at least annually covering phishing, passwords, device safety, handling personal data and reporting incidents. Attendance is recorded.

18. Incident response

What is an incident: any event that compromises or threatens information security, including lost devices, malware, unauthorised access, leaked credentials, data sent to the wrong person, system outages caused by attack, or a suspected personal data breach.

Step	Action	Owner
1. Report	Report immediately to the Technical Lead and DPO at office@site99ug.com / +256 741 760769	Anyone
2. Contain	Isolate affected accounts or systems, revoke credentials, stop the leak	Technical Lead
3. Assess	Determine what data, which people and which clients are affected, and the risk of harm	Technical Lead and DPO
4. Notify	Notify the Personal Data Protection Office within the legally required period (currently 48 hours of becoming aware) where reportable; notify affected individuals and clients without undue delay	DPO and management
5. Recover	Restore systems from clean backups, patch the cause, verify the fix	Technical Lead
6. Review	Record the incident, root cause, actions and lessons in the incident register and update controls	DPO and Technical Lead

Staff must not attempt to hide or fix an incident quietly; prompt reporting is always expected and protected.

19. Risk management

The Technical Lead and DPO maintain a risk register of key information security risks, assess likelihood and impact, assign owners and review it at least every six months and after any major incident or system change.

20. Compliance, audit and discipline

Compliance with this policy is checked through periodic internal reviews of access, backups, devices and suppliers. Violations may lead to disciplinary action up to termination or contract termination and, where the law is broken, referral to the authorities. Exceptions to this policy must be requested in writing and approved by management with documented compensating controls.

21. Review

This policy is reviewed at least annually and after significant incidents, legal changes or changes to our technology or services.

22. Contacts

Site 99 UG LTD, Kampala, Uganda – site99ug.com Technical / Security Lead: Bwanika Christian Ryan - +256 7723 93259 Data Protection Officer: Rwihura Eineamaani - +256 741 760 769

23. Approval

This policy was approved by the management of Site 99 UG LTD on the date below.

Name	Title	Signature	Date
Rwihura Eineamaani	Co-Founder		1st July, 2026
Tameem Kangave	Co-Founder		1st July, 2026

Version history

1.0.0 - 1st July, 2026