



APPROVED CORPORATE POLICY

Information Security Policy

The controls Chwezi Core Systems applies to protect its systems, the software it builds and hosts, and the information of its clients.

DOCUMENT ID	CCS-POL-ISP-01
VERSION	1.0
STATUS	APPROVED
CLASSIFICATION	Public
POLICY OWNER	Information Security Lead
APPROVED BY	Peter Bamuhigire, Founder and Chief Technology Officer
APPROVAL DATE	27 October 2026
EFFECTIVE DATE	1 November 2026
NEXT REVIEW	October 2027

Peter Bamuhigire
Founder and Chief Technology Officer
For and on behalf of Chwezi Core Systems Limited

27 October 2026
Date of approval
Effective 1 November 2026

Contents

1. Purpose	13. Secure software development
2. Scope	14. Vulnerability and patch management
3. Definitions	15. Logging and monitoring
4. Policy statement and principles	16. Backup, business continuity and disaster recovery
5. Governance, roles and responsibilities	17. Endpoints, mobile devices and remote working
6. Risk management and asset inventory	18. Physical security
7. Information classification and handling	19. Suppliers and third parties
8. People security	20. Incident management
9. Acceptable use	21. Client engagements and on-site work
10. Access control and authentication	22. Compliance, exceptions and breach of policy
11. Cryptography	23. Monitoring, review and related documents
12. Hosting, infrastructure and network security	24. Review and approval history

1. Purpose

This policy sets the rules Chwezi Core Systems Limited ("Chwezi", "we") applies to protect the confidentiality, integrity and availability of the information we hold, the systems we build and host, and the client environments we work in. It tells staff, contractors and clients what controls exist, who owns them and how often they operate.

2. Scope

This policy applies to:

- every director, employee, intern, contractor and consultant who works for Chwezi ("personnel");
- all information Chwezi creates, receives or holds, in any form, including client data held in systems we host;
- all systems we own, rent or operate: laptops and phones used for work, source code repositories, cloud and dedicated servers, email and collaboration tools, and the software products we develop and host (including Kraal Code, Maduuka and Aqar);
- work performed on client premises or in client systems, including cybersecurity assessments and CCTV and access-control installations.

Where a client contract imposes a stricter security requirement than this policy, the contract requirement applies to that client's work.

3. Definitions

Term	Meaning
Asset	Any information, software, device, account or service that has value to Chwezi or a client.
Client data	Information a client, or the client's users, store in or send to a system Chwezi builds, hosts or supports.
Information Security Lead	The person accountable for this policy. Until another person is designated in writing, this is the Founder and Chief Technology Officer.
Multi-factor authentication (MFA)	Sign-in that needs two or more independent factors, such as a password plus an authenticator code or hardware key.
Privileged access	Access that can change system configuration, security settings, other users' rights or production data in bulk, such as server root, database administrator or cloud console owner rights.
Production	A system that serves live users or holds live client data.
Security incident	An event that has compromised, or could compromise, the confidentiality, integrity or availability of an asset.
Personal data breach	A security incident affecting personal data, as defined in the Data Protection and Privacy Policy (CCS-POL-DPP-02).

4. Policy statement and principles

Chwezi protects information in proportion to the harm its loss or misuse would cause. Four principles govern how the rules in this policy are applied:

1. **Least privilege.** A person or system receives only the access needed for the current task, and loses it when the task ends.
2. **Defence in depth.** No single control is relied on alone; production systems are protected by network, identity, application and monitoring controls together.
3. **Security by design.** Security requirements are set at the start of every software project, not added after release.
4. **Evidence over assertion.** Each control produces a record (log, review sign-off, test result) that shows it operated.

Our control set is structured around the four control themes of ISO/IEC 27001:2022 (organisational, people, physical and technological). Chwezi does not currently hold ISO/IEC 27001 certification.

5. Governance, roles and responsibilities

Role	Responsibilities
Founder and Chief Technology Officer	Approves this policy and its exceptions; provides resources; receives the security report; holds the Information Security Lead and Data Protection Officer roles until others are designated in writing.
Information Security Lead	Owns this policy; maintains the risk register and asset inventory; runs access reviews; leads incident response; reports on security performance; arranges training.
Data Protection Officer	Advises on personal data matters; handles data subject requests and notifications to the Personal Data Protection Office (see CCS-POL-DPP-02).
Engineering leads	Apply the secure development rules in section 13; approve production deployments; maintain system documentation.
Systems administrators	Harden, patch, back up and monitor the infrastructure they are assigned; hold privileged access only through named accounts.
Project and engagement managers	Confirm client security requirements at contract stage and make sure the project team applies them.
All personnel	Follow this policy, complete security training, protect their credentials and report suspected incidents immediately.

6. Risk management and asset inventory

6.1 The Information Security Lead must maintain a register of information security risks, recording for each risk its owner, likelihood, impact, treatment and review date.

6.2 The Information Security Lead must review the risk register at least every six months, and whenever a new product, hosting provider or major client system is introduced.

6.3 The Information Security Lead must maintain an inventory of production servers, domains, cloud accounts, code repositories and work devices, with a named owner for each entry.

6.4 A project manager must not start work on a new client system that will hold personal or financial data until its security risks have been assessed and recorded.

7. Information classification and handling

7.1 Chwezi classifies information into four levels:

Level	Examples	Minimum handling rule
Public	Website content, published policies, marketing material	May be shared freely once approved for release.
Internal	Internal procedures, non-sensitive project plans	Must not be shared outside Chwezi without a business need.
Confidential	Client contracts, proposals, financial records, source code, system designs, staff records	Must be shared only with authorised people, stored in Chwezi-approved systems and encrypted in transit.
Restricted	Client production data, personal data, passwords and keys, security assessment findings, backups	Must be encrypted at rest and in transit, accessed only by named people with a current need, and never copied to personal devices or personal accounts.

7.2 Information that has not been labelled must be handled as Confidential.

7.3 Personnel must not paste Confidential or Restricted information, including client data and source code, into public artificial-intelligence tools, file-sharing sites or messaging groups that Chwezi has not approved for that purpose.

7.4 Personnel must dispose of Confidential and Restricted information securely: paper by shredding, and storage media by secure erasure or physical destruction, with the disposal recorded.

8. People security

8.1 Before granting access to Restricted information, Chwezi must verify the identity and references of the new staff member or contractor, to the extent the law permits.

8.2 Every staff member and contractor must sign a confidentiality agreement before receiving access to Confidential or Restricted information. The obligation continues after the engagement ends.

8.3 Every staff member and contractor must complete security and data protection awareness training within their first month and at least once every year after that. The Information Security Lead must keep a training record.

8.4 When a person leaves Chwezi or changes role, their manager must notify the Information Security Lead by their last working day. The Information Security Lead must remove all access the person no longer needs within one working day, and the person must return company devices and information.

9. Acceptable use

9.1 Personnel may use Chwezi systems for work purposes and for limited personal use that does not breach this policy or the law.

9.2 Personnel must not:

- share passwords, authenticator devices or accounts;
- attempt to access systems, data or accounts they have not been authorised to use;
- install unlicensed software or disable security software on work devices;
- connect work devices holding Restricted information to untrusted networks without the approved VPN or an encrypted connection;
- use Chwezi systems to harass, defame or infringe the rights of others, or for any act that is an offence under the Computer Misuse Act, 2011 or other applicable law.

9.3 Chwezi may monitor its own systems and accounts for security purposes. Monitoring is limited to what is needed to protect systems and data and is carried out in line with the Data Protection and Privacy Policy.

10. Access control and authentication

10.1 System owners must grant access on a need-to-know basis, through named individual accounts.

Personnel must not use shared accounts except where a system technically requires one; in that case the system owner must hold its credentials in the password manager and log its use.

10.2 The system owner must approve and record each grant of access to a production system, client system or code repository.

10.3 Systems administrators must enable MFA on email, code repositories, cloud and hosting control panels, password managers, remote access and every account with privileged access.

10.4 Personnel must use passwords of at least 12 characters, unique to each system, stored only in the Chwezi-approved password manager, and must change a password immediately if they suspect it has been compromised.

10.5 Administrators must use a separate privileged account, or a time-limited elevation, for administrative tasks; they must not use privileged accounts for email or web browsing.

10.6 Systems administrators must use SSH keys or an equivalent certificate-based method for server access, and must disable password login for server administration on production servers.

10.7 The Information Security Lead must review access rights to production systems, cloud accounts and code repositories at least every three months, and remove access no longer needed.

10.8 Engineering leads must make sure the software products we host provide role-based access control, session time-outs and audit trails, so that each client can enforce least privilege within its own organisation.

11. Cryptography

11.1 Systems administrators must configure every Chwezi system to encrypt data sent over public networks using TLS 1.2 or higher, and every website and application we host to redirect plain HTTP to HTTPS.

11.2 Systems administrators must encrypt Restricted information at rest, including client production databases and backups, using AES-256 or an equivalent current algorithm, through disk, volume or database encryption.

11.3 Every work laptop must have full-disk encryption enabled before it is used for Chwezi work.

11.4 Encryption keys, API secrets and certificates must be stored in the password manager or a dedicated secrets store, never in source code or shared documents. Access to them must be limited to the people who operate the system.

11.5 Systems administrators must renew certificates before expiry and must use automated renewal where the platform supports it.

12. Hosting, infrastructure and network security

12.1 Chwezi hosts its systems and websites with established data-centre and cloud providers. Some of our systems and websites are hosted on servers located in the **United States of America, Finland and Germany**. The Information Security Lead must keep a record of which system is hosted in which country and by which provider, and must give it to a client on request for that client's systems.

12.2 Chwezi must select hosting providers that operate physically secured data centres with controlled entry, power and cooling resilience, and that publish independent security attestations (such as ISO/IEC 27001 certification or SOC 2 reports).

12.3 Where a client contract requires its data to be hosted in a particular country or region, Chwezi must host that client's data there and must not move it without the client's written agreement.

12.4 Systems administrators must harden every production server before go-live: unused services disabled, default credentials removed, a host firewall enabled with only required ports open, and administrative interfaces restricted to approved addresses or the VPN.

12.5 Engineering leads must keep production, staging and development environments separate. Personnel must not copy live client personal data to development or test environments unless it has been anonymised or the client has agreed in writing.

12.6 Systems administrators must not expose database servers directly to the public internet.

12.7 Systems administrators must run malware protection or file-integrity monitoring on production servers, and must enable rate limiting or blocking of repeated failed sign-in attempts on internet-facing services.

12.8 Systems administrators must protect Chwezi email domains with SPF, DKIM and DMARC records, and must keep spam and phishing filtering enabled on company mailboxes. Personnel must report suspected phishing messages to the Information Security Lead and must not open their links or attachments.

13. Secure software development

- 13.1 Every software project must record its security requirements, including authentication, authorisation, data protection and logging needs, before development starts.
- 13.2 Developers must follow secure coding practice that addresses the OWASP Top 10 risks, including parameterised database queries, output encoding, server-side input validation and secure session handling.
- 13.3 Developers must keep all source code in Chwezi-controlled repositories with MFA enforced. A second developer or the engineering lead must review every change before it is merged into a production branch; an emergency fix may be released first, but must be reviewed within two working days after release.
- 13.4 Developers must not commit secrets to repositories. If a secret is committed, the developer must report it, and the system owner must revoke and replace it at once; removing it from history alone is not enough.
- 13.5 Developers must check third-party libraries and dependencies for known vulnerabilities before each release, and at least monthly for systems in production.
- 13.6 The engineering lead must approve every release to production, and the release must be deployed through a repeatable process that can be rolled back. A developer must not approve their own change for release; where the team is too small to separate the roles, the Founder and Chief Technology Officer must review the release record.
- 13.7 The engineering lead must have every major new release of a hosted product, and any system processing payment or health information, security-tested before go-live, through code review and vulnerability scanning at minimum.

14. Vulnerability and patch management

- 14.1 Systems administrators must apply security updates to operating systems, web servers, databases and application frameworks on the following timetable, counted from the date a fix is available:

Severity	Deadline
Critical, or actively exploited	7 days
High	30 days
Medium and low	Next scheduled maintenance, and within 90 days

- 14.2 If a patch cannot be applied in time, the system owner must record the reason and apply a compensating control, and the Information Security Lead must approve the delay.
- 14.3 The Information Security Lead must have internet-facing systems vulnerability-scanned at least every three months and after major changes.
- 14.4 The Information Security Lead must arrange a penetration test of each hosted product that holds client personal data at least once a year and after major architectural changes. The tester must not be a developer of the product under test. High and critical findings must be fixed within the deadlines in section 14.1.

14.5 Any person may report in good faith a vulnerability found in a Chwezi system through info@chwezicore.com. The Information Security Lead must acknowledge the report within 5 working days and record its assessment.

15. Logging and monitoring

15.1 Systems administrators must configure production systems to log authentication events, privileged actions, changes to security settings and application errors. Engineering leads must make sure hosted products keep an audit trail of significant user actions on business records.

15.2 Systems administrators must protect logs from alteration and keep them for at least 12 months, unless a client contract or the law requires a different period.

15.3 Systems administrators must monitor production systems for availability, failed sign-in patterns and unusual activity, with alerts sent to the responsible administrator.

15.4 Systems administrators must synchronise system clocks to a reliable time source so that logs can be correlated.

16. Backup, business continuity and disaster recovery

16.1 Systems administrators must back up production databases and client data at least daily, encrypt the backups, and store them in a different data centre from the primary server.

16.2 Systems administrators must retain backups for at least 30 days, unless a client contract specifies a different period.

16.3 Systems administrators must test restoration from backup at least every three months, for at least one production system on rotation, and record the result.

16.4 The Information Security Lead must maintain a disaster recovery plan for each hosted product that states the recovery steps, responsible people and the recovery time and recovery point agreed with clients.

16.5 Chwezi must keep source code, infrastructure configuration and documentation in a form that allows a production system to be rebuilt on a different provider if the primary provider fails.

17. Endpoints, mobile devices and remote working

17.1 Personnel must make sure that every work laptop and phone that accesses Confidential or Restricted information has a screen lock, full-device encryption, current security updates and, for laptops, active anti-malware protection.

17.2 Personnel may use a personal phone for work email and messaging only if it has a screen lock and current updates, and only through apps that Chwezi can sign out remotely.

17.3 Personnel must report a lost or stolen device to the Information Security Lead immediately, so that sessions can be revoked and the device wiped where possible.

17.4 When working remotely or in public places, personnel must lock unattended devices and take reasonable care that screens and conversations cannot be overseen or overheard.

18. Physical security

18.1 The last person to leave a Chwezi office must lock it. Staff must accompany visitors in areas where Confidential information is handled.

18.2 Personnel must keep paper documents and removable media holding Confidential or Restricted information in locked storage when not in use.

18.3 Chwezi does not operate its own data centre. Physical security of servers is provided by the hosting providers selected under section 12.2.

19. Suppliers and third parties

19.1 Before a supplier is given access to Confidential or Restricted information or to production systems, the Information Security Lead must assess its security controls and the location of its processing.

19.2 The Founder and Chief Technology Officer must not sign a contract with such a supplier unless it includes confidentiality, security and breach notification obligations, and data processing terms where personal data is involved.

19.3 The system owner must limit supplier access to what the service needs, grant it through named accounts, and remove it when the service ends.

20. Incident management

20.1 Every person must report a suspected security incident to the Information Security Lead immediately, by phone on +256 784 464178 or by email to info@chwezicore.com with the subject line "SECURITY INCIDENT". Personnel must not investigate beyond what is needed to contain the incident, and must not delete evidence.

20.2 The Information Security Lead must lead the response through these stages: identify, contain, eradicate, recover and review, keeping a written incident record of times, actions and decisions.

20.3 Where an incident affects a client's system or data, Chwezi must notify the client's designated contact without undue delay, and in any event within 72 hours of confirming the incident, unless the client contract sets a shorter period. Chwezi must give the client the information it needs to meet its own legal obligations.

20.4 Where an incident is a personal data breach, the Data Protection Officer must handle notification to the Personal Data Protection Office and to affected individuals as set out in the Data Protection and Privacy Policy (CCS-POL-DPP-02).

20.5 After every significant incident, the Information Security Lead must hold a review within 10 working days, record the root cause, and track corrective actions to completion.

21. Client engagements and on-site work

21.1 Personnel must perform cybersecurity assessments, vulnerability scans and penetration tests on client systems only under a written authorisation from the client that defines the scope, timing and contacts. Testers must stay within that scope.

21.2 Findings from security assessments are Restricted information. The engagement manager must share them only with the client's authorised contacts and must delete or return them at the end of the engagement, unless the client agrees otherwise in writing.

21.3 For CCTV, access-control and intruder-detection installations, installers must change default passwords before handover, give the client sole control of administrator credentials, and must not keep remote access after handover unless the client has agreed to it in a support contract.

21.4 Personnel working on client premises or in client systems must follow the client's own security rules in addition to this policy.

22. Compliance, exceptions and breach of policy

22.1 Chwezi must comply with the laws that apply to its information processing, including the Data Protection and Privacy Act, 2019 and the Computer Misuse Act, 2011 of Uganda, and the laws of other countries where we serve clients or host data, to the extent they apply.

22.2 An exception to this policy may be granted only by the Founder and Chief Technology Officer, in writing, for a defined period, with the risk and any compensating control recorded in the risk register.

22.3 Suspected breaches of this policy must be reported to the Information Security Lead. The Information Security Lead investigates; the Founder and Chief Technology Officer decides on the outcome. A breach by a staff member may lead to disciplinary action up to dismissal; a breach by a contractor or supplier may lead to termination of the contract. Breaches that may be criminal may be reported to the authorities.

23. Monitoring, review and related documents

23.1 The Information Security Lead must report to the Founder and Chief Technology Officer at least every three months on incidents, access review results, patch compliance, backup test results and open risks.

23.2 The Information Security Lead must review this policy at least once a year, and earlier after a significant incident, a change in law or a major change in our systems or hosting.

23.3 The Information Security Lead must keep the risk register, asset inventory, access review records, training records, incident records, backup test results and exception approvals for at least three years, in Chwezi's controlled document store.

23.4 Related documents:

- Data Protection and Privacy Policy (CCS-POL-DPP-02);
- Terms of Service, published at chwezicore.com;
- client contracts and data processing agreements, which may add client-specific requirements.

24. Review and approval history

Version	Date	Author	Approved by	Change	Next review
1.0	27 October 2026	Information Security Lead	Peter Bamuhigire, Founder and Chief Technology Officer	First approved issue	October 2027

Approved for and on behalf of Chwezi Core Systems Limited

Peter Bamuhigire, Founder and Chief Technology Officer — 27 October 2026