



Labl Fashion

RESPONSIBLE FASHION • DIGITAL EVIDENCE • MARKET ACCESS

www.lablfashion.co.ke • info@lablfashion.co.ke

CONTROLLED OPERATIONAL MANUAL

Digital System, Data, AI, GIS and Cybersecurity Manual

Govern LaDOS, digital records, AI-supported operations, GIS/weather data, integrations, cybersecurity and controlled interoperability with AfriEuro Links and CEOS.

Document control	Approved treatment
Document code	LF-MAN-07
Owner	Managing Director / designated manual owner
Version	1.0
Effective date	Upon Board/management approval
Review	Annual and after material legal, operational, incident or strategy change
Classification	Controlled internal and approved partner-use document

Labl Fashion LTD | Registration PVT-3QU23XV | Prepared July 2026

1. Purpose, scope and authority

Govern LaDOS, digital records, AI-supported operations, GIS/weather data, integrations, cybersecurity and controlled interoperability with AfriEuro Links and CEOS.

SCOPE Applies to all Labl Fashion information systems, devices, users, data, AI use cases, geospatial layers, weather feeds, APIs, cloud/services, payment interfaces and third-party processors.

This manual supports the Labl Fashion Strategic Plan and Comprehensive Business Plan 2027–2030. It does not replace applicable Kenyan law, binding customer/partner requirements, professional advice or a more stringent approved control. Where requirements conflict, work must pause and the manual owner must obtain an authorised decision.

2. Governing principles

- LaDOS is independent and fashion-specific; interoperability does not merge accountability.
- Collect and share the minimum data required for a defined lawful purpose.
- AI supports people; it does not autonomously decide employment, credit, compliance, product release or claims.
- Location, worker, customer design and community knowledge receive risk-based protection.
- Essential operations retain tested manual fallback and recovery.

3. Roles and accountability

Role	Core accountability
Board/MD	Approve risk appetite, material systems, high-risk use cases and major incidents.
System owner	Own value, users, availability, controls, roadmap and vendor performance.
Data owner/steward	Define fields, quality, access, lawful use, retention and evidence status.
Security lead	Manage risk, identity, vulnerabilities, monitoring, incident and recovery.
AI use-case owner	Document purpose, data, model, performance, human review and limitations.
GIS/weather owner	Control sources, accuracy, sensitivity, use and attribution.
Users	Protect credentials/devices, use authorised tools and report abnormal activity.
AfriEuro/CEOS interface owner	Approve minimum exchange, contracts, logs and revocation.

4. Standard operating procedure

The following sequence is the minimum controlled workflow. The owner may add risk-based checks, but may not omit a required approval, evidence or safeguard without an authorised exception.

4.1 Inventory and classify

Register systems, data, devices, interfaces, owners, sensitivity and criticality.

4.2 Access lifecycle

Request, approve, provision, review, change and revoke least-privilege access.

4.3 Change and release

Define requirement, test, security/privacy review, approve, deploy, monitor and rollback.

4.4 AI governance

Register use case, risk assess, test, approve, human review, monitor drift and retire.

4.5 GIS/weather governance

Approve source/licence, quality flag, timestamp, sensitivity, display and decision use.

4.6 Interoperability

Define purpose, fields, API/security, controller roles, retention, incidents and exit.

4.7 Incident response

Detect, contain, assess, preserve evidence, notify, recover, learn and correct.

4.8 Continuity

Backup, restore test, provider fallback, offline procedure and recovery priority.

5. Control matrix

Control point	Required control
Identity and access	Unique accounts, MFA where appropriate, role-based permissions and periodic review.
Customer design/IP	Approved repository, restricted sharing, contractual use and no unauthorised model training.
AI prohibition	No autonomous hiring/dismissal, wage, supplier exclusion, credit, compliance, release or claim decision.
GIS sensitivity	Aggregate vulnerable households and protect sensitive cultural/environmental sites.
Weather quality	Source, time, coverage, missing/late flag and no treatment of

Control point	Required control
	forecast as certainty.
API/interface	Authentication, encryption, field minimisation, logging, rate/error handling and revocation.
Payment integration	Licensed provider, tokenised/secure handling, reconciliation and no unlicensed custody.
Backup/recovery	Defined recovery objectives, protected copies and documented restoration tests.

6. Exceptions, incidents and escalation

1. Stop or contain any condition that presents immediate danger, illegality, serious harm, uncontrolled loss, material product risk or unauthorised disclosure.
2. Notify the supervisor/manual owner promptly; preserve people, physical and digital evidence without obstructing urgent care or legal duties.
3. Classify the event, assign an owner, document immediate correction and determine customer, worker, community, regulator, insurer, funder or Board notification.
4. Investigate proportionately, identify contributing and systemic causes, approve corrective/preventive action and verify effectiveness before closure.
5. Record authorised deviations with reason, scope, duration, compensating controls and expiry; repeated exceptions require system change or escalation.

7. Records and evidence

Records must be accurate, dated, attributable, legible, protected, retrievable and retained under the approved retention schedule. Personal, customer, community, financial, research and security information receives access proportionate to risk.

Required record	Minimum evidence expectation
System/data/interface register	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
Access request and review	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
Change and release record	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
AI use-case register	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
Model test/override/incident log	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
GIS/weather source register	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
Processor/vendor due diligence	Owner, date/period, subject, decision/status, source or attachment,

Required record	Minimum evidence expectation
	approval where required and retention location.
Security incident file	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.
Backup and recovery test	Owner, date/period, subject, decision/status, source or attachment, approval where required and retention location.

8. Performance indicators and management review

Indicator	Review question
System availability	What does system availability show about effectiveness, risk, trend, root cause and required decision?
Access reviews completed	What does access reviews completed show about effectiveness, risk, trend, root cause and required decision?
Data-quality exceptions	What does data-quality exceptions show about effectiveness, risk, trend, root cause and required decision?
Security incidents and response time	What does security incidents and response time show about effectiveness, risk, trend, root cause and required decision?
Approved AI use cases/overrides	What does approved ai use cases/overrides show about effectiveness, risk, trend, root cause and required decision?
GIS/weather feed quality	What does gis/weather feed quality show about effectiveness, risk, trend, root cause and required decision?
Interface failures	What does interface failures show about effectiveness, risk, trend, root cause and required decision?
Recovery tests passed	What does recovery tests passed show about effectiveness, risk, trend, root cause and required decision?
User training completion	What does user training completion show about effectiveness, risk, trend, root cause and required decision?

The manual owner reviews indicators monthly or quarterly according to risk, reports material exceptions through the management pack and proposes changes during annual management review. A positive metric never overrides evidence of harm, legal breach or stakeholder grievance.

9. Competence, communication and training

- Identify roles that require induction, supervised practice, formal qualification, refresher training or independent authorisation.
- Assess competence through observed performance, records, tests, work results or authorised sign-off—not attendance alone.
- Communicate changes before their effective date and confirm affected users can access the current controlled version.

- Withdraw access or require supervision where competence has expired, changed or proved insufficient.
- Retain training, assessment, authorisation and refresher records.

10. Review, change and approval

Trigger	Required action
Annual review	Confirm continued suitability, legal/contractual alignment, evidence, indicators, incidents and user feedback.
Material incident or audit finding	Review affected control immediately and implement approved corrective change.
Legal, market or system change	Obtain competent review before the new requirement or release becomes effective.
Process/organisation change	Update roles, records, training, permissions and continuity arrangements.
Manual revision	Issue new version, change summary, approval, effective date and superseded-version withdrawal.

Appendix A — Operational templates

The following templates form the minimum annex set. The manual owner may issue controlled electronic equivalents in LaDOS or another approved system.

A.1 System change request

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.2 Access request/review

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.

Field	Required entry
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.3 AI use-case assessment

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.4 GIS/weather source assessment

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.5 Interface data contract

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.

Field	Required entry
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.6 Security incident form

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

A.7 Backup/restore test

Field	Required entry
Reference and date	Unique number, date/time and related customer/project/order/partner/person as applicable.
Owner and participants	Responsible owner, contributors, reviewer and approval authority.
Facts/evidence	Objective information, source, attachments, system references and limitations.
Decision/action	Decision, conditions, immediate control, actions, due dates and status.
Verification/closure	Verifier, effectiveness evidence, closure date and residual issue.

Appendix B — Approval

This manual becomes controlled when approved by the authorised Labl Fashion authority. Printed copies are uncontrolled unless specifically registered.

Approved by	Capacity	Signature	Date
	Board Chair / delegated authority		
	Managing Director / Venture Lead		
	Manual owner		