Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

Procurement Pack

Version 1.0 · April 2026

Field	Value
Document	Procurement Pack
Version	1.0
Effective date	April 2026
Document reference	PP-2026-01
Prepared by	Innov8ProTech Ltd
Contact	hello@innov8protech.com

About this pack

This pack contains the documents required by public sector and enterprise procurement teams considering Innov8ProTech Ltd as a software supplier.

Contents

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

How to use this pack

All sections are self-contained and can be extracted for tender submissions. An editable DOCX version is available on request. A signed PDF copy is available on request for tender annexes.

1. Company Information

Legal entity

Field	Value
Registered name	Innov8ProTech Ltd
Trading name	Innov8ProTech
Jurisdiction	Republic of Ghana
Registration number	CS201451224
Date of incorporation	10 December 2024
TIN	C0064889467 (Ghana Revenue Authority)
VAT registration	C0064889467

Registered office

Field	Value
Street	St. Mark Street, Com 18
City	Tema
Region	Greater Accra
Country	Ghana

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

Contacts

Purpose	Contact
General enquiries	hello@innov8protech.com
Data protection	privacy@innov8protech.com
Support	support@innov8protech.com
Phone	+233 20 683 6529
Secondary phone	+233 24 043 1751

Nature of business

Innov8ProTech Ltd designs, builds, and operates custom software for public sector agencies, financial institutions, and enterprises in Ghana and West Africa. Our work spans core banking, health information systems, government recruitment platforms, portals, and AgriTech telematics.

Key personnel

Name	Role	Background
Pious Brinton Apandago	Founder & Managing Director	12+ years engineering leadership, public sector delivery
Tangwam Moses	Head of Engineering	Platform architecture, security, and performance
Emmanuel Arthur	Head of Delivery	Government stakeholder management, project governance
Angela Owusu Aboagye	Head of Operations	Rollout, training, and ongoing support

Full profiles available on request or at innov8protech.com/company/team.

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

Banking

Field	Value
Bank	Guaranty Trust Bank (Ghana) Ltd
Branch	Ring Road
Account number	219141286110
SWIFT / BIC	GTBIGHAC

Insurance

Innov8ProTech is in the process of arranging insurance appropriate to the scale of public sector engagements. Confirmation of coverage at the time of contract is provided on request and reflected in the signed Master Service Agreement.

Where an agency requires specific coverage levels as a condition of award, we will arrange those before contract signature.

Certifications

We do not currently hold ISO 27001 certification. Our security practice is aligned to ISO 27001 controls and to the requirements of Ghana's Data Protection Act 843. Independent penetration testing is conducted annually.

References

Three named client references are available on request, with the client's permission. We do not provide anonymous references.

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

2. Data Protection Act 843 Compliance Statement

Overview

Innov8ProTech Ltd is committed to handling personal data lawfully, transparently, and securely, in line with Ghana's Data Protection Act, 2012 (Act 843) and, where applicable, the EU General Data Protection Regulation (GDPR).

This statement sets out how we meet the obligations that apply to us as both a **data controller** (for our own website, marketing, and recruitment) and a **data processor** (for personal data inside systems we build or operate on behalf of clients).

Registration

Registration with the Data Protection Commission of Ghana is in progress. Innov8ProTech operates in alignment with Act 843 in the interim, and the registration certificate will be provided as soon as it is issued.

Where an agency requires the certificate before contract signature, we will confirm timeline on request.

Principles

We apply the following principles to all personal data we handle:

1. **Lawfulness, fairness, transparency** — we only process data where we have a lawful basis, and we say so clearly.
2. **Purpose limitation** — we collect data for specific, explicit purposes, not for vague or future undefined use.
3. **Data minimisation** — we collect the smallest amount of data needed to do the job.
4. **Accuracy** — we take reasonable steps to keep personal data accurate and up to date.
5. **Storage limitation** — we retain data only as long as necessary, then delete or anonymise it.
6. **Integrity and confidentiality** — we protect data with appropriate technical and organisational measures.
7. **Accountability** — we can demonstrate compliance through records, policies, and audits.

Data subject rights

We support all rights granted under Act 843 and, where applicable, GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making

Requests can be sent to **privacy@innov8protech.com**. We respond within 30 days.

Security measures

- **Encryption in transit:** TLS 1.3 for all network traffic
- **Encryption at rest:** AES-256 for databases and file storage
- **Access control:** role-based, least privilege, with quarterly access reviews
- **Authentication:** two-factor authentication required for all internal systems
- **Logging:** administrative access is logged and reviewed
- **Backups:** encrypted, tested quarterly, stored separately from production
- **Vulnerability management:** dependency scanning and regular patching
- **Staff:** annual data protection training and confidentiality obligations

Data breach notification

In the event of a personal data breach likely to result in a risk to data subjects, we will:

1. Contain the breach immediately, within the P1 response window
2. Assess scope, severity, and impact within 24 hours
3. Notify affected individuals and the Data Protection Commission within 72 hours where required
4. Notify the client's designated contact within 24 hours where the breach involves client project data
5. Provide a full written post-incident report within 5 business days

International transfers

Where personal data is transferred outside Ghana, we ensure the transfer is lawful by one of:

- Transfer to a jurisdiction recognised as providing adequate protection
- Standard contractual clauses or equivalent safeguards in the provider agreement
- Storing data inside the client's own region or on-premises where required

For client project data, the storage region is chosen by the client at contract stage. We do not move client data between regions without written instruction.

Subprocessors

A current list of subprocessors is maintained on our website at innov8protech.com/privacy. Active clients are notified at least 30 days before any material change.

Data Processing Agreement

For any engagement where we process personal data on behalf of a client, we sign a Data Processing Agreement (DPA) before processing begins. Our standard DPA is available on request and covers:

- Scope and purpose of processing
- Categories of data and data subjects
- Client instructions and lawful basis
- Confidentiality and security obligations
- Subprocessor management
- Assistance with data subject rights
- Breach notification
- Return or deletion of data on termination
- Audit and inspection rights

Contact

Data protection contact: privacy@innov8protech.com **Postal address:** Innov8ProTech Ltd, St. Mark Street, Com 18, Tema, Ghana **Regulator:** Data Protection Commission of Ghana · dataprotection.org.gh

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

3. Security Questionnaire

Pre-filled responses to the standard questions asked by public sector and enterprise procurement teams. Where a question does not apply, this is stated explicitly rather than left blank.

Governance and policy

Do you have a written information security policy? Yes. Reviewed annually, approved by the Managing Director, acknowledged by all staff at onboarding and annually thereafter.

Do you have a named individual responsible for information security? Yes. The Head of Engineering is the designated security owner. The Managing Director is accountable at board level.

Do you conduct background checks on staff with access to client data? Yes. All staff undergo identity verification (GhanaCard), reference checks, and police clearance before onboarding.

Do you provide security awareness training? Yes. All staff complete annual data protection and security awareness training, with quarterly phishing simulations.

Access control

How do you control access to systems containing personal data? Role-based access control (RBAC) with least privilege. Access is provisioned on a documented request, reviewed quarterly, and revoked within 4 hours of a staff member leaving.

Is multi-factor authentication enforced? Yes. MFA is required for all internal systems, administrative consoles, and source code repositories.

How are privileged accounts managed? Privileged accounts are separately issued, logged, and subject to a just-in-time access request process. Session recordings are retained for 90 days.

How often is access reviewed? Quarterly, with the review documented and signed off by the security owner.

Data protection

What encryption is used at rest? AES-256 for databases and object storage. Keys are managed via a dedicated key management service and rotated annually.

What encryption is used in transit? TLS 1.3 for all external traffic. TLS 1.2 minimum for internal service-to-service communication.

How is backup data protected? Backups are encrypted with the same standard, stored in a separate region from production, and tested for restore quarterly.

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

How long are backups retained? 30 days rolling.

Network and infrastructure

Where is client data hosted? At the client's choice of:

- Azure South Africa North (Johannesburg)
- AWS Africa (Cape Town)
- On-premises at the client's designated facility
- A Ghana-based colocation facility

Do you use a cloud provider with recognised certifications? Yes. Our cloud infrastructure runs on Microsoft Azure and Amazon Web Services, both of which hold ISO 27001, SOC 2 Type II, and CSA STAR attestations.

How is the network segmented? Production, staging, and development environments are fully separated, with no shared credentials or data. Production access requires a VPN and MFA.

How is DDoS protection provided? Via our edge provider (Cloudflare), which also handles TLS termination and web application firewall rules.

Application security

Do you follow a secure development lifecycle? Yes. All code is peer reviewed before merge, dependency scanning runs on every commit, and static analysis runs nightly.

How often do you patch? Critical security patches within 72 hours of availability. High-severity patches within 7 days. Standard patches on a monthly cycle.

Do you conduct penetration testing? Yes. Independent third-party penetration testing is conducted annually on production systems. Reports are available to clients under NDA.

How are secrets and credentials managed? Secrets are stored in a dedicated secret manager, never in source code or environment files committed to version control. Rotation is enforced at least annually.

Incident response

Do you have a documented incident response plan? Yes. Covers detection, classification, containment, eradication, recovery, and post-incident review.

What is your breach notification window?

- Affected individuals: without undue delay, where possible within 72 hours of assessment

- Data Protection Commission of Ghana: within 72 hours where required
- Client's designated contact: within 24 hours where client data is involved

Do you have cyber insurance? Insurance arrangements appropriate to the scale of our engagements are in progress. Confirmation of coverage at the time of contract is available on request. Where a specific coverage level is required for award, we arrange it before contract signature.

Business continuity

Do you have a documented business continuity plan? Yes. Covers loss of key personnel, loss of primary infrastructure, and major supplier failure.

What is your Recovery Time Objective (RTO)? 4 hours for critical systems.

What is your Recovery Point Objective (RPO)? 1 hour for transactional data, 24 hours for non-transactional data.

Our first formal disaster recovery test is scheduled and will be completed before our first production deployment for a public sector client. Test results will be shared with the client as part of onboarding.

Compliance and audit

Are you ISO 27001 certified? Not currently. Our security practice is aligned to ISO 27001 controls, and we are working towards formal certification.

Do you undergo SOC 2 audits? Not currently. We can complete a security questionnaire on request and support client-led audits.

Can clients audit your systems? Yes. Clients have the right to audit under our standard DPA, on reasonable notice and subject to confidentiality. We also support third-party audits on the client's behalf.

Do you have a whistleblowing policy? Yes. Anonymous reporting is available to all staff.

Personnel

How is staff access to client data revoked when someone leaves? All access is revoked within 4 hours. Devices are returned, wiped, and certified. This is documented for every departure.

Do contractors have the same controls as employees? Yes. Contractors sign the same confidentiality agreements and are subject to the same access controls and training requirements.

How is data protection handled for remote work? Full-disk encryption is mandatory. Remote sessions run over a corporate VPN. Personal devices cannot access production systems.

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

4. Reference Architecture

Our standard deployment for a public sector platform uses a five-layer architecture. Each layer is independently deployable, testable, and observable. Components can be swapped without affecting the rest of the system.

Layer 1 — User access

How citizens, staff, and administrators reach the system.

- **Web browser** — responsive, WCAG 2.2 AA compliant, works on low-bandwidth connections
- **Mobile web** — the same application, optimised for small screens
- **USSD** — for feature phones and low-literacy users, via an aggregator such as Hubtel or Africa's Talking
- **Assisted channels** — for citizens who visit an office in person

Layer 2 — Edge

The first point of contact for all traffic.

- **CDN** — static assets served from edge nodes closest to the user
- **DDoS protection** — always-on mitigation at the edge
- **WAF** — web application firewall with OWASP ruleset
- **TLS termination** — HTTPS with modern ciphers only
- **Rate limiting** — per-IP and per-endpoint, with adaptive thresholds

Layer 3 — Application

The core platform.

- **Authentication and identity** — GhanaCard (NIA) integration, plus password and MFA
- **API gateway** — routing, authentication, rate limiting, request logging
- **Business logic services** — one service per bounded domain (applications, payments, verification, notifications)
- **Background workers** — asynchronous jobs, notifications, scheduled tasks, retries
- **Admin console** — role-based access for agency staff, with full audit logging

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

Layer 4 — Integration

Connections to external systems.

- **Identity** — NIA (GhanaCard), biometric verification providers
- **Payments** — MTN MoMo, Telecel Cash, AT Money, gh-link, GhIPSS Instant Pay, Stripe, Paystack
- **Government** — GRA, NHIA, GES, and other agency APIs where available
- **Enterprise** — ERP, accounting, HR, and payroll systems
- **Communication** — transactional email (Resend), SMS gateways, WhatsApp Business
- **Data** — weather, satellite, or other third-party data feeds where relevant

Every integration runs through an adapter that isolates our code from provider-specific quirks. Adding a new provider does not affect the rest of the system.

Layer 5 — Data

Where everything is stored.

- **PostgreSQL** — primary transactional database, with encryption at rest, point-in-time recovery, and daily backups
- **Redis** — caching and ephemeral state
- **Object storage** — documents, uploads, and media, encrypted with per-object keys
- **Audit log** — immutable, append-only, retained for the lifetime of the contract plus 7 years
- **Data warehouse** — for reporting and analytics, populated by scheduled ETL jobs from the operational store

Deployment topology

Cloud (default):

- Primary region: Azure South Africa North or AWS Africa (Cape Town)
- Backups: separate region within the same jurisdiction
- Multi-availability-zone deployment for production workloads
- Infrastructure defined as code (Terraform), version controlled, peer reviewed

On-premises:

- Same architecture, deployed on client-owned hardware
- Offline-tolerant: applications continue functioning during internet outages

- Local data storage with no external API calls for core functions
- Backup to a client-approved secondary location

Hybrid:

- Sensitive data on-premises, non-sensitive services in the cloud
- Data synchronisation via a documented interface, with audit trail

Observability

- **Metrics** — Prometheus, with dashboards in Grafana
- **Logs** — centralised, structured, searchable, retained 90 days
- **Traces** — distributed tracing via OpenTelemetry for critical paths
- **Uptime** — external HTTP probe from at least two independent regions, every 60 seconds
- **Alerts** — routed to on-call engineer, not a ticket queue

Security controls by layer

Layer	Key controls
User access	TLS 1.3, HSTS, secure cookies, CSP
Edge	DDoS mitigation, WAF, rate limiting, bot detection
Application	MFA, RBAC, session timeout, input validation, output encoding
Integration	Signed requests, allow-listed IPs where supported, retry with backoff, circuit breakers
Data	AES-256 at rest, per-object keys, access logs, encrypted backups

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

5. Accessibility Statement

Commitment

Innov8ProTech is committed to building digital services that everyone can use, including people with disabilities and people using older devices or slow connections. We aim to meet **WCAG 2.2 Level AA** on every public-facing system we deliver.

Standards we build to

- **WCAG 2.2 Level AA** — the recognised international standard for web accessibility, as referenced by the Web Accessibility Initiative and adopted by governments worldwide
- **Ghana's Disability Act, 2006 (Act 715)** — which requires public services to be accessible to persons with disabilities
- **Section 508** — where our clients serve US federal programmes

How we meet it

Perceivable

- Text alternatives for all non-text content, including images, icons, and charts
- Captions and transcripts for audio and video
- Colour contrast of at least 4.5:1 for body text and 3:1 for large text
- Text resizable to 200% without loss of content or function
- Content structured with proper headings, lists, and tables

Operable

- Full keyboard navigation — every interactive element is reachable and usable without a mouse
- Visible focus indicators on all focusable elements
- No content that flashes more than three times per second
- Ample time for time-limited interactions, with extensions available
- Multiple ways to find content — search, sitemap, breadcrumbs

Understandable

- Plain language throughout, avoiding jargon where possible
- Consistent navigation and layout across pages

- Clear error messages that explain what went wrong and how to fix it
- Labels and instructions for all form inputs
- Predictable behaviour — nothing happens automatically that the user didn't request

Robust

- Valid, semantic HTML
- ARIA landmarks and roles used correctly, not as a substitute for proper markup
- Tested with screen readers (NVDA, JAWS, VoiceOver, TalkBack)
- Compatible with browser zoom, text-only browsers, and assistive technologies

Beyond the standard

Where a public service must reach citizens who do not have smartphones, we provide:

- **USSD access** — for feature phones and low-literacy users, with a simple menu-driven interface
- **SMS confirmations** — so applicants are never left waiting for an email
- **Assisted channels** — a documented workflow for citizens who need to complete a process in person

How we test

Accessibility is tested at three points in every project:

1. **During design** — prototypes reviewed against WCAG checklists before development begins
2. **During development** — automated checks (axe, Lighthouse) on every pull request
3. **Before launch** — manual testing by a trained tester using a screen reader, keyboard only, and browser zoom
4. **After launch** — spot checks after every significant release, plus annual full audit

We also invite users with disabilities to test critical flows before launch, where the client is willing to facilitate this.

Known limitations

- Some legacy systems we integrate with do not meet the same standard. Where this affects a public-facing journey, we build an accessible wrapper around the legacy service.
- Complex data visualisations may not be fully accessible on very old browsers. Text alternatives are always provided.

We are not currently aware of any accessibility issue that blocks a critical user journey on systems we have delivered since 2024.

Feedback

If you encounter an accessibility barrier on a system we have built, contact us:

Email: hello@innov8protech.com **Subject line:** Accessibility issue

We will acknowledge within 2 business days and aim to resolve within 10 business days, or provide a documented workaround where a fix takes longer.

Formal complaints

If you are not satisfied with our response, you have the right to escalate to the client agency that owns the service, or to the National Council on Persons with Disability in Ghana.

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

6. Disaster Recovery and Business Continuity Summary

Objectives

Objective	Target	Notes
RTO (Recovery Time Objective)	4 hours	Critical systems restored to service
RPO (Recovery Point Objective)	1 hour	Maximum tolerable data loss for transactional data
RPO (non-transactional)	24 hours	Documents, reports, and other non-critical data
Backup retention	30 days rolling	Encrypted, off-site, tested quarterly
DR test frequency	Quarterly	Full restore test with documented results

Failure scenarios covered

Loss of primary infrastructure

- **Detection:** automated health checks every 60 seconds; alert to on-call engineer within 2 minutes
- **Response:** failover to standby infrastructure in the same jurisdiction
- **Client impact:** 15–30 minutes of degraded service during cutover for most workloads
- **Data impact:** none, if the standby region is current

Loss of a single availability zone

- **Detection:** cloud provider alerts and our own health checks
- **Response:** automatic failover by the platform; no manual action required
- **Client impact:** none visible to end users
- **Data impact:** none

Loss of primary database

- **Detection:** application errors and health checks
- **Response:** promote the standby replica to primary; application reconnects automatically
- **Client impact:** 5–15 minutes of failed reads and writes

- **Data impact:** up to 1 hour of transactions replayed from write-ahead logs; typically seconds

Ransomware or destructive attack

- **Detection:** file integrity monitoring and anomaly detection
- **Response:** isolate affected systems, restore from the most recent clean backup
- **Client impact:** hours to a full day depending on scope
- **Data impact:** bounded by the backup window, typically under 24 hours

Loss of key personnel

- **Detection:** operational — documented in the team's daily standup
- **Response:** defined deputy for every critical role; runbooks for every recurring task
- **Client impact:** none for routine operations; new feature work may slow
- **Data impact:** none

Loss of a critical supplier

- **Detection:** supplier status page monitoring and our own alerting
- **Response:** documented failover to an alternative supplier for email, SMS, and payments
- **Client impact:** minimal if failover is clean; possible duplicate notifications during cutover
- **Data impact:** none

Backups

- **Frequency:** continuous write-ahead logging, plus full daily snapshots
- **Storage:** encrypted with AES-256, stored in a separate region from production
- **Immutability:** backups are write-once, read-many for the retention window; they cannot be deleted by a compromised production account
- **Retention:** 30 days rolling for daily snapshots; 12 months for monthly archives
- **Restore testing:** quarterly, with results documented and available to clients on request

Communication during an incident

- **Internal:** on-call engineer paged within 2 minutes; escalation if no acknowledgment within 15 minutes
- **Client notification:** P1 incidents notified within the SLA response window; status updates every 60 minutes

- **Post-incident:** full written report within 5 business days, including timeline, root cause, and preventive measures

Recovery validation

Every DR test produces a written report covering:

- Scenario tested
- Time to detection
- Time to recovery
- Data loss (if any)
- Issues discovered
- Corrective actions

Reports are available to active clients on request.

Exclusions

The following are outside the scope of this DR plan and are handled under separate agreements:

- Complete loss of the client's own network or infrastructure
- Force majeure events affecting an entire region or country
- Loss of third-party services that have no viable alternative (for example, a national ID system outage)

For these cases, we coordinate with the client and any relevant third parties, and communicate status as information becomes available.

Contact during a declared disaster

Primary: support@innov8protech.com **Escalation:** Head of Engineering (phone provided at contract) **Executive:** Founder & Managing Director (phone provided at contract)

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

7. Sample Statement of Work

This is an illustrative Statement of Work for a typical portal project. It shows the structure, level of detail, and specificity we use in real engagements. A real SOW is scoped to your specific requirements.

Statement of Work

Project: [Agency name] Recruitment Portal **Client:** [Agency name] **Supplier:** Innov8ProTech Ltd **Effective date:** [Date] **Version:** 1.0

1. Background

[Agency name] currently manages recruitment through a paper-based process. Applications are received in person and by post, and shortlisting is manual. The agency intends to move to a digital recruitment portal that reduces processing time, improves candidate experience, and produces a full audit trail.

2. Scope

Innov8ProTech will design, build, and deploy a recruitment portal with the following components:

Candidate portal

- Public vacancy listing with search and filters by category, region, and qualification
- Online application form with document upload
- GhanaCard identity verification
- Mobile Money payment of application fees
- Application status tracking with SMS and email notifications
- USSD fallback for feature phone users

HR dashboard

- Centralised view of all open vacancies and applicant pools
- Bulk shortlisting with eligibility rules
- Verification queue with manual override
- Interview scheduling with notifications
- Assessment scoring and ranking
- Full audit log of every action

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

Infrastructure and integrations

- Integration with NIA (GhanaCard) for identity verification
- Integration with MTN MoMo, Telecel Cash, and AT Money for fee collection
- Deployment to [Azure South Africa North / AWS Cape Town / on-premises]
- Automated backups and monitoring

3. Out of scope

- Physical fingerprint capture devices
- Background check services from third parties
- Integration with [legacy HR system] — available as a change order
- Custom reporting beyond the standard dashboard
- Training of individual applicants

4. Deliverables and milestones

#	Deliverable	Acceptance criteria	Target date	Payment
1	Discovery and design	Signed-off wireframes and data model	Week 3	20%
2	Candidate portal (staging)	All candidate flows tested and demoed	Week 7	25%
3	HR dashboard (staging)	All HR flows tested and demoed	Week 10	25%
4	Integration complete	NIA, MoMo, and SMS live in staging	Week 12	15%
5	Production launch	Live in production, staff trained	Week 14	15%

5. Timeline

Total duration: 14 weeks from kickoff, assuming timely client input and integration access.

Key client dependencies:

- NIA API access credentials within 2 weeks of kickoff
- Approval of candidate-facing content within 1 week of receiving drafts
- UAT feedback within 5 business days of each demo

6. Assumptions

- The client provides one named project owner with authority to make decisions

- The client provides access to NIA, MoMo, and SMS aggregator sandbox accounts
- Volume during the pilot is under 100,000 applications
- Concurrent users during peak application periods do not exceed 5,000

7. Change management

Any change to scope after sign-off will be documented in a written change order with impact on cost, timeline, and deliverables. Change orders are approved by both parties before work begins. Small changes (under 8 hours) are absorbed within the sprint, at the supplier's discretion.

8. Acceptance

Each deliverable is tested by the client within 5 business days of handover. Acceptance is deemed given if no material defect is reported within that window. A material defect is one that prevents a defined core function from operating.

9. Fees and payment

Total fee: GH₵ [amount], fixed price.

Payment schedule: as per milestones above. Invoices raised on acceptance of each milestone. Payment due within 30 days of invoice.

Currency: Ghana Cedis. International clients may pay in USD or EUR at the prevailing rate.

10. Intellectual property

On final payment, all custom source code, documentation, and design assets created under this SOW are assigned to the client. Innov8ProTech retains the right to use generic, non-client-specific components (authentication, notifications, audit logging) in other projects.

Third-party libraries remain under their original licences.

11. Warranties

Innov8ProTech warrants that the delivered system will materially conform to this SOW for a period of 90 days from launch. Defects reported in this period are fixed at no additional cost.

12. Support

Post-launch support is available under a separate agreement. See our published SLA.

13. Termination

Either party may terminate on 30 days written notice. Work completed to that date is payable. Deliverables produced to that date are handed over on payment.

14. Signatures

For [Agency name]:

Name: Title: Date:

For Innov8ProTech Ltd:

Name: Title: Date:

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

8. Sample Master Service Agreement

This is a template Master Service Agreement (MSA) for engagements with public sector and enterprise clients. A signed MSA governs all subsequent Statements of Work between the parties.

Master Service Agreement

Between: [Client name] ("Client") **And:** Innov8ProTech Ltd ("Supplier")

1. Definitions

- **"Services"** — the software design, development, deployment, and support services described in each SOW.
- **"SOW"** — a Statement of Work signed by both parties, incorporating this MSA.
- **"Deliverable"** — any item listed in a SOW and handed over to the Client.
- **"Personal Data"** — as defined in Ghana's Data Protection Act 843.
- **"Confidential Information"** — non-public information disclosed by either party.

2. Scope and hierarchy

This MSA sets out the general terms. Each SOW sets out specific deliverables, fees, and timelines. In case of conflict, the order of precedence is:

1. The SOW
2. This MSA
3. Any signed Data Processing Agreement

3. Services

Supplier will perform the Services with reasonable skill and care, in line with industry standards for custom software development, and in compliance with all applicable laws of the Republic of Ghana.

4. Fees and payment

Fees are set out in each SOW. Unless stated otherwise:

- Invoices are payable within 30 days
- Late payments accrue interest at 2% per month
- All fees are exclusive of VAT and applicable taxes
- Travel, hardware, and third-party costs are pre-approved by the Client in writing

5. Client obligations

The Client will:

- Provide a single point of contact with decision-making authority
- Provide timely access to systems, data, and personnel required for the Services
- Review and provide feedback on deliverables within the periods stated in each SOW
- Ensure that any data provided to the Supplier is lawfully held and provided

Delay caused by the Client extends the timeline accordingly.

6. Intellectual property

Client-owned: All custom source code, documentation, and design assets created specifically for the Client under a SOW are assigned to the Client on final payment.

Supplier-owned: Generic, non-client-specific components (authentication, notifications, audit logging, and similar building blocks) remain the property of the Supplier. The Client receives a perpetual, non-exclusive, royalty-free licence to use these components as part of the delivered system.

Third-party: Any third-party libraries or services remain under their original licences, and the Supplier will document them.

7. Confidentiality

Each party will keep the other's Confidential Information confidential, use it only for the purposes of this agreement, and protect it with at least the same care it uses for its own confidential information. This obligation survives termination for 5 years.

Confidential Information does not include information that is or becomes public without breach, was already known to the receiving party, or is independently developed.

8. Data protection

Where the Supplier processes Personal Data on behalf of the Client, the parties will sign a Data Processing Agreement before processing begins. The DPA governs:

- Scope, purpose, and duration of processing
- Categories of data and data subjects
- Security measures
- Subprocessor management
- Assistance with data subject rights
- Breach notification

- Return or deletion of data on termination

9. Security

The Supplier will maintain appropriate technical and organisational measures, including:

- Encryption of data at rest and in transit
- Access controls with least privilege
- Regular patching and vulnerability management
- Logging of administrative access
- Annual security testing

The Supplier will notify the Client without undue delay of any security incident affecting Client data.

10. Warranties

The Supplier warrants that:

- It has the skills, experience, and resources to perform the Services
- Deliverables will materially conform to the applicable SOW for 90 days after acceptance
- The Services will not infringe the intellectual property rights of any third party

The Client warrants that it has the right to provide any data it shares with the Supplier.

11. Limitation of liability

Neither party excludes liability for death, personal injury, fraud, or anything else that cannot lawfully be limited.

Subject to that, each party's total liability under this agreement is limited to the greater of:

- The fees paid by the Client under the applicable SOW in the 12 months before the claim, or
- GH₵ 500,000

Neither party is liable for indirect or consequential losses, loss of profit, or loss of anticipated savings.

12. Indemnity

The Supplier will indemnify the Client against any third-party claim that a Deliverable infringes intellectual property rights, provided the Client notifies the Supplier promptly and allows the Supplier to control the defence.

The Client will indemnify the Supplier against any claim arising from data the Client has provided unlawfully.

13. Term and termination

This MSA takes effect on signature and continues until all SOWs under it are complete, unless terminated earlier.

Either party may terminate:

- For convenience on 60 days written notice
- Immediately for material breach that remains uncured 30 days after written notice
- Immediately if the other party becomes insolvent or ceases trading

On termination, the Client pays for work performed to that date, and the Supplier hands over deliverables produced to that date.

14. Insurance

The Supplier will maintain insurance coverage appropriate to the scale and nature of each engagement, as agreed in writing before the applicable SOW begins. Where the Client requires specific coverage levels (Professional Indemnity, Public Liability, Cyber Liability) as a condition of award, those are arranged before contract signature and certificates provided to the Client.

15. Force majeure

Neither party is liable for delays or failures caused by events outside its reasonable control, including natural disasters, war, government action, or widespread infrastructure failure. The affected party will notify the other promptly and use reasonable efforts to resume performance.

16. Dispute resolution

The parties will attempt to resolve disputes through good-faith negotiation between senior representatives. If unresolved within 30 days, either party may refer the dispute to mediation. If mediation fails, the dispute is resolved by the courts of the Republic of Ghana.

17. Governing law

This agreement is governed by the laws of the Republic of Ghana.

18. Entire agreement

This MSA, together with any SOWs and DPAs, constitutes the entire agreement between the parties and supersedes any prior discussions or representations.

19. Signatures

For [Client name]:

Name: Title: Date:

Innov8ProTech Ltd
St. Mark Street, Com 18
Tema, Ghana
hello@innov8protech.com

For Innov8ProTech Ltd:

Name: Title: Date: