DEEP INFOSEC / PROCUREMENT

Public supplier profile

Deep InfoSec SARL | Cybersecurity, engineering & sovereign infrastructure

A practical company and service summary for supplier onboarding, early budget planning and procurement teams.

Company identification

- Registered legal name: Deep InfoSec SARL
- Country of incorporation: Senegal
- Commercial registration (RCCM): SN DKR 2023 E 55007
- Business address: Azur 15, Le Plateau, Dakar, Senegal
- Corporate enquiries: contact@deepinfosec.com
- Supplier onboarding: sales.general@deepinfosec.com

Core capabilities

- DeepShield — network defence, telemetry analysis and policy-controlled response
- Deep Advisor — attack-path analysis, remediation prioritisation and risk decision support
- Professional services — cybersecurity assessments, engineering, security architecture, audit and pentesting
- Industrial programmes — energy, OT, IoT, smart metering and critical-service resilience
- Sovereign infrastructure — data-centre and hybrid architecture, secure operations and capability transfer
- Advanced advisory — secure AI adoption and quantum-resilience planning

Commercial engagement formats

- Focused assessment — defined systems, deliverables and acceptance report
- Technical evaluation — product or engineering pilot with success and rollback criteria
- Implementation — milestone-based design and deployment with handover
- Managed service — agreed coverage, reporting and escalation plan

Commercial evaluation checklist

- Describe your critical service or project
- Identify the sites, users, assets and existing tooling
- Select the evaluation or service outcome
- Indicate any operating restrictions or maintenance windows
- Request an itemized quotation and delivery schedule

Support and technical continuity

- Incident priorities can be classified P1–P4 according to service impact. Product support hours, response objectives and escalation contacts are provided for the selected service. Production changes, OT commands and recovery actions follow customer authorization and documented acceptance.

Useful public resources

- Supplier profile: deepinfosec.com/en/procurement/company/index.html
- Commercial models: deepinfosec.com/en/procurement/commercial/index.html
- Support model: deepinfosec.com/en/procurement/support/index.html
- Integration & acceptance: deepinfosec.com/en/procurement/implementation/index.html
- Start purchasing: deepinfosec.com/en/evaluate/vendor/index.html

How a bounded technical evaluation is delivered

- Scope and context — critical services, relevant sites, systems, delivery ownership and operational boundaries
- Decision-focused questions — what the pilot must establish and what would stop expansion
- Technical method — permitted data sources, representative event paths, independent review and operational tests
- Acceptance — validation records, exceptions, remediation owners, rollback conditions and written decision
- Hand-over — documented evidence, configurations where applicable, maintenance procedures and knowledge transfer

Products, integration and industrial delivery

- DeepShield evaluation — network observation and event correlation before separately authorized enforcement
- Deep Advisor evaluation — attack-path evidence, control ownership, remediation options and retest
- Industrial energy / OT — non-disruptive site diagnosis, selected metering interfaces, local edge handling and recovery trials
- Delivery model — Deep InfoSec leads cyber engineering and assurance; field deployment disciplines can be mobilized with defined specialist responsibilities
- Public technical evaluation guides are available on the website and can be downloaded without registration

Public assurance and customer responsibilities

- Audit and testing services are scoped to the applicable PASC accreditation and engagement requirements
- Professional auditors hold ISO qualifications; specific personnel and certificate scopes are documented for the purchased assignment
- Managed data-centre services use ISO-certified infrastructure within the selected hosting scope
- The customer appoints technical ownership, approval and procurement contacts and authorizes the relevant data and test boundaries
- Sensitive operational records are exchanged only through the project channel; public brochures and company information remain directly accessible

Preparing the first purchase order

- Select assessment, controlled pilot, staged implementation or managed service
- Send the service or assets involved, country of delivery, estimated sites and the decision deadline
- Request a statement of work naming outputs, assumptions, timeline, owners, operating restrictions and acceptance criteria
- Ask for a line-item commercial schedule for experts, licensing, hardware, travel, operating coverage and applicable taxes
- Procurement contact: sales.general@deepinfosec.com; product specialists: sales.shield@deepinfosec.com and sales.advisor@deepinfosec.com