रा.इ.सू.प्रौ.सं
NIELIT

National Institute of Electronics and Information Technology, Kohima, Nagaland
Ministry of Electronics and Information Technology, Government of India
Meriema, New High Court Road, Kohima, Nagaland - 797001

Website: *https://nielit.gov.in/kohima/index.php*

Advt. No.: NIELIT/KMA/01/02/04-ADMN

Sl. No	Post	No.	Essential Qualification	Essential Experience	Desirable	Age (as on closing date)	Monthly Remuneration
1	AI Engineer	1	PhD in CS/IT/Cyber Security/Digital Forensics/Data Science/AI-ML **OR** Master's in the above domains **OR** B.E./B.Tech in CSE/IT/ECE with strong project work in AI / Cyber Security / Digital Forensics	2–5 yrs in ML/NLP/IR; LLM/RAG, embeddings & vector DBs; Python (PyTorch/TensorFlow), FastAPI; Elasticsearch/OpenSearch; MLOps (Git, Docker, CI/CD)	LangChain/ LlamaIndex; RAG eval (RAGAS); OCR/ASR for Indian scripts; legal/forensics NLP; data privacy/PII redaction	35	₹ 90000/- to ₹ 100000/-
2	Full-Stack Developer	1	PhD in Computer Science / IT / Software Engineering / related field OR M.Tech/M.E./M.S. in CSE/IT or equivalent OR B.E./B.Tech in CSE/IT/ECE or equivalent with strong full-stack development portfolio	3–5 yrs web apps; React/Next.js + TypeScript; Node.js/NestJS or Python/FastAPI; Postgres, Redis; OAuth2/OIDC/Keycloak; Docker, CI/CD; OWASP Top-10	OpenSearch integration; analytics dashboards; PDF/redaction pipeline; queues (RabbitMQ/Kafka); India-Stack flows etc	35	₹ 70,000 to ₹80000/-

3	Project Research Staff	2	Master’s degree in Computer Science / Information Technology / Cyber Security / Digital Forensics / Data Science / AI & ML OR B.E./B.Tech in CSE / IT / ECE or equivalent with strong project work in AI / Cyber Security / Digital Forensics	Minimum1 year **of relevant experience** in any combination of the following roles: project coordination, technical report analysis, academic coordination, or institutional administration in a Government department, PSU, academic institution, or similar organization. Demonstrated experience in: • Experience in data collection, cleaning, labelling/annotation and documentation, preferably for AI/ML models or knowledge bases • Experience in technical writing, such as authoring reports, SOPs, lab manuals, or training content in the cyber security / forensics domain • Reviewing and analysing technical reports/data and aligning them with project proposals, deliverables, and recommendations. • Preparing comprehensive reports, documentation, and Minutes of Meetings (MoM) to support PRSG/Working Group or similar committees.	Understanding of Indian cyber laws, IT Act, rules, and state-specific cyber-crime procedures Experience in compiling or maintaining SOPs, checklists, or reference guides for cyber investigation or digital forensics Prior involvement in developing training manuals, lab guides, or course content on cyber security / digital forensics	35	₹ 55000/- to ₹ 60000/-

4	Project Content Staff	1	Graduate in any discipline from a recognised University (minimum 50–60% or equivalent CGPA).	Minimum 5 years of experience with at least 2 years in administrative / accounts / project support in a Government department, PSU, academic institution, or similar organization. **Experience in:** Preparing note sheets, draft sanctions, and official correspondence. Handling TA/DA, reimbursement bills, and basic financial documentation. Proficiency in MS Office (Word, Excel, PowerPoint) and email handling. Basic working knowledge of office procedures, file management, and record-keeping (physical and electronic). Coordinating meetings/logistics and maintaining systematic physical and digital records.	Postgraduate degree / diploma in Management / Administration / Commerce / Computer Applications or related field. Certification / formal training in computer applications, office automation, or e-Office. Familiarity with Government project processes, including sanctions, UCs, and basic financial terminology.	35	₹ 40000/- to ₹ 45000

5	Cyber Forensic Lab Assistant		3 Years diploma ECE/CS/IT, **OR** B.Tech ECE/CS/IT.	At least 2 years' experience in Mobile Handset Repairing and 1 year experience in mobile forensics.	Crime Scene investigation skill set including First Response. Case reception and proper documentation. Excellent knowledge of vast mobile schematic diagram. Handling different method of extraction including test points, EDL, pin-point etc. Familiarity of extraction with MSAB XRY and Cellebrite UFED. Dedicated, Disciplined, Investigative & Analytical Mindset.	35	₹ 25000/- to ₹ 30000/-
6	Associate Cybersecurity Analyst	1	Masters/ B.Tech in Computer Science Engineering (CSE), Information Technology (IT), or a related discipline from a recognized university/institution	• Minimum 1.5 years of hands-on experience in cybersecurity, information security, or related domains. • Working knowledge of network security concepts, including firewalls, IDS/IPS, and VPNs. • Familiarity with Linux and Windows operating system security. • Ability to monitor, analyze, and respond to security logs, alerts, and incidents. • Understanding of common cyber threats and attack vectors, including phishing and malware. • Strong analytical, troubleshooting, and problem-solving skills.	• Knowledge of ethical hacking techniques and vulnerability assessment. • Understanding of OWASP Top 10 web application security risks. • Exposure to malware analysis and cyber forensics. • Experience in incident response support or SOC operations. • Familiarity with SIEM tools, log correlation, and alert triaging. • Relevant cybersecurity certifications (e.g., CEH, Security+, CHFI, or equivalent).	35	₹ 35000/- to ₹ 40000

Detailed role descriptions

1) AI Engineer

Role purpose: Build the AI backbone—RAG pipelines, retrieval/search, evaluation harnesses, and multilingual/legal-aware models that return grounded, auditable answers for investigators.

Key Responsibilities

- **Corpus & Data Curation**
  - Ingest and normalize heterogeneous sources (state police manuals, circulars, SOPs, rules, international treaties, case law summaries, training notes).
  - Design document schemas/metadata (jurisdiction, statute/section, effective date, precedence, language, sensitivity).
  - Implement ETL/OCR (Devanagari/Indic scripts), de-duplication, redaction for PII, and chain-of-custody friendly logs.
- **Retrieval & RAG**
  - Build hybrid search (BM25 + dense embeddings) with OpenSearch/Elasticsearch + vector DB (FAISS/Milvus/pgvector).
  - Create RAG pipelines (chunking, reranking, citations) with guardrails to prevent hallucinations; support multilingual queries.
  - Implement role-aware retrieval (LEA roles) and policy-based prompts for safe responses.
- **Modeling & Evaluation**
  - Fine-tune or instruct-tune domain adapters; explore small LLMs for on-prem.
  - Build evaluation harness (exact match/F1, groundedness, citation coverage, answer latency); use golden sets curated with SMEs.
  - Add safety filters (policy checks, toxicity, privacy, export controls where relevant).
- **Serving & MLOps**
  - Ship inference services (FastAPI), version models, set up A/B tests, telemetric logging, and drift monitoring.
  - Document reproducible experiments; maintain model registry and datasets with clear licenses.

2) Full-Stack Developer

Role purpose: Deliver a secure, scalable platform—RBAC frontend, API layer, data services, admin/analytics consoles—ready for sensitive LEA workloads.

Key Responsibilities

- **Architecture & Platform**
  - Implement modular services (auth, search, RAG, content ingestion, audit logging) with clear APIs.
  - Set up RBAC/OIDC (e.g., Keycloak), JWT rotation, session management, password and MFA policies.
- **Backend (Node/NestJS or Python/FastAPI)**
  - Build endpoints for query, citations, feedback, analytics; background workers for ingestion and re-indexing.
  - Design PostgreSQL schema (documents, jurisdictions, roles, events, audit trails); Redis for caching/queues.
- **Frontend (React/Next.js + TypeScript)**
  - Investigator UI (search, filters, pinned citations), admin dashboard (role/tenant management, usage analytics), analytics panels.
  - Multilingual/i18n, accessible components, responsive tables, printable reports, export (PDF/CSV).
- **Security & Observability**
  - Enforce OWASP Top 10 mitigations, secure file uploads, content-security policy, rate limiting.
  - Implement audit logs, tamper-evident event streams, and structured logs with ELK/EFK; metrics via Prometheus/Grafana.
- **CI/CD & Environments**
  - Containerize with Docker; pipelines for unit/integration tests; staging → beta → prod release strategy.
  - Infra as code (basic), secrets management, backups and restore drills.

3. Project Research Staff (PRS)

Role purpose: Applied research, prototyping, content curation, and experimentation to operationalise Cyber tools, datasets, and training assets.

Key responsibilities

- **AI Tool Prototyping:** Design, implement, and test AI/ML/NLP models for cybercrime investigation; document experiments and performance.
- **Dataset Curation & Annotation:** Collect, clean, and structure datasets of cyber laws, SOPs, forensic artefacts, logs, and case studies (national/state level), including labelling and metadata.
- **Forensic Manuals & Knowledge Assets:** Assist domain experts in drafting and updating cloud/IoT/enterprise forensic manuals, checklists, and quick-reference guides.
- **Gamified Platform & Question Bank:** Develop scenario-based questions, quizzes, and caselets for adaptive/gamified cyber security/forensics learning platforms.
- **AR/VR Crime Scene Support:** Work with technical partners on requirements, storyboards, and validation for AR/VR-based crime scene simulation POC.
- **Field Interaction & Feedback:** Coordinate with law enforcement/training academies to gather requirements, validate tools/manuals, and incorporate feedback into iterative improvements.
- **Documentation & Reporting:** Maintain research logs, versioned datasets, model cards, and contribute to technical reports, publications, and project presentations.
- **Quality, Ethics & Compliance:** Ensure data handling, privacy, and research activities follow legal, ethical, and organizational guidelines, keeping artefacts audit-ready.

4. Project Content Staff

Role purpose:
To support technical evaluation, documentation, and coordination of projects and academic/training activities by analysing reports and data, preparing high-quality documentation, managing portals and records, and facilitating smooth execution in alignment with defined objectives, deliverables, and institutional/government norms.

Key responsibilities

- **Technical Report & Data Analysis:**
  Review and analyse technical reports, project data, and deliverables for accuracy, completeness, and alignment with approved proposals and defined outcomes; refine recommendations to support data-driven decision-making.

- **Documentation & MoMs:**
  Prepare comprehensive reports, briefs, and Minutes of Meetings (MoM) for PRSG, Working Groups, and other committees, ensuring clarity, completeness, and timely circulation for informed discussions and strategic planning.

- **Cross-Functional Coordination:**
  Coordinate with cross-functional teams to integrate project findings and recommendations into broader institutional or national initiatives, ensuring smooth execution, follow-up on action points, and measurable impact.

- **Portal & E-Office Management:**
  Manage e-Office workflows, official emails, and grievance redressal portals; maintain and update project-related technical and financial data on relevant portals (such as PRIME) to ensure compliance, transparency, and audit readiness.

- **Academic & Training Support:**
  Assist in planning and coordinating academic schedules, faculty activities, workshops, and events; support preparation of lesson plans and project guidance for students, ensuring adherence to institutional policies and accreditation requirements.

- **Admissions & Outreach:**
  Support admission processes, including student counselling, documentation, record keeping, and achieving enrolment targets through structured processes and outreach initiatives.

- **General Administrative Duties:**
  Undertake additional office and divisional tasks as assigned by the reporting officer, contributing to efficient day-to-day operations and effective stakeholder engagement.

5. Cyber Forensic Lab Assistant

Role Purpose

To assist the cyber forensic team in mobile device handling and extraction support by ensuring proper case reception, evidence documentation, and disciplined lab practices, using practical handset repairing skills and basic mobile forensic tool exposure.

Key Responsibilities

- Receive mobile devices and related exhibits, verify case details, label items properly, and maintain case registers and documentation.
- Maintain chain-of-custody records and ensure secure storage and controlled movement of exhibits within the lab.
- Perform basic device checks (make/model/IMEI/condition/power state/lock status) and record observations as per lab format.
- Support mobile data extraction activities under supervision using MSAB XRY and Cellebrite UFED, and document the method and output details.
- Assist in handling extraction methods such as EDL, pin-out/pin-point and test point access, as directed, using schematic knowledge and repair experience.
- Ensure safe handling of devices to prevent damage, data loss, or contamination, and follow lab SOPs strictly.
- Maintain readiness of extraction accessories and lab tools (cables, adapters, power supplies), and report faults or shortages promptly.
- Support basic evidence packing, sealing, and return procedures with proper entries and acknowledgement records.

6. Associate Cybersecurity Analyst

Role Purpose

The Associate Cybersecurity Analyst supports the organization’s cybersecurity posture through continuous monitoring, analysis, and first-level response to security events. The role contributes to prevention, detection, investigation, and containment of threats across network, endpoint, and application environments, while ensuring timely escalation, accurate documentation, and adherence to established security policies and procedures.

Key Responsibilities

- Monitor and review security logs and alerts from firewalls, IDS/IPS, endpoints, servers, and related sources.
- Perform initial alert triage by validating events, identifying false positives, assessing severity, and prioritizing actions.
- Support incident handling for phishing, malware, suspicious access, and network anomalies, including basic containment actions under supervision.
- Analyze and correlate logs to identify abnormal activity and assist in confirming indicators of compromise (IPs, domains, hashes, processes).
- Assist with basic Linux/Windows security checks, access control verification, and investigation of endpoint irregularities.
- Support vulnerability scanning activities, validate findings, and help track remediation actions.
- Assist with SIEM/SOC processes such as alert handling, dashboard updates, routine tool health checks, and standard reporting.
- Maintain clear incident documentation and monitoring reports as per SOPs and audit requirements.
- Coordinate with relevant technical teams for resolution, escalations, and effective shift handovers (where applicable).