N-21013/9/2024-NeGD
National e-Governance Division
Digital India Corporation
Electronics Niketan, 6, CGO Complex Lodhi Road,
New Delhi – 110003
Website: www.negd.gov.in / www.dic.gov.in

Web Advertisement
24.08.2026

The National e-Governance Division (NeGD) is an independent business division under the Digital India Corporation, Ministry of Electronics and Information Technology. NeGD has been playing a pivotal role in supporting MeitY in Programme Management and implementation of e-Governance projects and initiatives undertaken by various Ministries/ Departments, both at the Central and State levels.

NeGD has been spearheading several innovative initiatives under the aegis of the Digital India Programme. Those have been developed keeping the vision areas of Digital India at the core- providing digital infrastructure as a core utility to every citizen, governance and services on demand and in particular, digital empowerment of the citizens of our country; some of these initiatives include DigiLocker, UMANG, Poshan Tracker, OpenForge Platform, API Setu, National Academic Depository, Academic Bank of Credits, Learning Management System.

It has myriad roles and responsibilities from supporting Central Line Ministries and State Government Departments on e-Governance projects, reviewing State Action Plans, offering support in technology management, strategy formulation & implementation of Emerging Technologies viz. AI, Blockchain, GIS etc., to facilitating digital diplomacy with focus on Indian startups and products

NeGD has been a leader in implementation and execution of a gamut of pilot/ infrastructure/ technical/ special projects and support components to framing core policies, project appraisals, R&D, and guiding /conducting assessments, undertaking activities for building capacities of both Government officials and] other stakeholders, and creating mass awareness about schemes and services under the Digital India Programme.

NeGD is currently inviting applications for the following positions purely on Contract basis initially for a period of 3 years which is further extendable as per the requirement of the project.

S. No	Position	Vacancy
1	Senior UI/UX Designer	01
2	Senior Security Engineer	01

* The maximum age limit shall be 55 years on the closing date of receipt of application.
** The place of posting shall be in New Delhi but transferable to project locations of NeGD as per existing policy of NeGD/DIC.
Screening of applications will be based on qualifications, age, and relevant experience. NeGD reserves the right to fix higher threshold of qualifications and experience for screening and limiting the number of candidates for interview. Only shortlisted candidates shall be invited for interviews. NeGD reserves the right to not to select any of the candidates without assigning any reason thereof.
The details can be downloaded from the official website of **DIC** and **NeGD**, viz. **www.dic.gov.in**, **www.negd.gov.in**.

Eligible candidates may apply ONLINE: https://ora.digitalindiacorporation.in/

Last date for submission of applications will be: 07.09.2026

Senior UI/UX Designer

AI Projects

JOB DESCRIPTION

A. Overview

NeGD is building a portfolio of AI-driven digital products for citizens at national scale — conversational assistants, agentic platforms, decision-support dashboards, and content tools whose primary users are members of the public and whose ownership rests with government. We are looking for a Senior UI/UX Designer to shape these experiences: someone working at the frontier of AI-native design who can turn probabilistic, agentic systems into interfaces that ordinary people can trust and use with confidence.

The ideal candidate pairs a strong, current portfolio — chatbots, agentic products, dashboards, and citizen- or consumer-facing digital services — with a genuine grounding in Human-Computer Interaction. This is a role for a designer who justifies decisions on the basis of interaction theory and usability evidence rather than aesthetic preference alone, and who is fluent in the newest generation of AI-assisted design tools and workflows.

The selected designer will work alongside product managers, engineers, policy teams, and government stakeholders to create intuitive, accessible, and visually compelling experiences for a diverse public — including first-time and low-digital-literacy users — where usability is not a nicety but a precondition for the product to serve its purpose.

B. Roles and Responsibilities

- Design and prototype interfaces for AI-driven products — conversational assistants, agentic platforms, data and decision-support dashboards, and content tools across web, mobile, and social channels — using industry-standard design and prototyping tools (e.g., Figma), AI assistants such as Claude, and cloud-based AI/design tooling (e.g., Azure or equivalent).
- Use generative AI and AI-assisted design workflows to accelerate ideation, prototyping, content generation, and iteration — and help the team adopt new methods as the tooling landscape evolves.
- Design conversational and agentic interaction flows — dialogue and prompt design, agent task flows, error and fallback states, and human-handoff patterns — applying core HCI principles (mental models, affordances and signifiers, cognitive load, visibility of system status, error prevention and recovery) to systems whose behaviour is probabilistic and whose trustworthiness must be actively earned and calibrated.
- Design for appropriate reliance in human-AI interaction: communicate uncertainty and system limits, surface sources and reasoning where relevant, and mitigate over-trust and automation bias in agentic and decision-support flows.

- Translate requirements and wireframes into polished, high-fidelity UI while maintaining design-system and brand consistency across a portfolio of government-owned products.
- Apply visual hierarchy, typography, layout, and responsive design — together with established interaction laws and models (Fitts's, Hick's, Miller's, Gestalt principles, progressive disclosure, recognition over recall) — to navigation and information-density decisions, with particular care for first-time and low-digital-literacy users.
- Run and participate in user research, usability testing, and design critique, with sustained attention to accessibility and digital inclusion across a diverse citizen base.
- Conduct task analysis, cognitive walkthroughs, and heuristic evaluations (Nielsen's heuristics) on existing and proposed interfaces, and convert findings into a prioritised, evidence-backed set of design changes.
- Define and track usability metrics — task success rate, time on task, error rate, drop-off, and System Usability Scale (SUS) scores — and use them to benchmark design changes release over release.
- Ensure all designs meet accessibility and government digital-service standards (WCAG 2.2 AA, GIGW 3.0) and Government of India norms.
- Deliver high-quality design assets, specifications, and documentation for smooth development handoff.
- Contribute to and evolve design systems, design tokens, and component libraries suited to government and citizen-service products.
- Collaborate closely with product, engineering, policy, and government stakeholders to align citizen needs, product goals, and technical and regulatory constraints.

C. Required Profile

Educational Qualifications

- Bachelor's degree in UI/UX Design, Human-Computer Interaction, Graphic Design, Computer Science (design specialisation), or a related field.
- A Master's degree, postgraduate diploma, or formal certification in Human-Computer Interaction, Interaction Design, Human Factors, or Cognitive Psychology is an added advantage.

Experience and Skills — Essential

- Minimum 5 years in UI/UX design, with demonstrated hands-on experience designing AI-driven products (chatbots, agentic systems, dashboards, or similar). Depth and quality of relevant work matter more than years alone.
- A strong portfolio of work for large-scale, citizen- or consumer-facing products where the user base is broad and non-expert and the stakes for usability and accessibility are high.

- Hands-on fluency with current design and prototyping tools (e.g., Figma), AI assistants (e.g., Claude), cloud-based AI/design tooling (e.g., Azure or equivalent), and raster/graphics tools (e.g., Adobe Photoshop, Canva) — and with the newest AI-assisted design techniques and workflows.

- Strong command of user-centred design, responsive layouts, visual hierarchy, and conversational/agentic UX patterns, built on a real grounding in HCI fundamentals — usability engineering, interaction models, and human perception, attention, memory, and decision-making as applied to interfaces — with the ability to explain and defend design choices in these terms.

- Practical command of usability and interaction evaluation methods — heuristic evaluation, cognitive walkthrough, task and workflow analysis, think-aloud protocols, contextual enquiry, and A/B or comparative usability testing.

- Understanding of human-AI interaction as a distinct design problem: trust calibration, explainability, uncertainty communication, graceful failure, and the design of human oversight and correction mechanisms.

- Familiarity with accessibility guidelines (WCAG 2.2 AA, GIGW 3.0) and inclusive design for a diverse, non-expert public.

- Knowledge of design systems, design tokens, and component-based UI frameworks (e.g., Material UI, Tailwind CSS).

- Solid grounding in branding, colour theory, and typography.

- Excellent communication and stakeholder-management skills, with the ability to work directly with cross-functional teams and clients and to incorporate feedback quickly.

- Outcome-driven; comfortable operating as an independent specialist or within a larger team, and able to lead design direction and push innovation across projects.

Experience and Skills — Desirable

- Prior experience delivering design work for government or public-sector projects (a plus, not a requirement).

- Experience with digital public services, learning platforms, or other high-scale citizen-facing products in India.

- Exposure to multilingual UI/UX and design for Tier 2/Tier 3 and rural digital users.

- Formal coursework, published work, or applied research in human-computer interaction, human factors, or cognitive psychology.

- Familiarity with current human-AI interaction guidance and toolkits (e.g., Google PAIR guidebook, Microsoft HAX toolkit, human-factors considerations under the NIST AI Risk Management Framework).

- Experience with quantitative usability measurement and benchmarking — SUS scoring, task-based benchmarking, and click/heatmap or eye-tracking analysis.

- Experience with UX analytics, experimentation, and data-informed design iteration.

– Relevant, up-to-date certifications in design, HCI, or AI-assisted design.

D. Selection Process

Shortlisted candidates will present their top three design works during the interview, to demonstrate design potential, craft quality, and depth of AI-driven design experience.

For at least one of these works, the candidate should be prepared to walk the panel through the HCI reasoning behind the design — the user model assumed, the evaluation method applied, and the usability evidence that informed the final decisions.

Senior Security Engineer

AI Projects

J0B DESCRIPTION

A. Overview

NeGD is building a portfolio of AI-driven digital products for citizens at national scale — conversational assistants, agentic platforms, document and decision-support systems, identity and verification services, fraud-detection solutions, and other AI-enabled government platforms.

We are looking for a **Senior Security Engineer** to secure these systems end to end: someone who is equally comfortable identifying vulnerabilities in a conventional web application or API, reviewing authentication and cloud configurations, and attacking an LLM, RAG pipeline, ML model, or autonomous agent.

This is a **hands-on engineering role**. The ideal candidate does not only define security policies, coordinate audits, or review reports. They can personally inspect code and architecture, build threat models, use offensive and defensive security tooling, reproduce vulnerabilities, write scripts and test harnesses, configure security controls, and work directly with engineers to remediate findings.

The role requires depth in established cybersecurity disciplines — application security, API security, identity, cloud and infrastructure security, secure SDLC, penetration testing, cryptography, vulnerability management, and incident response — together with practical understanding of the emerging attack surface introduced by AI systems.

The selected engineer will work alongside software engineers, AI/ML engineers, MLOps and DevOps/ SRE teams, product managers, AI safety specialists, and government stakeholders to build systems that are secure by design and resilient against both traditional and AI-specific attacks.

B. Roles and Responsibilities

– Conduct hands-on security assessment of web applications, APIs, microservices, mobile/backend services, cloud deployments, containers, and supporting infrastructure, using a combination of manual testing and automated security tooling.

– Perform application and API penetration testing covering authentication and authorisation failures, injection vulnerabilities, insecure business logic, SSRF, deserialisation issues, file-handling vulnerabilities, privilege escalation, session weaknesses, secrets exposure, and other OWASP-class vulnerabilities.

– Conduct security reviews of AI-enabled applications, including **LLM, RAG, agentic AI, predictive ML, computer vision, identity-verification, and fraud-detection systems**, identifying risks introduced by models, prompts, retrieval layers, tools, data pipelines, and integrations.

– Design and execute **LLM and agentic-AI red-team exercises** covering direct and indirect prompt injection, jailbreaks, system-prompt leakage, sensitive-data disclosure, insecure tool invocation,

excessive agency, permission bypass, output manipulation, cross-user data leakage, and policy-boundary violations.

– Assess **RAG security** including poisoning or manipulation of retrieved content, malicious document ingestion, retrieval-based prompt injection, source-integrity weaknesses, access-control failures in vector stores, sensitive-data retrieval, and trust-boundary failures between retrieval and generation components.

– Test traditional and machine-learning systems for relevant **adversarial ML threats**, including adversarial inputs, model extraction, model inversion, membership inference, data poisoning, training-data leakage, and abuse of prediction or inference APIs.

– Build reusable scripts, attack harnesses, payload libraries, test datasets, and automated security checks in Python, Bash, or equivalent languages so security testing can be reproduced and integrated into engineering workflows.

– Perform threat modelling for conventional and AI-enabled systems using frameworks such as STRIDE, attack trees, MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, OWASP API Security Top 10, and OWASP guidance for LLM and generative-AI applications.

– Review architecture and code for secure implementation of authentication, authorisation, session management, API security, input validation, output handling, file processing, secrets management, logging, encryption, and data isolation.

– Review **OAuth 2.0, OpenID Connect, SAML, RBAC, ABAC, service-to-service authentication, API keys, tokens, and workload identities**, and identify privilege-escalation or access-control weaknesses across applications and AI services.

– Integrate and operate security testing within the software delivery lifecycle, including **SAST, DAST, SCA, secrets scanning, container and image scanning, IaC scanning, dependency vulnerability management, and security gates within CI/CD pipelines**.

– Conduct manual code review and configuration review where automated tooling is insufficient, particularly for high-risk services, custom authentication flows, sensitive-data processing, and AI orchestration logic.

– Assess cloud, Kubernetes, container, network, API-gateway, WAF, secrets-management, logging, and model-serving configurations for exploitable misconfigurations and insecure defaults, working closely with DevOps/SRE and MLOps engineers.

– Review the security of AI model and data supply chains — training and evaluation data, model artefacts, open-source models, third-party APIs, packages, containers, model registries, prompt templates, embeddings, plugins, tools, and external knowledge sources.

– Define and help engineers implement practical mitigations for AI attacks, including prompt and context isolation, privilege minimisation, tool allow-listing, deterministic security controls outside the model, input/output validation, secure retrieval, sandboxing, human approval for high-impact actions, and monitoring for abuse.

– Verify that security controls work in practice by attempting to bypass them rather than relying solely on design documentation or vendor claims.

– Reproduce findings reported by VAPT providers, automated scanners, researchers, or internal teams; determine exploitability and severity; and work directly with engineering teams until remediation is technically verified.

– Support security incident investigation and root-cause analysis, including examination of application logs, cloud and infrastructure telemetry, authentication events, AI interaction logs, model/tool activity, and indicators of compromise or abuse.

– Contribute secure coding patterns, threat models, red-team playbooks, testing utilities, security checklists, and reusable engineering controls that can be adopted across multiple government AI projects.

– Stay current with developments in application security, cloud security, offensive security, adversarial machine

learning, LLM security, agent security, and AI supply-chain security, and translate relevant research into practical engineering controls and tests.

C. Required Profile

Educational Qualifications

– Bachelor's degree in computer science, Information Technology, Cybersecurity, Electronics, or a related engineering discipline.
– A master's degree in information security, Cybersecurity, Computer Science, Artificial Intelligence, or a related field is an added advantage.
– Strong demonstrable practical security capability may be considered alongside non-traditional educational backgrounds.

Experience and Skills — Essential

– Minimum **5 years of hands-on cybersecurity experience**, with substantial experience in application security, penetration testing, product security, offensive security, cloud security, or security engineering. Depth and quality of practical work matter more than years alone.
– Demonstrated ability to personally conduct security testing rather than only manage security vendors, compliance programmes, or audit processes.
– Strong practical knowledge of **web and API security**, including the OWASP Top 10, OWASP API Security Top 10, authentication and authorisation vulnerabilities, session management, access-control flaws, injection classes, SSRF, secrets exposure, and business-logic abuse.
– Hands-on proficiency with security tooling such as **Burp Suite, OWASP ZAP, Nmap, Semgrep, SonarQube, Snyk, Trivy, Gitleaks, Dependency-Track, Metasploit, or equivalent tools**, with the ability to go beyond scanner output and manually validate findings.

– Ability to read and reason about application code in at least one commonly used language such as **Python, JavaScript/TypeScript, Java, Go, or C#**, and sufficient coding ability to create security scripts, proof-of-concepts, test harnesses, or automation.

– Practical understanding of cloud and container security, including Docker, Kubernetes, IAM, secrets management, network segmentation, TLS, cloud storage, API gateways, WAFs, workload identity, and common cloud misconfiguration patterns.

– Strong understanding of identity and access security — OAuth 2.0, OpenID Connect, SAML, RBAC/ ABAC, token security, service identities, API authentication, privilege boundaries, and least-privilege design.
– Experience with secure SDLC and DevSecOps practices, including threat modelling, secure design review, code review, SAST, DAST, SCA, secrets scanning, vulnerability management, and integration of security controls into CI/CD.
– Working understanding of cryptographic security fundamentals including TLS, encryption at rest, key and certificate management, hashing, signing, PKI, and appropriate use of secrets-management systems.
– Demonstrated understanding of the architecture of modern AI applications — LLM APIs, system and user prompts, RAG, embeddings and vector databases, agents and tool calling, model serving, ML pipelines, and third-party/open-source models.
– Hands-on experience testing at least some **AI-specific security risks**, such as prompt injection, jailbreaks, sensitive-information disclosure, insecure tool use, RAG manipulation, adversarial inputs, model extraction, or data poisoning.

– Familiarity with frameworks and guidance such as **MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, OWASP Testing Guide, and OWASP security guidance for LLM and generative-AI applications**.

– Ability to distinguish between weaknesses that should be addressed through model behaviour or guardrails and security boundaries that must be enforced deterministically in application code, identity systems, infrastructure, or architecture.

– Strong analytical and communication skills, with the ability to explain an exploit to an engineer, a technical risk to an architect, and the business impact of a vulnerability to a non-security stakeholder.

– Outcome-driven and comfortable working as an independent hands-on specialist while collaborating closely with software, AI/ML, MLOps, DevOps/SRE, product, and governance teams.

Experience and Skills — Desirable

– Experience conducting structured red-team exercises against production or production-like **LLM, RAG, multimodal, or agentic AI systems**.
– Experience with adversarial machine learning frameworks or techniques, including **ART, Foolbox, CleverHans, or equivalent**, and attacks such as model extraction, inversion, membership inference, poisoning, or adversarial examples.
– Familiarity with AI-security testing and evaluation tools, emerging LLM red-team frameworks, guardrail testing frameworks, or experience creating custom attack harnesses where available tools are insufficient.
– Experience securing vector databases, ML pipelines, model registries, GPU/model-serving infrastructure, AI APIs, and model or data supply chains.

– Experience with AWS, Azure, GCP, sovereign cloud, on-premise Kubernetes, or comparable enterprise infrastructure.

– Experience with security monitoring, detection engineering, incident response, SIEM, audit logs, and investigation of suspicious activity across application and cloud environments.

– Prior work in government, BFSI, critical infrastructure, identity platforms, citizen-scale digital services, or other regulated/high-assurance environments is a plus.

– Familiarity with Government of India security and data-protection requirements, including MeitY security guidance, CERT-In requirements, STQC processes, DPDPA 2023, and relevant Government of India data-classification requirements.

– Relevant certifications such as **OSCP, OSWE, GWAPT, CISSP, CSSLP, CKS, cloud-security certifications, or equivalent** are desirable, but practical security capability will be given greater weight than certifications alone.

– Security research, responsible disclosure, CVEs, bug-bounty findings, CTF performance, open-source security contributions, conference presentations, technical blog posts, attack tools, or demonstrable personal security projects are strongly valued.

D. Selection Process

Shortlisted candidates will be expected to demonstrate practical security depth during the interview rather than relying solely on certifications or theoretical knowledge.

Candidates should be prepared to discuss **two or three security assessments, vulnerabilities, red-team exercises, or security-engineering projects that they personally worked on**, including the system architecture, attack path, tools and techniques used, exploitability assessment, remediation, and how the fix was validated.

The assessment may include a practical or scenario-based exercise covering both:

– **Conventional security**, such as analysing an application/API architecture, reviewing code or configuration, identifying an authentication or authorisation flaw, interpreting scanner findings, or developing a penetration-testing approach; and

– **AI security**, such as threat-modelling an LLM/RAG or agentic system, designing prompt-injection or data-exfiltration tests, analysing unsafe tool use, identifying trust boundaries, or proposing and validating controls against an AI-specific attack.

The selection process will place particular weight on whether the candidate can **personally investigate, exploit, automate, remediate, and verify security issues** across both traditional software systems and modern AI applications.

General Conditions applicable to all applicants covered under this advertisement

1. Those candidates, who are already in regular or contractual employment under Central / State Government, Public Sector Undertakings or Autonomous Bodies, are expected to apply through proper channel or attach a 'No Objection Certificate' from the employer concerned with the application OR produce No Objection Certificate at the time of interview.
2. NeGD reserves the right to fill all or some or none of the positions advertised without assigning any reason as it deems fit.

3. The positions are purely temporary in nature for the project of NeGD/DIC and the appointees shall not derive any right or claim for permanent appointment at NeGD/DIC or on any vacancies existing or that shall be advertised for recruitment by NeGD in future.
4. NeGD reserves the right to terminate the appointments of all positions with a notice of one month or without any notice by paying one month's salary in lieu of the notice period.
5. The designation of the selected candidates shall be mapped as per the existing designation policy of NeGD.
6. In case of a query, the following officer may be contacted:

HR Team
National e Governance Division, 4th Floor, Electronics Niketan,6-CGO, Complex Lodhi Road, New Delhi – 110003
Tel: 24301932
Email: Negdhr@digitalindia.gov.in