बैंकिंग प्रौद्योगिकी में विकास और अनुसंधान संस्थान

(भारतीय रिजर्व बैंक द्वारा स्थापित)

INSTITUTE FOR DEVELOPMENT & RESEARCH IN BANKING TECHNOLOGY

(Established by Reserve Bank of India)

Advertisement No: 01/2026 – 27	**Date: May 06, 2026**

Recruitment for the Senior, Associate & Lead Executives

Requirements:

Institute invites applications from talented, passionate and ambitious technology professionals to create and maintain appropriate and adequate IT infrastructure and Platform for sustainable enablement of development and research in emerging technologies. These opportunities will provide a unique opportunity to build, maintain and support infrastructure for development and absorption of emerging technologies having impact with India's digital infrastructure under the guidance of RBI. We are looking for enthusiastic and self-motivated human assets for adoption and absorption of AI and its emerging incarnations, Blockchain/Tokenization, Quantum and Post Quantum Cryptography, wider use of Digital signing in identification and access management, etc.

The current Infrastructure includes premises Private Cloud, Multiple layers of Network and Security to meet differentiated level of demand, requirement and use in Development/research and live Operations. The operation areas include Application/platform for Certifying Authority, Domain Registrar, Threat Intel Platform (Sachet – IBCART 3.0), Systems for enterprise internal use, Cyber Range for Supervisory Assessment, (CR for SA) (in collaboration with ReBIT-RBI : https://rebit.org.in) and also System and infrastructure for development, testing, PoC and upgrade of existing Applications/Platforms and new system in pipeline.

The Institute (https://www.idrbt.ac.in/about-idrbt/):

IDRBT, the Institute, was established by Reserve Bank of India in March 1996 as a Society (under Society Registration Act). The mission and vision of IDRBT continue to be brain trust for adoption and absorption of technology in BFSI sector as envisaged by RBI. The Institute became financially independent since 2004.

The Institute, since its inception, has been engaged in research and development of enabling platform/environment for emerging technologies and its

integration and adoption, in BFSI sector. During its journey the Institute has developed, grounds-up, the Indian Financial Network (INFINET), National Financial Switch (NFS) – for linking of ATMs, Structured Financial Messaging System (SFMS), National Electronic Funds Transfer (NEFT), Real Time Gross Settlement Systems (RTGS), Domain Registrar, etc. and continue to be the Certifying Authority under the Central Certifying Authority (CCA), MeitY, Govt. Of India for digital signature certificates, eSign etc.

Over the period, the Institute has evolved as a prime center for Research, Academics, Executive education, Consultancy, Development of Standards/ frameworks for AI, Cyber Security, Blockchain etc. The Institute had created and continue to engage and augment the Forum for Chief Information Security Officers (CISO in 2010), Chief Information Officers (CIO) Forum (2015), Chief Analytics Officers (CAO) Forum (CAO) (2016) and recently the Fin-Tech Forum. Executive Development and Certification Programmes form an integral part of the Institute′s initiatives To meet the ICT industry and banking sector demand, the Institute also runs the Post Graduate Diploma in Financial Technology (PGDFT), a full-time on-campus one-year programme.

i. Job Location : Hyderabad

ii. Engagement Areas : Lead/Senior Associates, System Associates/System Engineers

a) Application Security Developer
b) Development Security Operations Engineer
c) Security Developers
d) Digital Forensics
e) Network Security

iii. Job Description and Requirements:

Lead/Senior Associates/Associates/System Engineers		
a)	Application Security Developer	JOB DESCRIPTION: ✓ Perform manual and automated security testing of web applications and APIs using OWASP methodologies. ✓ Lead application security reviews including threat modeling, architecture risk assessments, and secure design consultations for new product features. ✓ Conduct API security testing focusing on authentication flaws, injection risks, and business logic vulnerabilities.

		✓ Manage the application vulnerability lifecycle: track, prioritize, and report on findings through to verified remediation. REQUIREMENTS: ✓ Bachelor's degree in Computer Science, Software Engineering, or a related field. ✓ 3–5 years of experience in application security testing and secure development in a financial or enterprise environment. ✓ Strong proficiency in web application penetration testing using Burp Suite Pro or equivalent. ✓ Hands-on experience with OWASP Top 10, OWASP API Security Top 10. ✓ Development background in at least one language: Java, Python, JavaScript/Node.js, or Kotlin/Swift. ✓ Knowledge of authentication and authorization standards: OAuth 2.0, SAML, OpenID Connect, and JWT security. ✓ Familiarity with static/dynamic analysis tools. ✓ Familiarity with Digital Certificates and HSMs is an added advantage.
b)	Security Engineer on premises for Nutanix Private Cloud Management	JOB DESCRIPTION: ✓ Operate and tune security tooling: vulnerability management platforms, SIEM integrations, and secret management vaults. ✓ Collaborate with development squads to remediate security findings and provide security coaching within sprint cycles. ✓ Build and maintain security dashboards and metrics to track vulnerability SLAs, mean time to remediate (MTTR), and pipeline health. ✓ Support incident response activities related to CI/CD pipeline breaches, cloud misconfigurations, or container escapes. ✓ Ensure DevSecOps, ISO 27001 ✓ Evaluate and onboard new security tools and advocate for developer-friendly security tooling. REQUIREMENTS: ✓ Bachelor's degree in Computer Science, Information Technology, or a related field. ✓ 3–5 years of experience in DevOps or DevSecOps roles within an enterprise or regulated environment.

		✓ Hands-on experience with CI/CD platforms (Jenkins, GitHub Actions, GitLab CI) and securing build pipelines. ✓ Proficiency with container technologies: Docker, Kubernetes, and container security tools. ✓ Experience with cloud platforms (AWS or Azure) and cloud-native security services (AWS Security Hub, GuardDuty, Azure Defender). ✓ Knowledge of Infrastructure-as-Code security: Terraform, Ansible, with tools like Checkov or KICS. ✓ Scripting skills in Python, Bash, or Go for automation and tooling development. ✓ Familiarity with OWASP SAMM, NIST SSDF, or equivalent secure software development frameworks.
c)	Security Engineer & Lead Operations	JOB DESCRIPTION: ✓ Design and develop security tools, APIs, and microservices to automate threat detection, vulnerability management, and compliance monitoring. ✓ Integrate security controls into CI/CD pipelines including SAST, DAST, SCA, and secrets management tooling. ✓ Build and maintain internal security dashboards, alerting systems, and reporting tools for SOC and risk teams. ✓ Conduct secure code reviews and threat modeling for new features and critical banking applications. ✓ Develop libraries and SDKs that enforce cryptographic standards, authentication, and authorization best practices across development teams. ✓ Collaborate with application teams to remediate vulnerabilities identified through SAST/DAST scans and penetration tests. ✓ Implement and maintain identity and access management (IAM) integrations including OAuth 2.0, SAML, and OpenID Connect. ✓ Participate in the security architecture review process for new digital banking products and APIs. ✓ Document security standards, developer security guides, and internal knowledge bases. ✓ Stay current with emerging threats relevant to financial applications (OWASP Top 10, API security risks).

		REQUIREMENTS: ✓ Bachelor's degree in Computer Science, Software Engineering, or a related field. ✓ 3–5 years of software development experience with a strong focus on application security. ✓ Proficiency in at least two programming languages: Java, Python, Node.js, or Go. ✓ Experience with SAST/DAST tools and integrating them into CI/CD workflows. ✓ Solid understanding of cryptography, PKI, TLS, and secure key management practices. ✓ Familiarity with OAuth 2.0, SAML 2.0, JWT, and OpenID Connect standards. ✓ Knowledge of OWASP Top 10, SANS 25, and secure SDLC frameworks. ✓ Experience building RESTful APIs with security best practices (rate limiting, input validation, API gateways).
d)	Digital Forensic Expert	JOB DESCRIPTION: ✓ Conduct end-to-end digital forensic investigations for cybersecurity incidents, insider threats, financial fraud, and regulatory inquiries. ✓ Perform forensic acquisition and analysis of disk images, memory dumps, network captures, and cloud logs maintaining strict chain of custody. ✓ Analyze endpoint artifacts: Windows/Linux file systems, registry hives, event logs, browser artifacts, and email forensics. ✓ Investigate network-based incidents using packet captures, NetFlow data, proxy logs, and SIEM correlation to reconstruct attack timelines. ✓ Perform malware triage and static/dynamic analysis to determine threat actor TTPs and scope of compromise. ✓ Prepare detailed forensic investigation reports suitable for legal proceedings, regulatory submission (RBI, SEBI), and executive briefings. ✓ Support e-Discovery processes and respond to legal holds in coordination with the legal and compliance teams. ✓ Collaborate with the SOC and threat intelligence teams to share indicators of compromise (IOCs) and improve detection capabilities.

		✓ Develop and maintain forensic procedures, evidence handling guidelines, and investigation playbooks. ✓ Stay current with emerging digital forensics techniques, threat actor behaviors, and financial cybercrime trends. REQUIREMENTS: ✓ Bachelor's degree in Computer Science, Cybersecurity, Digital Forensics, or a related field. ✓ 3–5 years of hands-on digital forensics and incident response experience, preferably in banking or financial services. ✓ Proficiency with forensic tools: EnCase, FTK (Forensic Toolkit), Magnet AXIOM, Autopsy, or equivalent. ✓ Experience with memory forensics tools and network forensics. ✓ Strong knowledge of Windows and Linux operating systems, file systems (NTFS, ext4), and artifact locations. ✓ Familiarity with cloud forensics on AWS, Azure, or GCP (CloudTrail, Azure Monitor, GCS audit logs). ✓ Understanding of malware analysis techniques, sandbox environments, and reverse engineering basics. ✓ Excellent report writing skills with experience preparing evidence-grade documentation for legal or regulatory purposes.
e)	Network Security	JOB DESCRIPTION: ✓ Monitor network traffic, firewall logs, IDS/IPS alerts, and SIEM dashboards for suspicious activity and security incidents. ✓ Investigate and respond to network security alerts, perform root-cause analysis, and document findings with remediation actions. ✓ Configure, manage, and optimize firewalls, VPNs, NAC, and network segmentation policies aligned with banking security standards. ✓ Conduct regular vulnerability assessments and penetration tests on network infrastructure; coordinate patching with IT teams. ✓ Ensure compliance with RBI guidelines, ISO 27001, PCI-DSS, and internal information security policies.

		✓ Participate in change management processes to review network architecture changes from a security perspective. ✓ Prepare and present network security reports and KPIs to senior management on a regular basis. ✓ Mentor junior analysts and contribute to threat intelligence sharing within the security team. REQUIREMENTS: ✓ Bachelor's degree in Computer Science, Information Technology, or a related field. ✓ 3–5 years of hands-on experience in network security within a banking or financial services environment. ✓ Strong knowledge of TCP/IP, OSI model, network protocols, and enterprise network architecture. ✓ Experience with SIEM platforms, IDS/IPS, and firewall management (Cisco ASA, Fortinet). ✓ Familiarity with RBI cyber security framework, PCI-DSS, and ISO 27001 compliance requirements. ✓ Hands-on experience with vulnerability scanners (Nessus) and network analysis tools (Wireshark, NetFlow). ✓ Understanding of Zero Trust architecture, network segmentation, and micro-segmentation concepts. ✓ Strong analytical, problem-solving, and incident documentation skills. .

Rules and Regulations

1. Only shortlisted applicants will be contacted.
2. Selected candidates will enter into an Employment Agreement containing *inter alia* Code of Conduct and Non-disclosure agreement.
3. Interested candidates may submit their application through the link provided on the Careers page of the Institute's website, along with an updated CV, a recent photograph, a valid identification document (such as an Aadhaar Card), and a cover letter highlighting their suitability for the position. Alternatively, candidates may apply by ☛ ***clicking here***.
4. Queries if any may be sent **pragati@idrbt.ac.in**.
5. The preliminary scrutiny of the candidature and suitability will be considered on the strength of the information submitted in the Application.