सिक्योरिटी प्रिंटिंग एंड मिंटिंग कॉरपोरेशन ऑफ इंडिया लिमिटेड
Security Printing and Minting Corporation of India Limited
मिनीरत्न श्रेणी-I, सीपीएसई/Miniratna Category-I, CPSE
भारत सरकार के पूर्ण स्वामित्वाधीन/Wholly owned by Government of India

Advt. No. 01/2026

Date: 07.02.2026

"Requirement of Young Professional in the area of Cyber Security on fixed term contract basis"

Security Printing & Minting Corporation of India Limited (SPMCIL) is a Miniratna Category – I Central Public Enterprise wholly owned by Government of India. It started functioning as a Corporatized entity with effect from 13th January, 2006 under the administrative control of Department of Economic Affairs, Ministry of Finance. The principal activity/business of the Company is designing and manufacturing of security papers, Printing of Currency notes, Passports, non-judicial stamp papers, postage stamps, Minting of the Coins etc.

The Operational units of the Company are strategically located across the Country having its four Mints at Mumbai, Kolkata, Hyderabad and Noida, four Currency/Security presses at Nashik, Dewas and Hyderabad, besides a high-quality Paper manufacturing mill at Narmadapuram.

SPMCIL invites application from qualified professionals with domain-specific expertise (i.e. experienced cyber security experts) on competitive and industry-aligned terms, thereby ensuring efficient, secure, and professional execution of responsibilities. Such officers will be appointed as Young Professional – Cyber Security Experts, as per requirement, on contract basis at its Unit located in Data Center, Noida and Disaster Recovery Center, Hyderabad. The details of the eligibility criteria for the assignment, compensation payable etc. are given below:

Post	**Requirement (in Number)**	**Post Qualification Experience**	**Remuneration**	**Maximum Age (as on 07.02.2026)**
Young Professional – Cyber Security	03 (02 at Data Center, Noida and 01 at Disaster Recovery Center, Hyderabad)	Min five (05) years relevant (Cyber Security) experience in reputed company	Rs. 50,000/- (all inclusive)	35 years

Essential Qualification:

1. 1st class Full Time B.E./B.Tech from recognized University/Institute in Computer Science/Information Technology/Electronics & Communication Engineering discipline with minimum 60% marks or equivalent CGPA.
2. Certifications in any one of CEH (Certified Ethical Hacker)/CCSP (Certified Cloud Security Professional)/ Certified Cloud Security Professional (CCSP)/CISSP/CompTIA CySA+/GSEC/OSCP (Offensive Security Certified Professional)/CISM

Preference to be given to those who have specialization in Cyber Security at Post Graduate level.

General Conditions: Young Professionals would be engaged for a fixed period for providing high quality services and for attending to specific and time-bound jobs. The appointment will be full -time basis and they would not be permitted to take up any other assignment during the period of engagement with SPMCIL. The engagement is of a temporary (non-official) nature and can be cancelled at any time without assigning any reason. The engagement does not confer any right whatsoever for any future regular employment in SPMCIL and should be treated as fixed term contract engagement only.

Tenure of Engagement: The tenure of Young Professional (Cyber Security) will be for the period of 3 years, however based on the performance it can be terminated or further extended.

Duties and Responsibilities:

a) Security Architecture and Design

- Develop and maintain a robust cyber security architecture aligned with industry standards (e.g. NIST, ISO 27001) and industry best practices.
- Design and implement secure solutions for network segmentation, threat detection, and incident response across IT and OT environments.
- Collaborate with IT and OT teams to integrate cyber security controls into existing and upcoming systems.
- Stay updated on emerging security threats, vulnerabilities, and technologies, and recommend enhancements to security infrastructure.

b) Vulnerability Management

- Conduct regular vulnerability assessments and penetration testing of IT and OT systems and networks.
- Develop and oversee remediation plans for identified vulnerabilities.
- Coordinate with internal teams and vendors for timely application of patches and system updates.

c) Threat Detection and Incident Response

- Implement and continuously monitor security tools (e.g. IDS/IPS, SIEM) to detect anomalies and potential threats.
- Lead cyber security incident response activities, ensuring prompt containment, mitigation and post-incident analysis.
- Develop and maintain incident response playbooks and conduct forensic investigations when required.

d) Risk Management and Compliance

- Perform cyber risk assessments to identify threats and evaluate their impact on operations.
- Ensure adherence to relevant national and international standards, guidelines, and data protection laws (e.g., CERT-In guidelines).
- Develop, update, and enforce cyber security policies, procedures, and standards.
- Lead internal audits and report findings to senior management.

e) Awareness and Training

- Design and deliver cyber security awareness programs for staff, contractors, and third-party vendors.
- Create security campaigns and materials to cultivate a security-aware culture across the organization.

f) Collaboration and Reporting

- Coordinate with IT, OT, and functional departments to implement and maintain a secure operational environment.
- Prepare and present reports on risk posture, ongoing threats, and mitigation strategies to senior management.

Skill Set Requirements:

- Strong knowledge of cyber security concepts, principles, and frameworks (e.g. NIST, ISO 27001, CIS Controls).
- Hands-on experience with security technologies such as:
    - Firewalls, IDS/IPS, endpoint protection platforms
    - SIEM tolls (e.g. Forti SIEM)
    - Vulnerability scanners (e.g. Nessus, Qualys)
- Proficiency in risk assessment methodologies and compliance frameworks.
- Strong problem-solving, analytical, and incident handling skills.
- Effective communication skills, capable of conveying complex technical details to both technical and non-technical stakeholders.

Various Entitlements/Service Conditions:

(i) **Leave**: He/She shall be eligible for one day paid leave for every 20 days of work. The leave may be availed with the prior approval of the controlling officer only after it actually becomes due and not in advance/anticipation.

(ii) **Increment**: He/She shall be entitled to 8% annual increase in his/her remuneration.

(iii) **TA/DA**: No TA/DA shall be admissible for joining the assignment or on its completion. However, in the course of performing professional duties, if he/she is deputed to out station Units, the admissible TA/DA will be at par with E-1 level Officer of SPMCIL.

(iv) **Medical**: He/She shall be entitled for reimbursement of premium for Mediclaim Policy upto Rs. 2 Lacs from a PSU Insurance Company for self, spouse and dependent children for the period of engagement exceeding 6 months. No other medical benefits shall be available.

(v) **Other allowances**: No other facilities like DA, accommodation, telephone, conveyance/transport, personal staff, medical reimbursement, etc, would be admissible.

Selection Process:

After receipt of applications and scrutiny, the candidates will be provisionally shortlisted for the screening process based on the merit i.e. qualification and experience profile. This screening will be subject to their fulfilling the eligibility criteria based on the documents (educational/experience etc.) produced at the time of screening. The screening process may consist of written test followed by Interview or only Interview which will be decided by Management based on number of applications received.

How to Apply:

All willing and interested candidates can apply online on SPMCIL website www.spmcil.com. The link will remain open from **07/02/2026** (10.00 AM onwards) to **06/03/2026** (upto 05:00 PM) and no other mode of application will be accepted. Candidates are requested to go to the SPMCIL website www.spmcil.com, click on the "Career" link and click on the "ONLINE APPLICATION" button provided on the page.

After submitting the details in the online application form, please wait for the intimation from the server, do not press back or refresh button. Candidates are required to keep a printout of the online Application Form facilitated in the Application Form page.

The applicants are requested to keep checking the Company's website www.spmcil.com for any information regarding issue of interview call letters/schedule of interview/selection process etc. which shall appear at www.spmcil.com.