F5.502 (1442)/DoIT&C/2025-13096-8832250 /DOIT/BSDC-299

Government of Rajasthan

(Department of Information Technology & Communication) Date: 31/12/2025

IT Building, Yojana Bhawan Campus,Tilak Marg, C-Scheme, Jaipur-302005

Vacancy Notice

Subject: Invitation of applications for deputation to the Rajasthan State Computer Security Incident Response Team (R-CSIRT), Jaipur, Rajasthan.

The Rajasthan State Computer Security Incident Response Team (R-CSIRT), being established under the Department of Information Technology & Communication (DoIT&C), Jaipur, will serve as the state-level nodal agency for managing, coordinating, and responding to cybersecurity incidents across all Government Departments, Critical Information Infrastructure (CII) sectors, and strategically important private organizations.

DOIT&C hereby invites applications from eligible officers for filling up the post of Director and Technical Lead- Incident Response (IR) in the Rajasthan State Computer Security Incident Response Team (R-CSIRT), Jaipur, Rajasthan on a deputation basis.

1. Responsibilities:

Director- CSIRT

- Head of the organization and responsible for all operations, implementation and scaling up the State CSIRT.
- Take charge of overall implementation and operationalization of the project. Management of the administrative and technical process.
- Manage and increase the effectiveness and efficiency of operational teams through improvements to each function as well as coordination and communication between various groups/activities
- Reports to appropriate authority in the Nodal Ministry.

Technical Lead (Incident Response):

- Providing a focused management and delivery approach across relevant areas of incident detection, response, containment, mitigation and post incident learning. Ensuring that proper operational procedures and practices are in place and are being enforced effectively for timely resolution of cyber security incidents reported to and tracked.
- Continuous improvement of operational systems, processes and policies.
- Coordination of activities related to implementation of solutions and systems for keeping track of latest cyber threats and devising mitigation measures.
- Identifying and scheduling of personnel, systems and functions and ensuring procedures and protocols are being followed to enable timely and effective response to detected events, incidents, malware/botnet reports, threat intelligence reports, and inputs from various sources such as CERT-In, other State CSIRTs, cyber security industry reports, notifications of stakeholders, security researchers, LEAs and ISPs.

- Acting as an escalation point for timely notification and seek guidance from Head (Operations) and Director for containment and resolution of critical incidents.
- Provide continuous assistance to Head Operations in long-term planning of solutions, systems and controls including an initiative geared toward operational excellence.
- Coordinating with other stakeholders recording and reporting security incidents particularly containing and remediating emerging cyber threats.
- Create and maintain procedural documentation supporting the on-going threat intelligence and coordination activities.
- Review and finalisation of daily/weekly/monthly reports.
- Reports to Head (Operations)

2. Eligibility Criteria

The details and eligibility criteria for the said posts are as follows:

Post	No. of Vacancy	Eligibility Criteria	Skills and Experience
Director (Pay matrix Level 24)	1(One)	**Serving or Retired Technical Officer** from any State/Central Government department or PSU, including but not limited to: C-DAC, NIC, NICSI, MeitY, DoIT&C, NIELIT, CERT-IN, BEL, ECIL, RISL, DRDO, ISRO, IRDAI, RBI, Public Sector Banks, and other relevant organizations with significant cybersecurity operations and expertise suggested by CERT-In.	• 20 years of technical experience and administrative experience. • Experience in cyber security domain in senior management level.
Technical Lead– Incident Response (IR) (Pay matrix Level 20)	1(One)	**Serving or Retired Technical Officer** from any State/Central Government department or PSU, including but not limited to: C-DAC, NIC, NICSI, MeitY, DoIT&C, NIELIT, CERT-IN, BEL, ECIL, RISL, DRDO, ISRO, IRDAI, RBI, Public Sector Banks, and other relevant organizations with significant cybersecurity operations and expertise suggested by CERT-In.	• 8 years of experience • SOC operations • Incident handling • Malware Analysis • Cyber Forensics • Network security (firewalls, UTM, IPS, Proxy, SIEM etc) • Log analysis

3. Terms and Conditions of Deputation

1. The period of deputation shall be initially for two years which can be further extended to one year.
2. Recruitment, appointment, salary, allowances, joining time, medical facilities, travelling allowance, and all other service conditions shall be governed by the relevant provisions of the Rajasthan Service Rules (RSR), the Rajasthan Civil Services (Classification,

Control & Appeal) Rules, the Rajasthan Civil Services (Revised Pay) Rules, and any other applicable service rules or orders issued by the Government of Rajasthan from time to time.

3. Leave shall be regulated in accordance with the provisions of the Rajasthan Service Rules (RSR).
4. Subject to the above rules, the terms and conditions of deputation shall be governed by the Rajasthan Civil Services (Deputation of Government Servants) Rules and other relevant instructions/guidelines issued by the Government of Rajasthan from time to time.
5. In cases where the appointment is made from an organization whose pay structure or Dearness Allowance pattern differs from that of DoIT&C, only the basic pay shall be protected. Perquisites shall not be protected, in accordance with the Rajasthan Civil Services (Revised Pay) Rules.

4. Application Procedure

1. Eligible and interested candidates may submit their applications in the prescribed format as provided in Annexure–I.
2. The application must be sent to the email ID rsoc@rajasthan.gov.in.
3. In case the applicant is currently in service, application shall be forwarded through the parent department.
4. Applications, complete in all respects and accompanied by all requisite documents, must be received by email within 30 (thirty) days from the date of publication of the vacancy notice in the Newspaper.
5. Only applications that are complete in all respects and duly supported by the prescribed documents shall be considered for appointment on a deputation basis. Incomplete applications, applications not accompanied by the required documents, or those received after the prescribed date shall not be considered.
6. The appointment shall be made on a deputation basis for a period of two years. The maximum age for appointment on deputation shall not exceed 66 years as on the closing date for receipt of applications.

The Authority reserves the right to withdraw this notice at any time, without assigning any reason.

(Mukesh Kumar Sharma)
Additional Director

Copy to:

1. PS to Secretary, DoIT&C
2. Sr. PS to Commissioner and Special Secretary, DoIT&C
3. Joint Secretary, DoIT&C
4. OIC- Website, DoIT&Cand RISL to upload the Vacancy Notice on departmental websites.

Additional Director

Annexure-I

APPLICATION FORM

(For Deputation Posts in R-CSIRT)

---

1. Post Applied For: -

- Name of the Post: _____
- Organization: Rajasthan Computer Security Incident Response Team (R-CSIRT)
- Department: Department of Information Technology & Communication (DOIT&C), Govt. of Rajasthan
- Vacancy Notice No. & Date: _____

---

2. Personal Details: -

Detail	**Information**
Full Name (in Block Letters)	_____
Father's / Mother's / Spouse's Name	_____
Date of Birth (DD/MM/YYYY)	_____
Age (as on closing date)	_____
Gender	☐ Male ☐ Female ☐ Other
Nationality	_____
Category	☐ General ☐ SC ☐ ST ☐ OBC ☐ EWS ☐ Other

---

3. Present / Last Employment Details: -

Detail	**Information**
Name of Present / Last Dept. / Organization	_____
Designation at Present Post / Retirement	_____
Pay Level / Last Pay Drawn	_____
Date of Retirement (if applicable)	_____
Total Length of Service (Regular)	_____
Holding analogous post before retirement?	☐ Yes ☐ No

---

4. Contact Details: -

Detail	**Information**
Office / Last Office Address	_____
Residential Address	_____
Mobile Number	_____
Email ID	_____

5. Educational Qualifications: -

SN.	Degree / Diploma	Board / University	Year of Passing	Specialization	Percentage / CGPA

6. Technical / Professional Qualifications: -

(Details relevant to Cyber Security / IT /CERT/CSIRT Operations, etc.)

_____

_____

_____

_____

_____

_____

_____

7. Experience Details: -

SN.	Organization	Post Held	Period (From–To)	Pay Scale	Brief description of Nature of Duties

---

8. Special Skills / Expertise: -

(Incident Response, SOC Operations, Malware Analysis, Network Security, Digital Forensics, CERT/CSIRT Operations, etc.)

_____

_____

_____

_____

_____

_____

---

9. Vigilance / Disciplinary Status: -

1. Any disciplinary/vigilance case pending or contemplated? ☐ Yes ☐ No
   (If yes, details: _____)
2. Any penalty has been imposed on the officer during the last10 years? ☐ Yes ☐ No
   (If yes, details: _____)
3. Whether applicant is under suspension: ☐ Yes ☐ No

---

10. Documents Enclosed: -

☐ Application forwarded through proper channel (for serving employees)

☐ Cadre clearance / NOC (if applicable)

☐ Vigilance clearance / Certificate of Clean Record

☐ ACRs/APARs of last 5 years (if applicable)

☐ Educational & technical qualification certificates

☐ Experience certificates

☐ Retirement / Pension Certificate (for retired employees)

☐ Any other relevant document: _____

---

11. Declaration: -

I hereby declare that the information furnished above is true and correct to the best of my knowledge and belief. I understand that in the event of any information being found false or incorrect, my candidature for deputation in R-CSIRT is liable to be rejected.

Place: _____

Date: _____

Signature of Applicant: _____

---

12. Certification by Parent Department / Last Employer: -

Certified that the particulars furnished by the applicant are correct. It is also certified that no vigilance/disciplinary case is pending or contemplated against the applicant and that the applicant will be relieved in the event of selection (for serving employees).

Signature: _____

Name & Designation: _____

Office Seal: _____

Date: _____