WE'RE HIRING

Role: Manager – Information Security
Department: Technology
Location: Mumbai

B A R C
BROADCAST AUDIENCE RESEARCH COUNCIL INDIA
What India Watches™

Job Role:

Lead and oversee our organization's information security efforts. Responsible for developing and implementing information security policies, procedures, and strategies to safeguard our organization's sensitive data, systems, and infrastructure from cybersecurity threats.

Job Responsibilities:

1. Security Strategy and Planning:

- Develop and maintain the organization's information security strategy, including short-term and long-term goals.
- Create and implement security policies, standards, and procedures to protect data, systems, and networks.
- Collaborate with senior management to align security initiatives with business objectives.

2. Security Risk Management:

- Identify and assess information security risks, vulnerabilities, and potential threats.
- Develop and maintain a risk management program, including risk assessments and mitigation plans.
- Stay updated on emerging threats and vulnerabilities and adjust security measures accordingly.

3. Security Operations:

- Oversee the day-to-day security operations, including monitoring, incident response, and security incident handling.
- Manage security tools and technologies, ensuring their effectiveness and relevance.
- Coordinate security awareness and training programs for employees.

4. Compliance and Governance:

- Ensure compliance with industry regulations, such as GDPR, HIPAA, and other relevant data protection laws.
- Collaborate with legal and compliance teams to address legal and regulatory requirements.
- Facilitate security audits and assessments.

5. Security Projects and Initiatives:

- Lead and manage security projects, such as network security upgrades, encryption initiatives, and security awareness campaigns.
- Develop and manage the security budget and allocate resources effectively.

6. Security Incident Response:

- Establish an incident response plan and lead the organization's response to security incidents.
- Conduct post-incident reviews and implement measures to prevent future incidents.

7. Vendor and Third-Party Security:

- Evaluate and monitor security practices of third-party vendors and service providers.
- Ensure that vendor contracts include appropriate security clauses and requirements.

8. Team Management:

- Recruit, train, and lead a team of information security professionals.
- Foster a culture of security awareness and responsibility within the organization.

Job Requirements:

- Bachelor’s degree in information security, Computer Science, or a related field. Master's degree is a plus.
- Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or other relevant certifications.
- A minimum of 8 years of experience in information security management.
- In-depth knowledge of security frameworks and standards (e.g., NIST, ISO 27001).
- Strong understanding of IT infrastructure, network security, and cloud security.
- Excellent communication and interpersonal skills.
- Proven ability to lead and manage a team effectively.