NaBFID | National Bank for Financing Infrastructure and Development

About NaBFID

National Bank for Financing Infrastructure and Development (NaBFID) has been set up under an Act of Parliament (NaBFID Act, 2021), as the principal entity for infrastructure financing in the country. The entity is regulated and supervised as an All-India Financial Institution (AIFI) by the Reserve Bank of India (RBI). NaBFID is poised to play an extremely crucial role in supporting infrastructure funding by driving the development of innovative financing instruments and development of bond and derivatives markets and promoting best practices in financing and data-driven risk management.

NaBFID is looking to hire a strong leadership team, committed to the cause for which NaBFID is set up and to help with the national agenda, inviting applications for role of ***Chief Information Security Officer****”.*

Job Profile

S/he will be responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems, and assets from both internal and external threats. He/she is also responsible for responding to data breaches and other security incidents.

Job Title	**Chief Information Security Officer**	**Grade**	VP
Department	Information Security	**Reporting To**	Head - Risk Management
Location	Mumbai	**Team**	To be built
Age	55 years and below (As on date of advertisement)		

Primary Job Duties/Responsibilities

The key job duties/responsibilities are enumerated below:

- Creating and implementing a strategy for the deployment of information security technologies and solutions to minimize the risk of cyber incidents.
- Preparing information security policy, cyber security policy and cyber crisis management plan.
- Driving and ensuring compliance to the extant regulatory instructions on information/ cyber security.
- Coordinating in assessing Business Impact Analysis of various IT assets and deriving respective RTO and RPO for each asset.
- Ensuring that current and emerging cyber threats to the financial sector and the Bank’s preparedness in these aspects are discussed in ISC and other related Committees.
- Developing cyber security KRIs and KPIs.
- Placing a review of cyber security risks/ arrangements/ preparedness of the Bank before the Board/ Board level Committee on a quarterly basis.
- Spearheading implementation of security standards/ IT control frameworks (such as ISO 27001) for critical IT functions.

- Conducting Vulnerability Assessment/ Penetration Testing (VA/ PT) of the IT assets (applications, systems and infrastructure) throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.)
- Managing the daily operation and implementation of the IT security strategy
- Conducting a continuous assessment of current IT security practices and systems and identifying areas for improvement
- Solving network related queries and problems satisfactorily, in a timely manner
- Direct significant effort into IT asset management, involving hardening, tagging, tracking, and auditing all IT assets across NaBFID
- Developing strategies to handle security incidents and trigger investigation
- Delivering new security technology approaches and implementing next generation solutions
- Overseeing the management of the IT security department, giving leadership to the team, and developing staff capabilities
- Ensuring adherence to the latest regulations and compliance requirements
- Running security audits and risk assessments
- Developing, implementing and testing of business continuity plans
- Planning and executing periodic disaster recovery drills / simulation exercises in order to establish the adequacy of the Business Continuity Plan
- Periodically communicating updates relating to IT and cyber security to various stakeholders internally & externally; viz., Board of Directors, senior management team, team members, colleagues of other departments etc.
- Must work to integrate the security requirements with IT and business requirements
- Insure against cyber risks and protect the organization from potential liabilities to the extent possible
- Handling IT related compliance issues and ensuring that the organization follows rules and standards
- Software Development Lifecycle (SDLC) Audit and periodic Code Reviews to ensure that applications continue to be secure
- Information Security Audit of IT Systems and controls
- Issuing and periodic review of device hardening guidelines, patch management guidelines, anti-virus / malware guidelines, User Access Management guidelines, privilege access management guidelines, end point management guidelines, connectivity guidelines for trading partners and external agencies, controls on mobile devices and wireless technology
- Developing and Implementation of scenario-based Incident response plans to deal with cyber crisis, contingencies and disasters, attacks on IT systems etc.
- Escalating and reporting the incidents to the Board and Senior Management and pro-actively notify CERT-In and RBI regarding cyber security incidents, as per regulatory requirements.
- Ensuring security review of all applications / change requests before go-live / production release
- Preparing, maintaining and review of IS Policy
- Managing and monitoring SOC and drive cyber security related projects
- Maintain and monitor on regular basis the threat landscape of the Bank
- Ensuring conduct of periodic tests to evaluate the adequacy and effectiveness of security control measures
- Any other assignment as may be assigned by the Bank from time to time

Professional Experience

- Minimum 15 years of experience; of which 10 years in Banking - IT related areas / projects involving IT Policy and Planning / Financial Networks and Applications / Financial Information Systems / Cyber Security Technologies / Payment Technologies; of which at least 5 years of experience in Information Security.
- Knowledge of common information security management frameworks, such as ISO/IEC 27001
- Innovative thinking and leadership with an ability to lead and motivate cross-functional and interdisciplinary teams.

Educational Qualifications

Engineering Graduate / post-Graduate in related field such as Computer Science, IT, Electronics and Communications or a Cyber Security related field or MCA or equivalent qualification from recognized University/ Institution.

Preferred: Certified Information Systems Security Professional (CISSP) /Certified Information Security Manager (CISM)/ Certified Chief Information Security Officer (CCISO) / Certified Information Systems Auditor (CISA)

Term

Contractual Engagement will be for a minimum of 3 years to maximum of 5 years, which may be renewed for additional term at the discretion of NaBFID.

Remuneration

Remuneration will be offered based on qualification, experience, suitability, last drawn salary, and market benchmark and shall not be a limiting factor for suitable candidates.

Interested candidates (Indian Citizens) may send their CVs (including a passport sized photograph) via email to *recruitment@nabfid.org.* ***The subject line should STRICTLY be APPLICATION FOR THE POST OF <Job Code>"***.
All applications will be held in strict confidence and should be received on or before 25-July-2023 by 06:00 pm IST.

Selection will be solely at the discretion of NaBFID's Selection Committee, and their decision will be final.