Job Description

POSITION DETAILS			
Functional Designation	Chief Information Security Officer	**Department**	Information Security
Sub Department	Information Security	**HR Grade**	Vice President
Location	Corporate Office	**Reporting Manager**	

Job Purpose

The Vice President and Chief Information Security Officer are pivotal in safeguarding the NBFC's information and technology assets, reducing cybersecurity risks, and ensuring compliance with regulations. This position requires strong leadership, cybersecurity expertise, and a deep understanding of the financial industry's specific security challenges.

Principal Accountabilities

1. Information Security Strategy: Develop and implement the company's information security strategy, aligning it with business objectives.

2. Cybersecurity Leadership: Lead the information security team, providing guidance, mentorship, and resource management.

3. Risk Assessment: Identify, assess, and prioritize information security risks, including cyber threats, data breaches, and vulnerabilities.

4. Security Policies and Procedures: Establish and enforce security policies, procedures, and best practices to protect the company's data and technology infrastructure.

5. Regulatory Compliance: Ensure that information security practices and policies comply with relevant regulations, such as data protection laws and financial industry standards.

6. Security Awareness Training: Develop and conduct security awareness programs to educate employees on cybersecurity best practices.

7. Incident Response: Develop and manage an incident response plan to address security breaches and data incidents, including communication with stakeholders and authorities.

8. Security Audits and Assessments: Oversee regular security audits, vulnerability assessments, and penetration testing to identify and address weaknesses.

9. Threat Detection and Prevention: Implement advanced threat detection and prevention systems to safeguard against cyber threats and intrusions.

10. Data Protection: Ensure the protection of sensitive data through encryption, access controls, and data loss

prevention measures.

11. Security Architecture: Design and maintain a secure technology architecture, including firewalls, intrusion detection systems, and security information and event management (SIEM) systems.

12. Vendor Security: Evaluate and manage the security of third-party vendors and partners with access to the NBFC's data and systems.

13. Disaster Recovery and Business Continuity: Develop and maintain disaster recovery and business continuity plans to minimize downtime in case of security incidents.

14. Budget Management: Manage the budget allocated for information security operations efficiently.

15. Security Reporting: Provide regular reports to senior management and the board of directors on the state of information security, ongoing initiatives, and areas for improvement.

16. Compliance and Ethical Hacking: Ensure ethical hacking and penetration testing are conducted to identify security vulnerabilities.

17. Emerging Threats and Technologies: Stay updated on emerging cybersecurity threats and technologies to adapt security strategies accordingly.

Desired Profile

A bachelor's degree in a relevant field such as Information Security, Computer Science, or Cybersecurity is often a minimum requirement.
Many CISOs hold a master's degree (e.g., MSc or MBA) in Cybersecurity, Information Assurance, or a related discipline. An advanced degree can be an advantage.
This is a widely recognized certification for information security professionals and is often required or preferred for a CISO role.
This certification demonstrates expertise in information security management and governance, which is crucial for a CISO.