# Job Description

| | |
|---|---|
| Position: | **Head, Information Technology Security** |
| Department: | IT Security and Compliance Office |
| Reporting to: | Chief Information Technology Officer |
| Location: | Head Office |

## I. Duties and Responsibilities

### a. Information Security Governance and Strategy

- Chair & lead the Information Security Committee based on the defined & approved charter.
- Define and maintain the SBILH Bank's Information Security Strategy aligned with business objectives and regulatory expectations.
- Establish and oversee the Information Security Management Framework (ISMF).
- Develop, review, and enforce information security policies, standards, procedures, and guidelines.
- Ensure clear segregation of duties between IT operations, system development, and information security.
- Provide regular reporting to senior management and committees on security posture, risks, and key issues.

### b. Regulatory Compliance and Policy Alignment

Ensure full compliance with:

- NBC Technology and Cyber Risk Management Guidelines (TCRMG).
- Relevant regulations and directives issued by MPTC.
- Relevant requirements from other Cambodian government ministries and authorities.
- Coordinate regulatory inspections, reviews, and follow-ups related to information security.
- Translate regulatory requirements into practical, enforceable security controls.
- Ensure timely remediation of regulatory findings and audit observations.

### c. Risk Management and Control Oversight

- Identify, assess, and monitor information security risks across applications, infrastructure, data, and third parties.
- Define and maintain security controls aligned with the SBILH Bank's risk appetite.
- Participate in enterprise IT risk assessments and technology change reviews.
- Ensure appropriate security risk treatment plans are implemented and tracked.
- Support operational risk management and reporting.
- Support Risk Management Committee (02nd line of defend) from 01st line of defend aspect.

### d. Security Operation and Incident Management

- Establish and oversee security monitoring, detection, and incident response processes.
- Lead response to information security incidents, including cyber incidents and data breaches.
- Ensure proper incident escalation, investigation, root cause analysis, and corrective actions.
- Coordinate with regulators and authorities where required during major security incidents.
- Conduct regular security drills, tabletop exercises, cyber security simulation, and awareness campaigns.

### e. Technology, System and Data Security

Oversee security architecture and controls for:

- Core banking systems (CMS, CBS).
- Digital banking channels.
- Payment systems.
- Data platforms and integration layers.
- Ensure secure system development practices (in coordination with DevSecOps and System Development teams).
- Review and approve security requirements for new systems and technology changes.
- Ensure data protection, access control, encryption, and logging mechanisms are in place.

### f. Third Party and Vendor Security

- Define and enforce third-party information security requirements following NBC TCRMG.
- Conduct security risk assessments of vendors, service providers, and outsourcing partners.
- Ensure contracts include appropriate security, confidentiality, and audit clauses.
- Monitor vendor compliance and remediation of security gaps.

### g. Security Awareness, Training and Culture

- Promote a strong information security culture across the SBILH Bank.
- Ensure regular security awareness training for staff and management.
- Advise business units on secure use of technology and data.
- Act as trusted advisor on information security matters.
- Other tasks assigned by the line manager.

## II. Qualification

- Bachelor's degree in Information Security/Cyber Security, Computer Science, Information Technology or related field.
- Master's degree in computer science or equivalent is an advantage.
- Professional Certifications (Strong Advantages).
- CISSP, CISM, CISA, CRISC or equivalent internationally recognized certifications.
- ISO/IEC 27001 Lead Implementer/Lead Auditor is an advantage.
- Minimum 8-10 years of experiences in Information Security, IT Risk, or Technology Risk Management.
- At least 3-5 years in a senior leadership or head-level role, preferably within banking and financial services.
- Proven experience working in a well rounded regulated financial institute.
- Experience in working with senior management, management committee, auditors and regulators.
- Hands-on experience in managing regulatory compliance, audits, and inspections.
- Strong exposure to cyber security, data protection, and incident management.
- Experience in secure SDLC implementation.
- DevSecOps practitioner.
- Strong knowledge of (NBC TCRMG, MPTC ICT and Cybersecurity related regulations and other relevant regulatory requirement).
- A very good understanding of global standards and frameworks such as: ISO/IEC 27001/27002, NIST Cybersecurity Framework, COBIT, ITIL (security and incident aspects), PCI Security Standards Council.
- Strong leadership skill, integrity and independent judgement.
- Ability to communicate complex security risks in business terms.
- Skill in implementing DevSecOps process & practice.
- Solid understanding of application security, vulnerability management, and secure SDLC.
- High commitment and be willing to work under pressure.