POSITION DESCRIPTION

Position title:	**Information Security Manager**
Location:	**Head Office**
Reports to:	Chief Information Officer
Entities:	GMHBA
Organisational level:	Manager
Reports:	1 Direct reports

Job Purpose:

The Information Security Manager manages GMHBA Information Security and compliance to APRA CPS234 under delegation from the CIO and manages ITSG responsibility and compliance to the GMHBA Risk Management Framework.

Accountabilities:

Strategy & Leadership

- As a member of the Leadership team, contribute to setting and delivery of the GMHBA's overall strategic plan and objectives.
- Set and deliver strategic and annual plans for Information Security to support the delivery of the overall GMHBA strategy and plans.
- Design and implement the Information Security System, in conjunction with key stakeholders. This includes framework design, system design, policies, standards, and end-to-end processes.
- Ensure resourcing, performance and bench strength of the team is aligned to deliver plans. Anticipate future skill requirements and acquire and develop these in appropriate time frames.
- Participate on committees, internal and external, as required.
- Collaborate and seek input from specialist functions and others as required, to maximise performance outcomes.
- Be a role model and ambassador to others in setting, and upholding, the company values, culture and performance standards.

Information Security Management System and CPS234 Regulation Compliance

- Manage the ISMS under delegation from CIO working with external security specialists as appropriate.

- Review the Threat Risk Assessment of systems and processes with Managers of IT and all relevant stakeholders, such consulting services, Vendors, Online Applications, Operations, Application Architect, Business development and Marketing and Digital inclusion
- Work with functional departments to address ISMS requirements and achieve compliance, ensuring all ISMS activities are carried out consistently.
- Develop the GMHBA Information Security Policy and procedures and ensure appropriate testing and auditing of Information Security policy controls
- Manage and execute on the Information Security calendar of events.
- Manage and review all security exemptions.
- Providing information in relation to the ISMS to the CIO for management review.
- Build security awareness in the organisation and communicate governance and compliance objectives to ensure an appropriate compliance and risk aware culture.

Information Security Reporting

- Manage the Information Security Steering committee agenda to allow for effective understanding and decision making and maintain an open channel of communication with the Information Security Steering Committee.
- Providing the Information Security Committee with high level results of comprehensive risk assessments and business impact analysis (BIA).
- Provide effective reporting for the GMHBA board as determined by CPS234 regulation

Information Asset Management

- Classifying assets and ensuring information, business applications, information systems and networks are protected in line with their importance to the organisation.
- Enforcing asset protection policies and creating awareness on accountabilities and compliance needs.
- Owning and ensuring that threats and risk to assets are understood and mitigated to acceptable levels.
- Monitoring the state of safeguards implemented to protect assets.
- Determining which users are authorised to access information, computer systems and networks.
- Approving access privilege levels assigned to users or user groups in conjunction with the relevant system owners.
- Signing off on business security requirements relevant to their assets.

- Authorising changes to business applications, information systems and networks

GMHBA Risk Management Framework

- Ensure ITSG adherence to GMHBA risk management framework
- Managing the ITSG Operational Risk Register.
- Ensuring DR and Business Continuity Plans are documented and tested on a scheduled basis.

Regulatory and Reporting

- Manage Information Security audits and submit for all other as required.
- Manage ITSG audit recommendations and monitor remediation efforts, reporting progress to CIO and GMHBA GRC department.
- Ensure compliance with the Company's Delegated Authorities, Business Plan, Policies and Standards.
- Keep up to date with regulatory trends and changes, and ensure the company anticipates and navigates changes successfully.

Stakeholders & Advice

- Provide expert advice and recommendations to key stakeholders to facilitate understanding for robust decision making.
- Take opportunities to maintain positive and constructive relationships with regulators, auditors and other external stakeholders.
- Responsible for Information Security training and awareness across GMHBA.

Other

- Participate in the design, build and roll-out of business change programs designed to strengthen GMHBA's performance
- Embrace the mindset and actively contribute towards embedding the GMHBA Way including working in an Agile environment.
- It is not the intention of this position description to limit the scope or accountabilities of the position but to highlight the most important aspects of the position.
- The accountabilities described within may be altered in accordance with the changing requirements of the role.
- Perform 1st Line of Defence duties by identifying operational risks, investigating their root causes and provide support to mitigate risk through understanding control effectiveness and recommending risk improvement.

Review date: 09/08/2019
Approved by P&C Manager

Key Relationships:

Internal:

- Executives
- Senior Management
- Steering Committees
- Project Managers
- ITSG Leadership Team

External:

- IT Vendors
- Information Security Vendors
- Information Security public forums

Skills, Experience and Qualifications:

Mandatory

- Extensive IT security and risk experience within a regulatory, internal audit or compliance environment.
- Experience with the development of general controls and/or IT compliance related standards.
- Working knowledge and exposure of IT Governance, Risk and Compliance practices.
- Strong technical and analytical aptitude.
- Experience in developing and rolling out information security compliance programs using ISO 27001
- Experience in developing and rolling out PCI DSS compliance programs
- Experience in operating at Board and Executive level
- Bachelor's degree with emphasis in related field or equivalent experience.
- Certified Information Security Manager (CISM) Certification
- Certified Information System Security Professional (CISSP) Certification

Highly desirable

- Experience in private health insurance
- Experience working under APRA regulatory framework