Position Description

Information Security Analyst

September 2024

TEAM	REPORTS TO
Information Security & Data Governance	Information Security & Data Governance Manager
EMPLOYMENT TYPE	**DIRECT REPORTS**
Full time – permanent	Nil
LOCATION	**KEY CONTACT**
Flexible hybrid model - Primary location: Newborough/Melbourne office and working from home	Tim Brewer, Information Security & Data Governance Manager

WHO IS LATROBE?

At Latrobe, our people are at the heart of what we do. We are committed to creating an environment where diversity is celebrated, equity is achieved, and inclusion and belonging are prioritised and celebrated.

We're known for being the *health fund with heart* - a not-for-profit, regional private health insurer with more than 90,000 members across Australia. We support our members through the highs and lows of their health, and we give back to our community.

Our aspirational vision is to be the number one, member owned private health insurer in Australia. Our purpose is supported by 5 key values:

We display trust and respect always	*We focus on shared results*	*We engage & empower*	*We are accountable*	*We create a positive work environment*

POSITION OBJECTIVE

The Information Security Analyst role supports the delivery of the Information Security and Data Governance functions at Latrobe Health Services.

Working closely with the Data Governance Lead and Cybersecurity Lead, this role undertakes activities to identify and address risks associated with information security and data governance. The Information Security Analyst manages tooling, evaluates risks, and works with stakeholders across the business to remediate issues that arise. Core activities include evaluating and testing security controls, maintaining data inventories and lineages, and generating reports.

The role also fosters a strong risk culture by spreading knowledge of best practices through all levels of the business.

Position Description

REQUIREMENTS OF THE POSITION

Key duties and responsibilities

- Conduct and report on data governance impact assessments.
- Contribute to cybersecurity risk assessments, including third party risk assessments.
- Work with data owners and stewards to build and curate data inventory, including the data catalogue, critical data elements glossary and third-party register.
- Maintain definitions, metadata, data lineage, ownership, and usage patterns, while ensuring efficient data storage, access control, and security.
- Utilise various tools to support the operating effectiveness and continual improvement of Data Governance and Information Security maturity.
- Lead Information Security and Data Governance Service Desk activities by triaging and responding to incoming support requests and escalating where appropriate.
- Respond to Information Security and Data Governance incidents and requests for assistance in a timely manner.
- Provide Information Security and Data Governance training and support to Latrobe's staff.
- Conduct and report on security control effectiveness tests.
- Contribute to, and support the process for, information asset identification, classification and ownership.
- Stay up to date with changing cybersecurity trends and all applicable legislative requirements.
- Ensure the application of Latrobe information security and data governance standards and policies.

Leadership, teamwork and relationship building

- Model the Latrobe Way values and behaviours in the delivery of individual performance; actively contribute to a constructive, high performing team and organisational culture.
- Develop and maintain professional relationships with peers and stakeholders at all levels across the business to support inter-departmental collaboration.
- Independently prioritise work to support consistent achievement of individual and team key performance indicators; appropriately escalate issues impacting either performance and/or the business; and demonstrate a flexible, adaptable, mobile and energised (FAME) mindset.
- Be a highly effective team member and thought leader with energy, enthusiasm and creativity – able to work autonomously and as part of a team.

Accountability and extent of authority

- Ensure compliance with the Private Health Insurance Code of Conduct and applicable procedures are always maintained.
- Maintain knowledge of Latrobe's policies, processes and procedures and ensure all advice provided and processes undertaken are in accordance with the Private Health Insurance Act and Rules, the Private Health Insurance Code of Conduct, other relevant legislation, Latrobe's fund rules and current policies

- Actively maintain awareness of all risk and compliance obligations defined through Latrobe's Risk Management Framework.
- Consistently achieve individual goals and objectives and actively lead own growth and achievement planning and implementation.

Judgement and decision making

- Interpret and work within organisational policy and procedure and/or legislation applicable to the position.
- Actively offer and implement a course of action and solutions based on evaluation and analysis of numerical and written information focused on results.
- Make decisions which are objective and free from undue influence consistent with Latrobe's risk culture and approved strategic priorities and objectives.
- Make decisions consistent with Latrobe's operational delegations and delegate or escalate matters appropriately.

Experience skills and knowledge

- Strong interpersonal, relationship management, and communication skills.
- Experience managing technology platforms, including identity and access management (IDAM) controls and role-based access configuration (RBAC) controls. Power BI and cloud-based data governance tool (Informatica, Alation, Collibra) experience a plus.
- Strong experience with, and knowledge of, formal change management procedures.
- Excellent problem-solving and business analysis skills including the ability to analyse end-to-end processes to identify risks.
- Knowledge of cybersecurity concepts such as vulnerabilities, threats, risks, and controls, and how they interact in a complex technology ecosystem.
- Knowledge of cybersecurity frameworks and guidelines such as NIST and ISO 27001 and data governance frameworks and methodologies such as DAMA-DMBOK and NIDG.
- Tertiary qualifications in Information Technology or Cybersecurity, or equivalent experience desired.

Mandatory checks

- An Australian Police check will be conducted for all new employees to Latrobe Health Services prior to commencing in a role.
- Employment at Latrobe Health requires candidates to have Australian citizenship or to be a permanent resident of Australia or to have a valid visa that provides work rights in Australia.