IT and Cybersecurity Manager (12-month Contract)

About ClavystBio

ClavystBio is a life sciences investor and venture builder set up by Temasek to accelerate the commercialization of breakthrough ideas into health impact.

We invest and partner with innovators, entrepreneurs and founders to launch and grow global companies from Singapore. Our focus spans therapeutics, digital health and MedTech, with an emphasis on first-in-class science and technology.

Our collaborative space, Node 1, provides plug-and-play spaces for ventures that have graduated from incubators to progress to their next milestones. By bringing startups together, we foster a vibrant and supportive community.

Since our inception in 2022, ClavystBio has committed over US$220 million in investments in the life sciences sector.

For more information, please visit https://www.clavystbio.com/ and follow us on LinkedIn.

Job Summary

ClavystBio is looking for a IT and Cybersecurity Manager to oversee and execute ClavystBio's Data and Cybersecurity activities and projects. In this role, you will report to both the Chief Operations Officer and the Operations Lead, and work closely with the rest of the team.

Key Responsibilities

Data-related Special Projects

- Assess and improve ClavystBio's overall data strategy, systems development, and data management
    - Work with relevant Leads to analyse current and future business requirements for communication, data storage, management and analytics across investment and corporate development functions
    - Provide overall recommendation for ClavystBio's data infrastructure considering such requirements
    - Evaluate and assess current systems and applications used as well as other alternatives to provide a holistic recommendation on ClavystBio's data strategy going forward
    - Evaluate and implement solutions aligned with the overall data strategy, working with external service providers if necessary
    - Create detailed documentation of strategy and system design and communicate effectively with project teams and stakeholders
- Assess, develop and implement overall data access and governance framework in view of ClavystBio's data strategy
    - Assess, optimise, document and communicate Identity and Access Management (IAM) framework and policies for ClavystBio

- Set-up processes for tracking, managing (e.g. employee movements) and regular review of IAM
- Establish best practice data governance frameworks including data segregation, retention and lifecycle management

- Support relevant Leads in the implementation of priority data and knowledge management solutions identified such as a Customer Relationship Management System
  - Understand business needs and data-technology landscape and concepts (e.g. generative AI) to provide technology assessment and recommendation of available solutions
  - Co-create business-centric and/or automated processes to ensure data integrity, currency and reliability

IT and Cybersecurity

- Overall ClavystBio officer-in-charge to oversee and manage the organization's IT and cybersecurity efforts, which include prevention, monitoring, detection, and incident response to cybersecurity threats and intrusions
- Develop and implement ClavystBio's cybersecurity strategy, policies and procedures
  - Review existing IT policies and provide recommendations in line with industry best practices
  - Provide recommendations on IT security architecture including associated software
  - Ensure compliance with cybersecurity regulations and standards, and report on security status and incidents
- Work closely with external IT and cybersecurity provider(s) to:
  - Direct the deployment and management of ClavystBio's cybersecurity solutions to protect critical services and systems
  - Develop and implement protocols to monitor and detect cyber threats
  - Develop security testing protocols, including vulnerability assessment, penetration testing
  - Develop incident response plans and recovery programs, and evaluate forensic tools to address security breaches
  - Oversee responses to security incidents
  - Lead the development of awareness training programme for employees

Candidate Profile

- At least 8 years' experience in Data Architecture or equivalent role. An IT security or cybersecurity background is likewise required. Bachelor's degree in Computer Science, Information Management or related field as well as relevant certifications (e.g. CISSP, CISM, CRISC, GIAC) preferred.
- Knowledge on data governance, data management framework and processes, local and global data regulations and laws (e.g. PDPA, GDPR), and commercial data management tools
- Knowledgeable on full range of services within a cybersecurity function (e.g. enterprise anti-malware, security assessment tools, 2FA) and able to discuss overall solution
- Ability to balance business needs, technology and security considerations

- Ability to analyse, design, develop and implement a solution roadmap based on current vs future states
- Understanding of risk management principles and experience in policy, standard and guideline implementation in cyber security and technology risk domain
- Ability to interact confidently with internal and external stakeholders to establish problems and explain solutions
- Attention to detail, ensuring accuracy in system maintenance and security protocols.
- Change management capabilities will be advantageous

If you are interested in applying for this position, please email your resume to Christina Cheong at cheong.christina@clavystbio.com