JOB DESCRIPTION- General Manager IT Strategy and Security

Job ID:	FIN007
Job title:	General Manager – IT Strategy & Security
Award/agreement:	Award-Free
Location:	Harry Perkins Institute of Medical Research Nedlands and Murdoch
Supervisor:	Chief Financial Officer
Reports:	No direct reports

ACCESS AND SECURITY:
- *Building RFID card with photo ID*
- *IT Systems, Office 365 and Adobe Creative Suite*

POSITION SCOPE:
The General Manager IT Strategy and Security will effectively manage the organisation's technology and security needs. This will include overseeing the IT governance and service model and the key partnership with the University of Western Australia.

Competencies (skills, knowledge and abilities)	Behaviors (conducts themselves)	Goals
Strategic thinking: The ability to develop and implement a long-term plan that aligns with the organization's goals and objectives.	Visionary mindset: Able to envision the future state of technology and security within Perkins and develop a roadmap to achieve that vision. Analytical approach: Assesses complex data, trends, and market information to make informed decisions and identify opportunities and risks for Perkins. Good decision maker: Makes sound decisions based on a combination of data, analysis, and business objectives, considering both short-term and long-term implications. Problem solver: Identifies and addresses strategic challenges and obstacles,	Development of a long-term strategic direction for IT security and safety at Perkins

	finding creative solutions, and adapting plans as necessary.	
Leadership: The ability to inspire and motivate a team to achieve their best performance, and to create a culture of accountability and excellence	Builds trust and respect: Builds and maintain trusting and respectful relationships with team members, peers, and stakeholders. Demonstrates integrity, ethical behavior, and consistency in actions and decisions. Is aspirational: Articulates a compelling forward-thinking vision for Perkins' IT and cyber safety initiatives. Inspires others by communicating the purpose, value, and impact of their work. Is accountable: Sets clear performance expectations and holds self and team members accountable for goals and deliverables. Provided regular feedback, recognises achievements, and addresses performance issues in a timely and constructive manner. Is adaptable: Leads by example during challenging situations, demonstrating resilience and adaptability. Embraces change, encouraging innovative thinking, and navigating uncertainties effectively.	Creates a positive and productive work environment, inspires others to excel, fosters collaboration, and drives the achievement of organisational goals in the field of IT and cyber safety.
Technical expertise: A strong understanding of IT infrastructure, network security, and cyber threats is essential to effectively manage technology and security operations	Acts as a mentor and guide: Provides guidance, support, and mentorship to IT teams and other stakeholders on technical matters. Shares knowledge, best practices, and insights to help others enhance their technical skills and understanding	Provision of strong technical expertise across IT services

	Ethically aware: Ensures the ethical and responsible use of technology: Demonstrates a strong understanding of ethical considerations, legal requirements, and privacy regulations related to IT and cybersecurity. Upholds ethical standards and ensuring compliance with relevant laws and regulations. Technical problem solver: Applies a systematic and analytical approach to diagnose and solve complex technical issues related to IT infrastructure, network security, and cybersecurity. Utilises expertise and knowledge to identify root causes and develop effective solutions. Continuous learner: Stays updated with emerging technologies, industry trends, and best practices in to ensure the organisation remains at the forefront of technology and security advancements.	
Communication: The ability to effectively communicate technical information to non-technical stakeholders and to convey complex ideas in a clear and concise manner	*Jargon debunker: Avoids and/or translates technical information* *Active listener: Actively listens to others' perspectives, concerns, and questions. Shows genuine interest and attentiveness to foster open dialogue and understanding.* *Empathetic: Seeks to understand the perspectives, knowledge, and backgrounds of non-technical stakeholders. Is empathetic towards their concerns and*	All communications will convey appropriate information that will be targeted, useful and well understood

	challenges and addresses them with sensitivity. *Skilled writer: Able to write skills in various formats, including emails, reports, and documentation. Uses clear and concise language, proper grammar, and appropriate formatting to effectively convey technical information.* *Storyteller: Uses storytelling techniques to convey complex ideas or concepts in a relatable and engaging manner. Creates narratives that help non-technical stakeholders connect with the importance and impact of IT and cyber safety initiatives.*	
Risk management: An understanding of risk management principles and the ability to develop and implement risk mitigation strategies is essential to ensure the security of the organisation's technology and data	Proactive mindset: Is proactive in identifying emerging risks and staying updated with the latest cybersecurity threats and vulnerabilities and taking preemptive measures to address them. Compliance focused: Ensures that the organisation's technology and cybersecurity practices comply with relevant laws, regulations, and industry standards, and implementing necessary controls to address any compliance gaps. Awareness driven: Promotes a culture of risk awareness and cybersecurity within the organisation, overseeing the training and education to employees about	The development and implementation of a risk management plan and actions related to IT strategy and security

	cybersecurity best practices and their roles in risk mitigation.	
Project management: The ability to manage complex projects from conception to completion, including planning, budgeting, and resource allocation	Planner: Develops comprehensive project plans, including defining project scope, objectives, deliverables, and timelines. Organises tasks, activities, and resources to ensure smooth project execution. Outcomes orientated: Delivers the project to completion ensuring the goals are met within time and on budget	Effective management of complex projects on a consistent basis.
Business acumen: A strong understanding of business operations and financial management is important to ensure that technology investments align with the organisation's overall strategy and financial objectives.	Understands values proposition: Articulates the value proposition of technology investments and initiatives in terms of their potential impact on business outcomes, efficiency, profitability, and competitive advantage Improvement orientated: Continuously evaluates and reassesses the impact of technology investments on business outcomes. Seeks feedback and insights from stakeholders and makes adjustments as necessary to enhance the effectiveness and alignment of technology initiatives Strongly financially literate: Possesses knowledge of financial management principles, including budgeting, cost analysis, and return on investment (ROI) evaluation. Can analyse the financial impact of technology investments and make	Technology investments are well-aligned with the organisation's overall business strategy and financial objectives, driving value and contributing to the organisation's success.

	informed decisions based on financial considerations.	
Collaboration: The ability to work effectively with other departments and stakeholders to develop technology solutions that meet the needs of the organisation	Connects with others: Engages with key stakeholders across the organisation, such as executive management, IT teams, and business units, to understand their needs and incorporate their input into strategic planning processes. Listens for understanding: Seeks to understand the issue at hand from the perspective of others and builds a shared understanding of what is possible	People across Perkins will have a shared understanding of strategic objectives and safety measures and will know they have had input

Primary duties/responsibilities:

1. Strategic Planning: Develop and implement IT strategies and roadmaps that align with the overall goals and objectives of Perkins. This includes defining the IT vision, setting priorities, and identifying technology initiatives that support research and operational requirements.
2. IT Governance: Establish and maintain IT governance frameworks, policies, and procedures to ensure effective management and utilisation of technology resources. This includes defining roles and responsibilities, establishing decision-making processes, and ensuring compliance with regulatory and security requirements.
3. Cybersecurity Management: Oversee the development and implementation of comprehensive cybersecurity programs and policies to protect sensitive research data, intellectual property, and other digital assets. This involves assessing and managing cybersecurity risks, overseeing regular security audits, and implementing security controls and incident response plans. This can be done in conjunction with the current service provider.
4. Infrastructure Management: Oversee, with the IT Infrastructure Manager, the management of the IT infrastructure of the medical research institute, including network infrastructure, servers, storage, and data centres. This includes ensuring high availability, scalability, and reliability of IT systems, as well as implementing disaster recovery and business continuity plans.
5. Research Technology Support: Collaborate with researchers and research teams to understand their technology requirements and provide support for research-specific tools, applications, and data management systems. Ensure that research activities are enabled by robust and secure IT infrastructure and solutions. This will be done in conjunction with the University of Western Australia

6. Vendor Management: Oversee technology vendors and manage vendor relationships to ensure the delivery of high-quality services and products. This includes negotiating contracts, monitoring service level agreements, and overseeing vendor performance.
7. Budgeting and Resource Management: Develop and manage IT budgets, ensuring efficient allocation of resources, and monitoring expenditure. This involves identifying cost-effective technology solutions, optimising procurement processes, and tracking financial performance.
8. Team Leadership: Build and lead a high-performing IT team, including hiring and developing staff, setting performance objectives, and providing guidance and mentoring. Foster a culture of collaboration, innovation, and continuous learning.
9. Stakeholder Engagement: Collaborate with key stakeholders across the medical research institute, including researchers, clinicians, administrative staff, and senior management. Understand their technology needs, communicate IT initiatives and progress, and solicit feedback to ensure alignment with organisational goals.
10. Compliance and Regulatory Requirements: Ensure compliance with relevant laws, regulations, and industry standards related to data privacy, information security, and research ethics. Stay updated on evolving regulations and proactively implementing necessary controls and processes.
11. Technology Innovation and Adoption: Identify emerging technologies and trends that can enhance research capabilities and operational efficiency. Assess the feasibility and value of adopting new technologies, overseeing technology pilots and proofs of concept, and promoting innovation within the medical research institute.

Essential skills
- Highly developed leadership skills with the ability to impact and influence across the organisation.
- In-depth knowledge of information technology systems, networks, infrastructure, and cybersecurity coupled with a solid understanding of IT strategy, enterprise architecture, cloud computing, data management, and emerging technologies
- Ability to demonstrate a high level of technical expertise acquired in a similar role.
- Strong knowledge of IT governance and compliance measures and ability to implement these across an organisation.
- Proven experience in developing and maintaining strong relationships across business and technology teams.
- Able to develop and successfully communicate business aligned IT strategies, frameworks, and roadmaps.
- Excellent project management skills with the ability to deliver complex projects across a diverse organisation.

Desirable skills
- Understanding of the technology requirements within the medical research context.

Qualifications:
- A bachelor's in computer science, information systems, or a related field or ability to demonstrate technical knowledge based on industry support qualifications or work experience.

Eligibility:
- Australian Citizen or eligible to lawfully work in Australia.

COMPLIANCE

Perkins Values

All staff members are to adhere to the Perkins Values perkins.org.au/about-us/vision/

Workplace Health and Safety

All supervising staff are required to undertake effective measures to ensure compliance with the Work Health and Safety Act 2020 (WA) and related Perkins requirements.

All staff must comply with requirements of the Work Health and Safety Act and all reasonable directives given in relation to health and safety at work, to ensure compliance with Perkins and Legislative health and safety requirements.

Details of the safety obligations can be accessed at intranet.perkins.org.au/policies/human-resources-policies/ (Only available to Perkins staff).

Equity and Diversity

All staff members are required to comply with the Perkins' Code of Conduct and Equity and Diversity principles. Details of the Perkins policies on these can be accessed at intranet.perkins.org.au/policies/human-resources-policies/ (Only available to Perkins staff.)