JOB DESCRIPTION

JOB TITLE:	Chief Information Officer
DEPARTMENT:	Executive
JOB HOLDER:	New Role
REPORTS TO:	Executive Director
JOB STATUS:	100% FTE Permanent

JOB PURPOSE

The Chief Information Officer (CIO) is responsible for developing and executing a comprehensive IT strategy that not only drives digital transformation but also embeds advanced cybersecurity practices at every level of our operations. The CIO oversees the Head of Data, supporting them to realise optimal data security and analysis within a supportive and secure technology environment. The CIO will ensure that all technology systems and processes are secure, efficient, and aligned with our organisational goals, acting as a critical driver for innovation and risk management.

The CIO is a key member of the executive leadership team and works collaboratively with all senior leaders. This role is designed to include strategic cybersecurity oversight and digital innovation across the organisation and its global footprint.

DIMENSIONS

Annualised Financial Data:

- Oversight of the IT, data, and cybersecurity budget (approximately $4 million annually, subject to strategic priorities).
- Management of CapEx/OpEx forecasts, including investments in software, hardware, licensing, and advanced cybersecurity solutions.

People:

- Leadership of a multi-disciplinary team encompassing IT infrastructure, systems integration, and dedicated cybersecurity specialists.
- Direct responsibility for both full-time and part-time staff, ensuring continuous skill development and effective team performance.

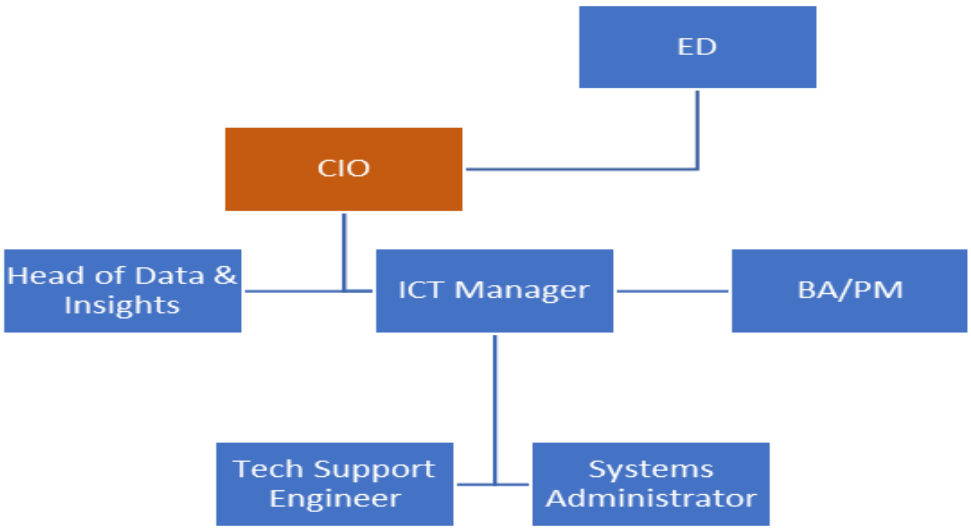
Other Relevant Responsibilities:

- Oversight of multiple interconnected IT systems and platforms, all underpinned by rigorous cybersecurity measures.
- Coordination with numerous internal departments and external vendors to ensure high service quality and secure technology operations.
- Through role on Leadership Team, actively contribute to organisation's strategic planning and direction, financial and risk management, and influence and support international dossiers.

DATE:	**25/02/2025**

JOB DESCRIPTION

ORGANISATIONAL STRUCTURE



CONTEXT

The CIO will balance the need for immediate operational support with long-term strategic planning, ensuring that our digital infrastructure not only supports current business needs but also safeguards against emerging cyber threats. The CIO will oversee the data team, working to ensure the team has the technology assets, capabilities, budget and organization support to deliver a fully realized data strategy. This role is central to positioning our organisation as both an innovator and a secure, resilient enterprise.

This CIO role is pivotal to MSF Australia's future—driving technological innovation and data insights while ensuring our technology infrastructure remains secure, resilient, and aligned with our strategic objectives.

DATE:	**25/02/2025**

JOB DESCRIPTION

ACCOUNTABILITIES	KEY PERFORMANCE INDICATORS
Strategic IT & Cybersecurity Leadership: • Develop and implement an MSFA IT strategy that incorporates advanced cybersecurity measures to support organisational goals. • Lead the digital transformation agenda, ensuring that IT solutions are innovative, secure, and scalable. Cybersecurity & Risk Management: • Oversee the updates to, implementation, and continuous improvement of MSFA cybersecurity protocols across all technology platforms. • Update monitoring systems and rapid response procedures to mitigate risks and reduce security incidents. Digital Transformation & Innovation: • Working with business partners to support their goals, identify and integrate emerging technologies that enhance operational efficiency while ensuring security compliance. • Champion initiatives that foster a culture of innovation and proactive risk management. Data • Deliver and continuously improve data governance policies, plans, procedures and training within a technology environment that meets business needs • Ensure Head of Data and Data team are enabled to deliver on improved data analytics to meet the priorities of the business • When technology and data teams have differing perspectives, represent the perspectives and make recommendations to ED as to how to proceed Team Leadership & Development: • Build, mentor, and empower cross-functional IT and cybersecurity teams. • Implement professional development programmes to ensure the team remains at the forefront of industry trends. Vendor & Resource Management: • Manage strategic relationships with external	IT & Cybersecurity Strategy Alignment: • Delivery and ongoing updates and maintenance of a comprehensive IT and cybersecurity roadmap, aligned with the organisation's long-term business objectives. Cybersecurity Resilience: • Implementation of advanced security protocols across all platforms within 6 months, with a measurable reduction in security incidents over the first year. • Achievement of key compliance benchmarks and industry standards. Data Security & Analytics • Provide appropriate resources, decision making and governance for execution of data road map • Provide key management reports based on data analytics Systems Integration & Operational Efficiency: • Seamless integration of IT systems that enhance workflows and reduce operational disruptions across departments within 12 months. Team Development & Vendor Performance: • Successful upskilling of IT and cybersecurity teams through continuous professional development initiatives. • Consistent achievement of service-level agreements (SLAs) with external vendors . Budget & Investment Outcomes: • Maintenance of IT and cybersecurity budget adherence within an acceptable variance (e.g., within 5% of the planned budget).

DATE:	**25/02/2025**

vendors, ensuring adherence to cybersecurity standards and service-level agreements.
- Ensure vendors have a full understanding of and are responding to business needs, balanced with technological innovation and cyber and data security.
- Oversee resource planning to ensure efficient and effective allocation of technology investments.

Financial & Budgetary Oversight:
- Direct and manage the IT and cybersecurity budgets, ensuring alignment with strategic priorities and financial constraints.
- Monitor multi-year forecasts and maintain adherence to budgetary targets with minimal variance.

Cross-Departmental Collaboration:
- Work closely with other executive leaders to align IT, Data and cybersecurity initiatives with broader business objectives.
- Ensure that technology solutions integrate seamlessly with the needs of various departments, from operations to finance to HR.

Leadership Team
- Actively contribute to organisation's strategic planning and direction, financial and risk management, and influence and support international dossiers.
- Provide to the Leadership Team and Board information, insight and solutions on technology, cybersecurity and data to strengthen their decision making and compliance

Innovation & Technology Adoption:
- Successful deployment of new technology solutions on a quarterly basis that drive organisational efficiency and security enhancements.

Leadership
- Actively participate in engaged and informed discussions on dossiers presented at Leadership Team and as requested by ED, at Board meetings
- Create coherent, clear and solution oriented presentations for both platforms on dossiers within your remit

DATE:	**25/02/2025**

CHALLENGE & CREATIVITY / DECISION-MAKING

Balancing Innovation with Security:

- Evaluate and implement technology investments that address immediate needs while mitigating long-term cyber risks.

Navigating Rapid Technological Change:

- Lead the integration of emerging technologies, managing the inherent risks and regulatory challenges associated with digital innovation.

Team and Vendor Management:

- Cultivate a high-performing, agile team that is responsive to both operational demands and strategic cybersecurity challenges.
- Ensure vendor partnerships deliver high-quality, secure technology solutions.

KNOWLEDGE, SKILLS & EXPERIENCE

- A degree in Information Technology, Computer Science, or a related field is required.
- Advanced qualifications or industry certifications in IT management and cybersecurity (e.g., CISSP, CISM) are highly desirable.
- Extensive experience in senior IT leadership roles, with a proven track record in strategic planning, digital transformation, and cybersecurity management.
- Experience in global or not-for-profit environments is an asset.
- Deep knowledge of IT infrastructure, cloud technologies, systems integration, and advanced cybersecurity practices.
- Up-to-date understanding of emerging cyber threats and regulatory requirements.
- Demonstrated experience in managing multi-million-dollar budgets and optimising technology investments.
- Ability to balance operational efficiency with strategic innovation.

COMPETENCIES

Leadership:

- Lead by example. In MSF-A Australia, the following five values form the foundations of our culture: Transparency, Respect, Understanding of Diversity, Stepping In and CollaboraTion.
- Proven ability to inspire and lead diverse teams while fostering a culture of innovation, accountability, and security.

Strategic Thinking:

- Visionary mindset capable of translating business objectives into actionable IT and cybersecurity strategies.

DATE:	**09/04/2025**
Signed: (Job Holder)	
Signed: (Manager / Director)	

Cybersecurity Expertise:
- Exceptional skills in risk assessment, threat mitigation, and the implementation of proactive security measures.

Communication:
- Excellent communication skills, adept at translating complex technical concepts to non-technical stakeholders.

Problem Solving:
- Strong analytical and decision-making abilities, with a proactive approach to resolving technological and cybersecurity challenges.

Collaboration:
- Demonstrated ability to work effectively across departments, ensuring that IT initiatives support and enhance organisational goals.

DATE:	**09/04/2025**
Signed: (Job Holder)	
Signed: (Manager / Director)	