# MELBOURNE WATER POSITION DESCRIPTION

Chief Information Security Officer (CISO)

| REPORTS TO: | DIRECT REPORTS AND TEAM SIZE: |
|---|---|
| Chief Information Officer | This role has 4 direct reports and up to 10 indirect reports (IT Service Provider's Security personnel). |

## THIS ROLE EXISTS TO: (PURPOSE)

The primary purpose of the CISO role is governance and oversight of cybersecurity across all aspects of digital technology (including IT and OT). The role is primarily accountable for the development, maintenance and execution of Melbourne Water's enterprise-wide Cyber Security strategy. This strategy must align with the Melbourne Water Digital Strategy, the Victorian Government Cyber Security Strategy 2016-202x, and the objectives of the recently appointed Victorian Government Water Services sector CISO. The accountabilities and responsibilities of the CISO role are founded on a Cybersecurity Services Catalogue.

The Cyber Security strategy will document a "future-state" - what should cybersecurity look like at Melbourne Water in 12, 24, 36 months' time? It will also include an implementation plan of the projects and initiatives required to achieve this future state. Responsibility for the strategy's execution and implementation will rest with other groups, both internal and external to Melbourne Water, but accountability remains with the CISO.

The CISO will also have both accountability and responsibility for a cybersecurity assurance function. This function will confirm that the business outcomes identified in the Cyber Security strategy, are being delivered by the projects within the Cyber Security strategy implementation plan and other initiatives (e.g. Internal Audit remediation).

Finally, the CISO will act as an advocate and champion for cybersecurity across the organisation. This will include influencing key stakeholders, driving appropriate behaviour and culture changes, building awareness through effective communication, and leading the strengthening of cybersecurity knowledge and capability across the workforce.

The CISO role has further secondary purposes (refer below).

## KEY ACCOUNTABILITIES:

- Accountable and responsible for the safety and wellbeing of all Cybersecurity & Risk team members.
- Both accountable and responsible for the development of the Cyber Security Strategy including a "future state" and a risk-prioritised implementation plan, that include personal, physical, information technology (IT) and operational technology (OT), that is aligned to the Victorian Government Cyber Security Strategy and endorsed by the Water Services CISO.
- Accountable for the execution of the Cyber Security Strategy implementation plan, but responsibility will rest with other teams and third parties.
- Both accountable and responsible for the Cybersecurity Assurance program (2nd line of defence) to ensure that the outcomes identified in the Cyber Security Strategy implementation plan are delivered by the projects within the Cyber Security strategy implementation plan and other initiatives (e.g. Internal Audit remediation).
- Accountable for the delivery of operational day-to-day Cyber Security services (as defined in the service catalogue) to Melbourne Water employees, contractors and customers, but responsibility will rest with other teams and third parties.

- Accountable for Melbourne Water's compliance with the Victorian Protective Data Security Framework (VPDSF), including an annual attestation by Melbourne Water's Managing Director to the Office of the Commissioner for Privacy and Data Protection (OVPDP), but responsibility will rest with other teams and third parties.
- Accountable for the ongoing cybersecurity maturity as measured by National Institute of Standards and Technology (NIST) cybersecurity framework for both IT and OT, the Australian Signals Directorate (ASD) Essential 8, and other frameworks as identified (e.g. Microsoft Secure Score).
- Accountable for leading and promoting appropriate cybersecurity awareness, culture and behaviours across the organisation at all levels.
- Accountable and responsible for monitoring the external threat environment and assessing the impact of changes upon Melbourne Water and reflecting those changes in the IT Risk Management Framework.
- Accountable and responsible for the ongoing management and maintenance of the IT Risk Management Framework to reflect the "current state" of Melbourne Water's IT risks and controls.

| KEY RESPONSIBILITIES | KPIs |
|---|---|
| **Business Partnering**<br>• Develop and maintain strong relationships with business stakeholders, acting as the cyber security champion for all of Melbourne Water, offering guidance on how best to benefit from IT security technology and controls.<br>•<br>• Participate in strategic and budgetary planning processes, prepare and administer the cyber security capital and operating budgets; provide recommendations on desired policies and goals and implement new/revised programs according to established guidelines. | • Learn and understand the business operating models and platforms.<br>• Acknowledged as the business champion at the executive level to minimise security risk within the organisation while taking a pragmatic approach to risk. |
| **Governance**<br>• Ensure that roles and responsibilities necessary to deliver cybersecurity services are clearly defined, regularly communicated, well understood and well embedded, including ensuring compliance with business, statutory and legislative obligations. | • Ensure reliable processes are defined and implemented to estimate costs and benefits of change initiatives across the business.<br>• Champion and adhere to enterprise methodologies, processes and standards |
| **Strategy**<br>• Develop, maintain and lead the organisation through the Security Strategy and any related IT risk and related strategies. | • Provide consistent overall strategic guidance; procure and deliver all security related solutions; act as a focal point for all security related strategies and implementation plans. |

| | |
|---|---|
| • Initiate and make decisions critical to the organisations ability to protect, detect and respond from cyber security threats.<br>• Develop and implement strategies essential for Melbourne Water to achieve compliance obligations to the Victorian Protective Data Security Framework (VPDSF) and other compliance obligations e.g. ASD Essential 8, NIST, etc.). | • Be the focal point for IT in conveying security to the Audit, Risk Finance Committee, and the Board and to Executives.<br>• Zero data breaches at Melbourne Water.<br>• Zero number of Audit reports rated "D" (Risk exposure outside the acceptable tolerance level) or "E" (Risk exposure is well outside an acceptable level) relating to Information Security within three years.<br>• No "High Risk" Audit or Compliance findings outstanding more than six months after report publication. |
| **Culture and Behaviour**<br>• Promote appropriate awareness of cybersecurity, and healthy cybersecurity culture and behaviours at all levels<br>• Develop and foster cybersecurity skills and capabilities across the organisation | • Appropriate awareness of cybersecurity across the workforce (as measured by survey)<br>• Appropriate cybersecurity behaviours across the workforce (as measure by penetration test/audit)<br>• Cybersecurity and related roles filled with capable and motivated staff (as measured by Engagement Survey, Performance Reviews) |
| **Influence**<br>• Lead and manage with positive influence consistent with the values of Melbourne Water.<br>•<br>• Inspire and influence stakeholders, developing long term relationships facilitating the investment intake.<br>• Manage and positively influence the customer experience within the assigned domain; ensure a professional, responsive and authoritative service at all times.<br>• Form, monitor and maintain long term relationships and strategic engagement with the business at a senior level for the assigned domain. | • Be proactive and pre-emptive in thinking; make decisions critical to the high level planning and execution of business initiatives through the use of technology.<br>• Develop and maintain a client-cantered relationship within the assigned domain continually explore opportunities to add value to the assigned domain ensuring service offerings align to the business strategy.<br>• Positive customer feedback from customers including the Board. |

| | |
|---|---|
| • Communicate early and often, work alongside the assigned domain, forecasting future needs and aligning resources to meet those needs. | |
| **Delivery and Operation**<br>• Delivery - Work closely with key stakeholders to manage the implementation and maintenance of security control techniques and technologies.<br>• Operation - Support effective enterprise risk management; and support the establishment of measurable controls that map to all relevant regulations and standards. | • Continuously improve the security framework methodologies for protecting MW's intellectual property, information assets, regulated data and reputation.<br>• Continually improve MWs maturity rating with respect to the NIST Framework |
| **Skills and Quality**<br>• Skills - Develop the skills across the team to thrive in this digital work environment.<br>• Quality - Continually look for ways to improve process and provide cost effective technology solutions.<br>• Provide inspiration, vision and direction for the growth and success of the team, set the focus for the team providing short and long term operational principles.<br>• Coach, empower and mentor the team to lead them to their goals, have a deep interest in their development, work with them to improve their skills and implement development plans to ensure their performance is at the optimal level.<br>• Make decisions by processing information quickly and assessing alternatives and consider the consequences of which impact a wider range of people. | • Work collaboratively with the team and promote new ways of working and empowering approaches.<br>• Review and update processes, ensuring fit for purpose, consistent with best practice and in line with legislative requirements.<br>• Performance Management - work collaboratively with team to plan, monitor and review teams work objectives and overall contribution to the organization. |

## SKILLS, KNOWLEDGE AND EXPERIENCE REQUIRED:

- Senior level experience in leading an Cyber Security and IT Risk teams through significant change and cultural uplift within a large and complex organisation
- Significant experience in business partnering or consulting, utilizing a services design orientation and a strong demonstrable customer focus.
- Experience in the provision of strategic advice and guidance to senior level management; being agile and impactful

- Demonstrated experience in adaptive leadership and collaboration and in challenging change environments
- Strong commercial acumen to drive fit-for-purpose and value-for-money outcomes.
- Possesses a solid mix of information security and business experience, emphasizing the ability to define and align business requirements to information security outcomes.
- Possesses strong communication skills, and an ability to explain complex technical and security issues in a simple, straightforward manner.
- Security qualifications , accreditations and current certification in:
    - CISSP, CISM, CISA, ISO27001 LA and/or CRISC.
- Demonstrated practical experience (implementation and risk assessment of security standards and framework) in one or more of the following: VPDSF, NIST 800-53, ISO 27001, ISO 27002, ISO 31000, PCI DSS and COBIT 5.0.

## KEY RELATIONSHIPS:

All Melbourne Water employees are responsible for managing aspects of our customer/stakeholder relationships and service interactions, and will work proactively to deliver a consistent customer experience.

**INTERNAL**

- Melbourne Water Board
- Board Audit, Risk & Finance Sub-Committee
- Chief Information Officer
- IT Senior Management Team
- Internal Audit
- Direct reports of each Domain
- Key business stakeholders and customers including senior managers, direct reports
- Project Stakeholders across the business.

**EXTERNAL**

- Cybersecurity subject matter experts (SME’s)
- IT system integrators, suppliers and vendors
- Consultants, external auditors, Department of Premier & Cabinet and DEWLP industry peers
- Relevant cybersecurity governance and knowledge-sharing forums at the industry, state and federal level.

## SALARY RANGE:

- Melbourne Water reserves the right to remunerate people according to their ability to perform the functions of the role based on their qualifications, skills and experience.

## OTHER COMMENTS:

This role requires the following:

- Tertiary degree and evidence of post-graduate (or equivalent) follow-up in an IT security discipline.
- Victorian Driver’s License
- Criminal Records Check

**Location**: 990 La Trobe Street, Docklands and other Melbourne Water sites as required.

Job level: Hay 19
Assessed by: P&C
Date Assessed: June 2021
Last reviewed date: