MICTSETA | Media, Information And Communication Technologies Sector Education And Training Authority

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES

INTERNAL / EXTERNAL ADVERTISEMENT
DIVISION: INFORMATION, COMMUNICATION AND TECHNOLOGY

28 October 2024

REFERENCE NUMBER	**POSITION:** **PERMANENT**	**NUMBER OF VACANCIES AVAILABLE**
ICT: 30 /2024	**MANAGER: ICT GOVERNANCE & SECURITY** **ALL INCLUSIVE REMUNERATION: TCTC (PER ANNUM)** **R 862 210 00 – R1 215 326.00**	**1**

MICT SETA seeks to employ a suitably qualified and competent **Manager: ICT Governance & Security** who will be responsible for safeguarding MICT SETA's systems, networks, and data against threats and vulnerabilities, including assessing, analysing, and responding to security incidents and implement preventive measures for improved resilience to protect the MICT SETA's technology and information from cyber-attacks.

The role will be based at our Midrand Head office and will report to the **Chief Information Officer.**

MINIMUM REQUIREMENTS:

- Bachelor's degree (NQF Level 7) in Computer Science, Information Technology, Information Security or related field
- A minimum of 5-7 years of experience in ICT governance, risk management, or information security.
- Professional certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified in Risk and Information Systems Control (CRISC) are preferred.

Board Members: Simphiwe Thobela (Chairperson), Matome Madibana (Chief Executive Officer), Ayanda Mqela, Lesiba Langa, Loyiso Tyira, Nomonde Gongxeka-Seopa, Nozibele Mlambo, Ntombikayise Khumalo, Rochelle Blaauw, Sipho Zwane, Sontaga Mantlhakga, Tebogo Mamorobela, Thabo Mofokeng, Viwe James

- Experience in developing and implementing ICT governance frameworks and security policies.
- Strong knowledge of relevant laws, regulations, and standards (e.g., POPIA, ISO 27001).
- Proven experience in managing ICT risk assessments, audits, and compliance initiatives.
- Excellent communication, leadership, and stakeholder management skills
- Willingness to work outside of official hours
- A valid driver's license and willingness to travel is essential

ROLES AND RESPONSIBILITIES

ICT Strategic and Operations Management

- Develop, implement, and maintain a comprehensive information security strategy and program.
- Manage the organisation's security architecture, including firewalls, intrusion detection/prevention systems, and endpoint protection.
- Conduct regular security assessments, vulnerability testing, and penetration testing to identify and mitigate risks.
- Oversee the management of identity and access management (IAM) systems, including user provisioning, authentication, and authorisation.
- Ensure the secure configuration and management of ICT infrastructure and applications.
- Ensure policies align with industry standards and regulatory requirements.
- Contribute to the development of supporting operational plans for the business unit to ensure execution of the strategic objectives and goals.
- Drive the implementation of the technology and information security operational plan by developing and allocating operational activities to various business units and ensuring alignment to the achievement of operational targets.

- Use insights gained through business information to compile reports, and metrics to measure success and inform the business decision making process and realign objectives.
- Keep abreast of changes in legislation, regulations and respond to changes through adjustments to the strategy and operational plans as required.
- Assist in monitor and continuously evaluate progress of the business unit's achievements against the operational plan and strategic objectives.
- Continuously improve current practices and processes for improved security.

Functional Management

- Establish and maintain an incident response plan to manage security breaches, data breaches, and cyber-attacks.
- Lead the investigation, containment, and resolution of security incidents, coordinating with internal and external stakeholders.
- Conduct post-incident reviews and implement corrective actions to prevent future occurrences.
- Maintain a log of all security incidents and prepare reports for senior management.
- Contribute to the maintenance of the ICT risk registers
- Conduct security and risk assessments of change requests and ICT projects
- Report to management on risk assessments & audit results
- Develop controls to ensure compliance and security.
- Sustain controls throughout the data and service life cycle.
- Design and manage security systems, including firewalls, intrusion detection systems, anti-virus software, encryption tools, and other technology risks mitigations.
- Collaborate with developers and ICT operations teams to ensure security-by-design principles are integrated into cloud architectures and development pipelines.
- Maintain up-to-date knowledge of emerging security threats, technologies, and best practices in security.

- Facilitate with internal and external stakeholders to perform penetration testing and vulnerability assessments to identify and remediate security vulnerabilities and weaknesses.
- Perform security assessments of third-party vendors and partners to ensure they meet security requirements and standards such as ISACA.
- Coordinate with relevant teams to ensure readiness for potential incidents.
- Contribute to management and Board reports.
- Prepare and present quarterly, weekly, and monthly reports on security status and incidents.
- Report on compliance, risk management activities, and security initiatives.
- Provide insights and recommendations to CIO and senior management based on report findings.
- Develop and implement cyber security frameworks to protect against cyber threats.
- Stay updated on the latest cyber security trends and technologies.
- Implement and manage security and event management systems.
- Conduct internal and external security audits to identify vulnerabilities.
- Assist in implementing corrective actions based on audit findings.
- Ensure physical and logical security of all ICT facilities.
- Implement access control measures to protect sensitive information.
- Monitor facilities for security breaches and take appropriate actions.
- Assist in the establishment and functioning of the Security Operations Centre (SOC)

Policy Development and Implementation

- Develop and enforce ICT policies and procedures related to governance, risk management, and security.
- Ensure that ICT policies are communicated to all stakeholders and regularly reviewed and updated.
- Collaborate with legal, HR, and other departments to align ICT policies with organisational policies.

Stakeholder Management and Relations

- Act as the primary point of contact for ICT governance and security matters.
- Engage with internal and external stakeholders, including auditors, regulatory bodies, and vendors, on ICT governance and security-related issues.
- Provide regular reports to the CIO, senior management, and the board on the status of ICT governance, risk management, and security.
- Collaborate with IT teams, business units, and external partners to ensure alignment and compliance.
- Assisting with provisioning of effective and efficient ICT services and solutions to various departments within MICT SETA to enable them to achieve their strategic objectives.
- Coordinate and facilitate communication channels with internal and external key stakeholders to ensure proper messaging of ICT standards.
- Implement and monitor Service Level Agreements with the relevant stakeholders.
- Ensure that agreed service levels are consistently met on monthly basis.
- Gather and disseminate accurate and timely information to all relevant stakeholders.
- Ongoing management of strategic partners and vendors to ensure that they perform according to the SLA's.
- Implementation of vendor scorecards to measure compliance with company expectations.
- Ensure that company SLAs are measurable and aligned with strategic partners and vendor service agreements.
- Conduct regular reviews of strategic partners and vendor contracts to ensure SLA's are measurable and enable consistent delivery.
- Development and maintain ICT Service Catalogue
- Continuous improvement of ICT practices and processes.
- Coordinate with service providers for regular security audits and reviews.

Governance, Risk and Compliance

- Identify, assess, and manage ICT risks, including cyber threats, data breaches, and information leaks.
- Develop and implement risk management processes, including risk assessments, risk registers, and mitigation plans.
- Ensure compliance with relevant laws, regulations, standards, and frameworks, such as POPIA, ISO 27001, and NIST.
- Liaise with internal and external auditors to coordinate ICT audits and address findings.
- Assist the CIO with establishment, maintenance and improvement of Standard Operating Procedures, policies, and guidelines.
- Assist with monitoring implementation of all relevant ICT policies in compliance with legislative prescripts and international best practices.
- Participate in Risk assessments, develop mitigation plans, and implement risk action plans.
- Develop a process for data classification for security, risk, and business impact.
- Ensure the implementation of formal ICT security-based documentation, auditing, and testing processes.
- Prepare Management reports and contribute to Board reports.
- Ensure compliance with relevant laws, regulations, and standards.
- Assist in the development and implementation of an ICT governance framework aligned with organisational goals and industry best practices.
- Establish governance policies, procedures, and standards for ICT security.

Budget and Finance Management

- Contribute into the development and implementation of the departmental budget by ensuring financial stability.
- Ensure expenditure is in line with budget requirements.
- Assist in the management of procurement process to ensure compliance with the legislation e.g. (PFMA, PPFA, and BBBEE).
- Maximise revenue and reduce expenditure through effective cost control measures.

- Ensure that the ICT related assets are economically acquired, adequately implemented, maintained and protected in all respects.

Security Awareness and Training

- Develop and implement an information security awareness and training program for the MICT SETA.
- Conduct regular security awareness campaigns, workshops, and training sessions.
- Monitor and report on the effectiveness of security awareness initiatives and adjust as needed.

People Management

- Build and lead an effective and cohesive team through the effective management of office resources.
- Ensure the enhancement of relevant knowledge and skills through continuous coaching, mentoring and nurturing of talent in the business unit.
- Contribute to the creation of a high-performance culture and manage team performance effectively by translating and communicating the annual performance goals and measures into individual work plans based on agreed upon objectives.
- Ensure the working environment contributes to improving employee engagement, recognition and increased productivity.
- Ensure the management of poor performance and disciplinary matters in line with the MICT SETA's policies and procedures.

ICT Service Continuity / Disaster Recovery

- Improve ICT services through implementation of secure technologies.
- Assist in the development of ICT Service Continuity / Disaster Recovery Plans and lead in implementation thereof.
- Maintain business continuity plans to ensure continuation of critical operations during disruptions.
- Design and test disaster recovery plans to minimize data loss and downtime.

- Establish methods and procedures to enable the CIO and MANCO to assess risks and business impact in determining ICT Service Continuity practices.
- Manage backup procedures and systems.

COMPETENCIES		
VALUES	**FUNCTIONAL**	**BEHAVIOURAL**
• Customer Centricity • Ethical • Innovative • Committed • Meritocracy • Collaboration • Responsiveness	• Technology Management • ICT Security • Strategic Capability and leadership skills • Stakeholder Management and relations • Financial Management • Project Management • People Management • Business Writing Skills • Communication (Verbal and Written) • Change Management • Conflict Management • Risk Management	• Organisational and planning • Decision making • Emotional Intelligence • Resilience • Problem solving and analysis • Interpersonal relations • Team leadership • Attentive to detail and accuracy

Application:

Please click the link to apply https://forms.office.com/r/KKMHANYQCn by no later than **12 November 2024.**

Queries may be directed to 011-207-2649.

Should candidates not hear from us within 30 days after the closing date of applications, they should consider their applications as unsuccessful. Please note that this is an open position.

♿ **White, Indian, Coloured and people with disabilities are highly encouraged to apply for this position in-line with the MICT SETA Employment Equity Targets.**

POPIA DISCLAIMER- By applying for MICT SETA's vacancy, you hereby expressly give MICT SETA consent to process your personal information in accordance with the relevant provisions of the Protection of Personal Information Act 4 of 2013 ("POPIA"). Further, the MICT SETA shall retain personal information as per the regulations set out by the National Archives and Records Service of South African Act (NARSSA), Act. 43 of 1996, *as amended.*

Please refer to the MICT SETA POPIA Disclaimer for further information ***(https://www.mict.org.za/popia-disclaimer/)***