UNIVERSITY OF SOUTH AFRICA

PORTFOLIO: INFORMATION COMMUNICATION AND TECHNOLOGY

POSITION: HEAD: DIGITAL SECURITY MANAGEMENT (P4)
(5-YEAR FIXED-TERM CONTRACT)

(REF: HDSM_ICT/VP:COI/AM/2024)

UNISA is publicly funded Higher Education Institution in South Africa dedicated to distance education. In keeping with its mandate as a Comprehensive, Open and Distance Learning (CODeL +) Institution offering a variety of academic and career-focused programmes, Unisa is inviting applications for the position of **Head: Digital Security Management P4.**

The purpose of the position is to:

- To inspire innovation, improve productivity and ultimately contribute to data privacy and protection of the integrity of UNISA qualifications and offerings through appropriate digital and cyber protection measures across the UNISA teaching and learning ecosystem, and associated UNISA solution platforms to enable CODeL.
- In this role the incumbent will develop and implement an appropriate digital security programme for UNISA. He or she will enable management of appropriate digital security controls, policies, procedures, techniques, and technologies to consistently protect enterprise communications, systems and assets from possible digital threats both internally and externally.

KEY DUTIES/RESPONSIBILITIES

Strategic Direction, Alignment and Governance:

- Developing operational plan and KPI's in support of the departmental strategy and the institution's overall vision and strategy
- Leading strategic technological planning for digital security management solutions and platforms to achieve business goals by prioritizing technology initiatives and coordinating the evaluation, deployment, and management of current and future technologies.
- Developing and implementing plans, policies and practices that control, protect and optimize the value of data and information assets in line with the relevant information security management strategies.
- Defining and implementing appropriate information security management frameworks and digital security management strategies.
- Participating as a member of the middle management team in governance processes of the information security management, and ICT strategic planning.
- Reporting on progress against strategic initiatives
- Participating in Institutional governance structures
- Overseeing and reporting on legislative and statutory compliance as defined by government and relevant professional bodies.

Digital Security Management

- Providing tactical and operational leadership regarding all operations of the Directorate to provide digital security planning, manage digital security operations and ensure digital assets protection.
- Driving all aspects of digital security planning, including digital security lifecycle management, information risk management, threat management and understanding of security insurance management.
- Ensuring an effective security operations centre that manages vulnerabilities and threats, manages security incidents, and responding to alerts following relevant processes and procedures.
- Protecting the institution's digital assets by implementing identity and access management, providing thought leadership on adoption of best practices, and providing investigative capabilities.
- Leading the management of cyber risks related to the use, storage and transmission of data and information systems.
- Effectively analyse risk within the context of business problems and mitigating risks with common security controls.
- Continuously assess and improve the organization's cyber security controls.
- Providing advice on the integration of security practices across operational processes within the institution.
- Leading the implementation of cost-effective digital security management capabilities, processes, procedures, best practices, and tools.
- Developing and delivering measures and metrics for ongoing assessment of the information security posture.
- Promoting appropriate behaviours and practices to create a culture of information security awareness within the institution.
- Directing, and or assisting on, investigations into information security breaches and take appropriate actions aligned to the institutional policies.
- Collaborating with the appropriate departments to develop and maintain a data protection plan that supports institutional needs.
- Leading the alignment of the organizational business needs, activities, and drivers with cost effective digital security technology capabilities.
- Driving the development of business or technology alignment plans for data protection solutions to the executive team, staff, partners, customers, and stakeholders.
- Ensuring effective digital security governance controls for appropriate introduction or adoption
- Facilitate and promote digital security management capabilities within the institution.

People Management

- Implement Talent Management throughout the directorate:
    - Talent identification and development
    - Performance management
    - Succession Planning
    - Ensuring and ODeL competent workforce

- Leading, mentoring and empowering employees and change within the directorate to promote high performance, optimal working environment, and cost-effective operations.
- Guiding and influencing strategic leadership in embedding the values and desired culture of the Institution in line with the Transformation Charter and ODeL 2016-2030 Strategy
- Embedding sustainability through a green Institution-wide culture.

- Driving a high-performance culture by taking accountability for an effective and well-articulated performance management process.
- Ensuring the resourcing of the directorate through recruitment and filling of positions to meet the operational requirements of the institution.
- Promoting the positive employee relations and climate through employee engagement within the directorate
- Promoting wellness and healthy balanced workforce
- Fostering an organizational culture and climate that is ethics and value driven.

Budgeting and Financial Management

- Compiling and managing the directorate's budget in line with the departmental budget
- Directing and monitoring the directorate's expenditure within budgeted parameters and reporting on variances periodically
- Managing the process of allocation of financial resources within the directorate
- Managing the function's resources sustainably in accordance with financial principles
- Authorizing the procurement of relevant services, equipment, and materials
- Safeguarding the assets allocated to the directorate.

Qualification

- Minimum of Bachelor Honours Degree in Computer Science or Postgraduate Diploma in Computer Science or Professional Bachelor's Degree (NQF 8) in Computer Science.

- In-depth understanding of best practices within information security including knowledge of ISO / IEC 27001, COBIT, the NIST standards and frameworks, and CIS controls.

- **Certification in one or more of the following will be an added advantage:**
    - Certified Protection Professional (CPP),
    - Certified Information Systems Security Professional (CISSP),
    - GIAC Security Operations Manager Certification,
    - CompTIA Advanced Security Practitioner (CASP+),
    - Certified SOC Analyst (CSA),
    - Certified Security Operations Centre Practitioner (CSOCP).
    - Certified Information Security Manager (CISM)
    - Certified Ethical Hacker (CEH)
    - GIAC Security Essentials Certification (GSEC)
    - Systems Security Certified Practitioner (SSCP)
    - Certified Data Privacy Solutions Engineer (CDPSE)
    - Certified Digital Asset Advisor (CDAA)

Experience

- Minimum of 10 years of relevant work experience with at least 5 years in a management role
- Demonstrable skills in decision-making and problem-solving.
- Proven ability to proactively manage all aspects of cyber security.
- Has performed various roles in the information security management value chain.

Closing Date: 29 February 2024

Please note that Skill Placement has been appointed as the service provider for the response handling process and all correspondence.

Enquiries: **Mr. Godwin Murerwa – 078 111 9007/011 764 1052** application can be forwarded by email to: **godwin@skillplace.co.za**

Interested candidates should send a detailed cover letter indicating their suitability for the position, a detailed comprehensive Curriculum Vitae, and copies of the following documents:

- All educational qualifications;
- Identity document; and
- Proof of SAQA verification of foreign qualifications, where relevant.

The contact details of three contactable references must be provided, one which must be from your present employer. Should you not be currently employed a contactable reference from your previous employer must be provided. Short-listed candidates will be required to prepare a presentation on the interview date

The detailed advertisement together with the prescribed application form can be found on the UNISA website (**http://www.unisa.ac.za/vacancies**). UNISA is not obliged to fill an advertised position.

Late, incomplete, and incorrect applications will not be considered.

Recommended candidates might be subjected to competency assessment

We welcome applications from persons with disabilities.

Appointments will be made in accordance with UNISA***'s Employment Equity Plan and other applicable legislation.***