SENIOR CYBER SECURITY AND DIGITAL ASSETS MANAGER

Post Number : DBS 104
Grade : P-5
Parent Sector : Sector For Administration and Management (ADM)
Duty Station: Paris
Job Family: Computer Sciences / Information Technologies
Type of contract : Fixed Term
Duration of contract : 2 years
Recruitment open to : Internal and external candidates
Application Deadline (Midnight Paris Time) : 22-SEPT-2021 (EXTENDED)

UNESCO Core Values: Commitment to the Organization, Integrity, Respect for Diversity, Professionalism

OVERVIEW OF THE FUNCTIONS OF THE POST

The position is located in the Bureau of Digital Business Solutions in the Sector for Administration and Management.
Digital technologies play a key role in the fulfilment of UNESCO's mandate and the delivery of its programme. To support and enable the strategic transformation agenda, new digital technologies are being implemented across the Organization. The Bureau of Digital Business Solutions (DBS) plays a key role in this implementation. DBS serves as the Secretariat for the Organization's digital transformation governance, facilitating the development and evolution of the One-UNESCO Digital Strategy.
As a key partner in the implementation of this strategy, the Bureau's work includes the design and deployment of coherent and integrated corporate solutions to support the delivery of UNESCO's programmatic outputs, while ensuring that all digital/IT services remain functional and operational at all times, and information management, digital/IT risk mitigation and cybersecurity measures are in place.
The objectives and outputs of the Bureau are highly service oriented, requiring business engagement, customer focus and innovative digital solutions. New ways of working are needed that provide both effectiveness and efficiency in solution delivery, built on best in class principles of user experience design and digital/IT architectures.

Reporting to the Chief Information and Technology Officer (CITO), the Senior Cyber Security and Digital Assets Manager supports the delivery of the Bureau's outputs and digital transformation as a whole, and is responsible for leading the design, development, advancement and implementation of the information and cybersecurity programme portfolio. The incumbent heads the Information Security and Digital Assets Management Section and directs a team of cyber-security and information management staff and external partners.
The key responsibilities of the role are as follows:

- Serve as a programme leader in the area of cybersecurity and information management, conceptualizing, developing strategy for and overseeing the design and implementation of major systems initiatives in the areas of cybersecurity and information/content management. Identify cybersecurity goals, objectives and metrics, and establish the direction for the Organization-wide vision and roadmap for cybersecurity, including policies, standards, priorities and projects.
- Formulate and develop policies and frameworks for digital risk management and cybersecurity to advance programme and organizational objectives.
- Recommend information security investments which mitigate risks, strengthen defences, and reduce vulnerabilities in systems development, including internal and customer facing applications and products.

- Direct the implementation and monitoring of access management and information security frameworks, strategies, standards and policies.
- As the Organization's chief information security officer (CISO), lead technology risk management, product/system selection and the negotiation of high-level contracts, agreements and services.
- Provide authoritative technical and policy advice, and clear and concise responses to senior managers and strategic stakeholders, both internally and externally to stakeholders, on the use of secure and reliable systems in a changing business environment as well as the implications of various alternatives and other related issues.

- Monitor information security trends globally and collaborate with peers in UN-system organizations, Member States and the private sector on information security related initiatives; develop effective Organization-wide communication systems to quickly disseminate information and solutions to manage potential threats and mitigate risk and to ensure the consistent implementation of approaches and processes that guarantee information security compliance.
- Drive the coordination and conduct of audit exercises and regulatory enquiries, support the Organization from a cybersecurity and digital risk perspective, and ensure audit follow up and risk mitigation action are taken according to organizational and international standards and best practices.
- Exercise strategic human and financial asset management. Prepare, monitor and assess the budget, work programme and spending plan of the Section, direct and empower a team of Section staff and external technical partners, plan and manage work assignments, coach, mentor and evaluate team and staff performance using metrics and data analytics among other mechanisms, and substantively participate in recruiting, selecting and building the capacity of staff.
- Work horizontally to drive technological, risk management, security and information management performance, business and customer engagement, and the development of secure solutions to resolve information management issues that impact a critical area of the organization's work, including through the use of data analytics.
- Serve as a member of the DBS Management Team and deputize for the CITO as required.
- Perform such other duties as may be assigned.

COMPETENCIES (Core / Managerial)

Communication (C)
Accountability (C)
Innovation (C)
Knowledge sharing and continuous improvement (C)
Planning and organizing (C)
Results focus (C)
Teamwork (C)
Professionalism (C)
Building partnerships (M)
Driving and managing change (M)
Leading and empowering others (M)
Making quality decisions (M)
Managing performance (M)
Strategic thinking (M)

For detailed information, please consult the UNESCO Competency Framework.

REQUIRED QUALIFICATIONS

Education

- Advanced University degree (Master's degree or equivalent) in the field of in computer science, information systems, or a related field.
- Senior level professional certifications in information security such as CISSP (Certified Information Systems Security Professional) are a plus.

Work Experience

- Minimum of ten (10) years of progressively responsible and relevant professional work experience in the field of computer science, information systems, including demonstrated management experience in developing and implementing cybersecurity and organizational information management programme.
- Relevant experience acquired at the international level.
- Experience in performing and supervising cybersecurity assessments.
- Experience in the design, development, deployment and operation of threat hunting and incident management solutions and related processes.
- Experience in reviewing and providing advice on the design of secure information technology solutions including with respect to cryptographic controls, integrated authentication solutions, information security classification models, and threat modelling.
- Proven experience in managing/coordinating large and diverse working groups or teams, and providing policy advice and guidance on information security risk management.

Skills & Competencies

- Knowledge of, and commitment to UNESCO's mandate, vision, strategic direction and priorities.
- Institutional leadership capacity, high sense of objectivity and professional integrity, diplomacy, tact and political astuteness.
- Proven skills in administration and the management of financial and human resources.
- Demonstrated strategic planning and management abilities, including capacity to administer extensive programmes, financial resources and exercise appropriate supervision and control.
- Excellent analytical and organizational skills, including in establishing plans and priorities, and in implementing them effectively, as well as in devising implementation plans.
- Ability to interact with a wide range of high-level partners, as well as demonstrated building and maintaining partnership development.
- Capacity to provide intellectual leadership to guide staff, as well as ability to build trust,manage, lead and motivate a diversified body of staff in a multicultural environment with sensitivity and respect for diversity, exercise supervision and control, as well as ensure continuous training and development of staff.
- Proven ability to work collaboratively and to build and maintain partnerships with internal and external stakeholders.
- Excellent communication, interpersonal and representational skills, and demonstrated ability to advocate, and negotiate with staff and a wide range of stakeholders/partners at all levels within and outside the Organization.
- Sound judgement and decision-making skills.

Languages

- Excellent knowledge in English (oral and written).

DESIRABLE QUALIFICATIONS

Education

- Business Management or Business Operations degree.

Work Experience

- Experience or a propensity for running or managing IT for a business.
- Experience with ISO27000, ITIL and CCM (Cloud Controls Matrix) frameworks.

Skills & Competencies

- Familiarity with the work and general functioning of international organizations and/or the United Nations system.

Languages

- Good knowledge of French (oral and written).
- Knowledge of other official UNESCO languages (Arabic, Chinese, Russian or Spanish).

BENEFITS AND ENTITLEMENTS

UNESCO's salaries consist of a basic salary and other benefits which may include if applicable: 30 days annual leave, family allowance, medical insurance, pension plan etc.
For full information on benefits and entitlements, please consult our Guide to Staff Benefits.

SELECTION AND RECRUITMENT PROCESS

Please note that all candidates must complete an on-line application and provide complete and accurate information. To apply, please visit the UNESCO careers website. No modifications can be made to the application submitted.
The evaluation of candidates is based on the criteria in the vacancy notice, and may include tests and/or assessments, as well as a competency-based interview.
UNESCO uses communication technologies such as video or teleconference, e-mail correspondence, etc. for the assessment and evaluation of candidates.
Please note that only selected candidates will be further contacted and candidates in the final selection step will be subject to reference checks based on the information provided.

UNESCO applies a zero tolerance policy against all forms of harassment.
UNESCO is committed to achieve and sustain gender parity among its staff members in all categories and at all grades. Furthermore, UNESCO is committed to achieving workforce diversity in terms of gender, nationality and culture. Individuals from minority groups, indigenous groups and persons with disabilities, as well as nationals from non-and under-represented Member States (last update here) are equally encouraged to apply. All applications will be treated with the highest level of confidentiality. Worldwide mobility is required for staff members appointed to international posts.

UNESCO does not charge a fee at any stage of the recruitment process.