



## VACANCY ANNOUNCEMENT

### Information Systems Officer (Cybersecurity), P-4 Administration and Operations Division ICT Subdivision

Deadline for application	Announcement number	Expected date for entry on duty	Duration of appointment	Duty Station
14 June 2026 23:59 hrs CET	VA 26/031/A&O	As soon as possible	1 year with possibility of extension	Bonn, Germany

Publication date: 15 May 2026, Post number: 31046199 Funding: 64ZCR/16809

**The United Nations Framework Convention on Climate Change (UNFCCC)** is the focus of the political process to address climate change. The UNFCCC secretariat supports the Convention, its Kyoto Protocol and the Paris Agreement through a range of activities, including substantive and organizational support to meetings of the Parties and the implementation of commitments. It is a dynamic organization working in a politically challenging environment to help resolve one of the defining environmental issues of our time.

#### **Where you will be working**

The Administration and Operations division (A&O) will deliver a wide range of operational services that support the intergovernmental process, related institutions, bodies and mechanisms, including conferences and meetings, the regulatory systems under the Kyoto Protocol, and the daily operations of the secretariat and its divisions.

This position is located in the Information and Communication Technology (ICT) sub-division. The incumbent reports to the Manager of the ICT sub-division.

ICT will provide a reliable, sustainable and coherent IT infrastructure; operate and maintain existing mandated systems that support the intergovernmental process and improve the overall level of ICT, with a focus on extending and improving critical user-facing services.

Under the general supervision of the ICT Manager, the incumbent provides oversight, technical and programmatic information security guidance on the delivery, operations and maintenance of ICT services.

#### **Your responsibilities**

Within limits of delegated authority and depending on location, the Information Systems Officer will be responsible for the following duties:

**Information Security Governance:** Responsible for developing and implementing policies, Standard Operating Procedures, and guidelines to ensure the protection of information and systems from cyber security risks, to confirm that cyber security is aligned with organizational objectives, and to assess the requirements for their implementation. This role establishes mechanisms to identify and evaluate cyber security risks, develops mitigation strategies, collaborates with cross-functional teams, oversees the implementation of cyber security controls, conducts audits of cyber security practices, and provides guidance on cyber security.

#### **Specialty specific:**



- Develop and maintain policies, processes, procedures, and guidelines related to cybersecurity, ensuring that they are aligned with organisational goals.
- Define and implement the cybersecurity governance framework to meet the organisational and regulatory requirements, and key performance indicators related to governance.
- Develop cybersecurity strategies and implementation plans of protective measures for information assets.
- Oversee that cybersecurity plans provide adequate cybersecurity for networks, facilities, systems, and information.
- Participate and advise on cybersecurity matters in governance and management committees.
- Keep abreast of the current and emerging security issues, risks, threats, vulnerabilities, and advancements in cyber security techniques and technologies.
- Develop and manage security awareness trainings and other communications to increase personnel's understanding of cyber security policies, procedures and regulatory requirements.
- Prepare reports that identify technical and procedural findings and provide recommended remediation strategies/solutions including detailed mitigation plan and remediation plan.
- Make recommendations and prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.

#### **Information Security Compliance:**

- Provide guidance on designing, implementing, auditing, and conducting compliance testing activities to ensure adherence to cyber security compliance requirements.
- Provide guidance in the design and implementation of applicable cyber security frameworks, and ensure its policies, processes, procedures, and controls are appropriately mapped to relevant UN internal regulatory and compliance requirements.
- Continuously assess the efficiency and effectiveness of control systems, recommend necessary remediations and propose steps for improvements to ensure ongoing compliance.
- Contribute to the development of the organization's cyber security strategy, policy, and procedures in consultation with senior management and legal team, as necessary.
- Ensure the confidentiality, integrity, and discreet handling of sensitive information in compliance with the UN data privacy, security requirements, and standards.

#### **Information Security Threat and Incident Management:**

- Respond to information security incidents according to the security incident response technical procedures.
- Conduct network monitoring and intrusion detection analysis.
- Conduct regular incident response exercises to test the effectiveness of the incident response plans, playbooks and procedures.
- Conduct processes of investigation into infrastructure and application intrusions, as well as data theft carried out by threat actors and through various threat vectors.
- Validate and maintain incident response plans and processes to address potential threats, in alignment with the business continuity and disaster recovery plans.
- Perform other duties within your functional profile as assigned and deemed necessary for the efficient functioning of the office



### **Competencies:**

**Applying Professional Expertise:** Demonstrates expertise of subject matter and the transferable skills required for the function; Shows the capacity to apply knowledge to deliver results based on acquired background and experience; Seeks opportunities to apply own technical skills across related disciplines; Keeps abreast of new developments and technologies in the field of expertise; Actively seeks to expand the existing level of job knowledge and expertise.

**Being Accountable:** Uses UN funds, assets and resources responsibly, effectively and efficiently; takes ownership of own work plan, honors commitments and acknowledges responsibility for any failure in planning or delivering work; respects and operates in compliance with the UN regulations and rules; ensures that own work and contributions to the team are complete, accurate and of the highest quality; takes corrective action to address issues that compromise compliance or delivery.

**Communicating with impact:** Speaks clearly and directly and is able to express views in an understandable, credible and persuasive manner; Writes in a well-structured and logical manner, in keeping with established UN standards; Openly shares information and keeps people informed; Uses appropriate communication tools to disseminate information; Listens carefully to understand other's views and responds appropriately; Seeks feedback and adjusts language, tone, style and format to match the audience.

**Delivering results:** Conducts a critical analysis of situations to develop sound goals and work plans; Consults with others to develop integrated, consistent and harmonized plans; Allocates and uses time efficiently, and monitors own performance against timelines and milestones; Foresees risks, plans for contingencies, and adapts to take account of changing circumstances; Perseveres to deliver projects and pursues results despite obstacles and setbacks; Manages competing demands and focuses on priorities to deliver results.

### **Your qualifications**

#### **Educational Background:**

---

**Required:** An advanced university degree (Master's degree or equivalent) in computer science, information systems, mathematics, statistics, information security, cyber security, or a related field. A first-level university degree (Bachelor's degree or equivalent) in combination with an additional two years of qualifying experience may be accepted in lieu of the advanced university degree.

#### **Experience:**

---

**Required:** A minimum of seven years of progressively responsible experience in information security management related to cybersecurity with a focus on domains such as governance, risk management, compliance, and threat assessment. Managerial experience in collaborating with senior management, ICT leaders, business units, and other stakeholders to ensure that cyber security is effectively integrated into all aspects of the organization's operations, processes, and communications is required. At least two years of hands-on technical expertise in core Azure and Microsoft 365 identity management, data protection, and security technologies, including Azure Defender,



Entra ID, Azure Monitor, Sentinel SIEM, and the Microsoft Purview portal, are requisites for this position.

**Language skills:**

---

**Required:** Fluency in spoken and written English, knowledge of a second official UN language is an advantage.

**Other:**

---

An active certificate in Information Security (e.g.CISM, CISSP) or equivalent is highly desirable. Ability to manage multiple projects under strict timelines.

**What is the selection process?**

Evaluation of qualified candidates may include an assessment exercise which may be followed by a competency-based interview. The above listed set of competencies will be applied for this particular post.

**How to apply:**

Candidates, whose qualifications and experience match what we are looking for, should use the online application system available at <http://unfccc.int/secretariat/employment/recruitment>

**Please note:**

1. Service is limited to the UNFCCC secretariat.
2. We will confirm receipt of your application. However, only candidates under serious consideration and contacted for an interview will receive notice of the final outcome of the selection process.
3. Indicative net annual salary and allowances:  
US\$ 86,027  
(plus variable post adjustment, currently 38.3% of net salary),  
plus other UN benefits as indicated in the link below:  
<https://unfccc.int/secretariat/employment/conditions-of-employment.html>

UNFCCC secretariat is committed to diversity and inclusion within its workforce, and encourages candidates, irrespective of gender, nationality, religious and ethnic backgrounds, including persons with disabilities to apply.