UNITED NATIONS CHILDREN'S FUND
JOB PROFILE

I. Post Information

Job Title: **ICT Manager (Cybersecurity Architecture and Engineering)** Supervisor Title/ Level: **Chief, Information Security** Organizational Unit: **ICTD Digital Core, CIO Office** Post Location: **Valencia, Spain**	Job Level: **P4** Job Profile No.: **129003** CCOG Code: Functional Code: Job Classification Level: **P4**

II. Organizational Context and Purpose for the job

The fundamental mission of UNICEF is to promote the rights of every child, everywhere, in everything the organization does — in programs, in advocacy and in operations. The equity strategy, emphasizing the most disadvantaged and excluded children and families, translates this commitment to children's rights into action. For UNICEF, equity means that all children have an opportunity to survive, develop and reach their full potential, without discrimination, bias or favoritism. To the degree that any child has an unequal chance in life — in its social, political, economic, civic and cultural dimensions — her or his rights are violated. There is growing evidence that investing in the health, education and protection of a society's most disadvantaged citizens — addressing inequity — not only will give all children the opportunity to fulfill their potential but also will lead to sustained growth and stability of countries. This is why the focus on equity is so vital. It accelerates progress towards realizing the human rights of all children, which is the universal mandate of UNICEF, as outlined by the Convention on the Rights of the Child, while also supporting the equitable development of nations.

Strategic office context : *(Please provide an overview of the office context in which this position works, briefly summarizing UNICEFs current objectives in that particular office/division, as well as the specific role of the positions section in contributing to their achievement)*

The overarching strategic goal of UNICEF's Information and Communication Technology Division (ICTD) is to transform and build partnerships with our stakeholders to successfully implement UNICEF programmes globally through innovative technology-enabled solutions.

UNICEF is going through an exciting digital transformation that will influence the work across the organization. We are looking for dynamic, innovative professionals to drive the transformation and play a key role in shaping the way forward.

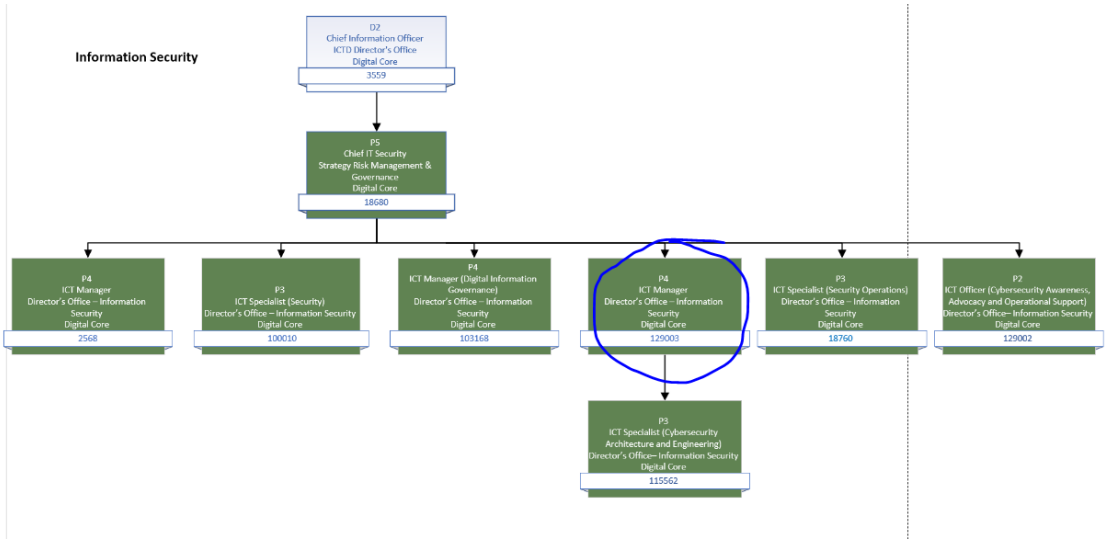
A new cybersecurity program and a review and re organization of the cybersecurity team have been created to accompany DX and is equally set to transform the way UNICEF develops, manages, and safeguards its digital assets.

The aim of this new program and review is to establish a robust, forward looking Cybersecurity Organization that combines the standard functions of Executive leadership, Security Operations Oversight, Security Architecture and Engineering, Governance and Compliance, Investigation support and Cybersecurity Awareness.

As part of this broader cybersecurity strategy UNICEF aims at increasing the organization's maturity with regards to its Cybersecurity Architecture and Engineering practice, with special emphasis on the development and integration of beneficiary and donor centric digital products.

Additionally, the Information Security section is enhancing UNICEF global threat detection and response capabilities by deploying a new set of tools and companion services and making them available for integration with especially purpose-built digital products.

This post is instrumental to the maturation of the Cybersecurity Architecture and Engineering practice, and the implementation of the necessary changes that will support it.



Purpose for the job *(Please outline the overall responsibility of this position)*

The role is a dynamic and pivotal one within the ICT Division. The incumbent is a technical lead with strong managerial skills and deep technical knowledge, that will strategically guide a unit that will mature UNICEF's Cybersecurity Architecture and Engineering practice, creating global standards and guidelines, directly contributing to the design of high profile global digital platforms and products and providing direct support to the Global Digital Portfolio, and Regional and Country offices that design and develop digital products.

The Cybersecurity Manager will play an instrumental role in shaping the cybersecurity landscape of our organization by Maturing a Robust Cybersecurity Architecture and Engineering practice and contributing to better integrate Cybersecurity practices in the Digital Products Software Development Lifecycle.

The position will also enhance cybersecurity risk management by driving compliance and best practices in the areas of Software Development and Systems Design, fostering collaboration across sections, divisions and country offices involved on the development of digital products, cultivating a Security-First culture and innovating with cutting edge technologies and practices.

This position supervises the ICT Specialist (Cybersecurity Architecture and Engineering) **115562**. The position might also supervise consultants.

III. Key functions, accountabilities and related duties/tasks *(Please outline the key accountabilities for this position and underneath each accountability, the duties that describe how they are delivered. Please limit to four to seven accountabilities)*

Summary of key functions/accountabilities:

Manages and leads the Cybersecurity Architecture and Engineering unit:

- Provides leadership and supervision to the Cybersecurity Architecture and Engineering Unit.
- Establishes clear individual performance objectives, goals and timelines; provides timely guidance to enable the team to achieve their goals. Motivates and inspires staff so they perform at their best.
- Identifies training opportunities to meet staff development needs aligning with the Section goals.
- Builds a positive and collaborative work culture
- Nurtures and empowers talent so staff can reach their full potential.
- Collaborate with other IT and business units to promote a security-conscious culture.

Designs and Develop Global Cybersecurity Architecture and Engineering Guidelines and procedures:

- Develop and enhance a comprehensive Global Cybersecurity Architecture and Engineering practice, establishing forward-thinking digital products security strategies to promote proactive secure software and broader digital platforms design and development.
- Align security architecture and engineering efforts with overall security objectives and initiatives, in collaboration with the broader information security team and other relevant ICTD sections, such as TAO and SCS, and regional and country offices when applicable.

Supports the secure design and development of UNICEF flagship digital products and broader digital ecosystem:

- Partner with application development and operations teams, and business stakeholders to define and promote secure development practices for both existing and new digital products.
- Provide expert advice on developing and maintaining security standards, policies, and guidelines for application development in collaboration with other members of the Information Security team and other section SMEs.
- Enhance software security design standards, integrating security best practices throughout the entire software development life cycle (SDLC).
- Oversee and coordinate the security reviews and

Support to the broader UNICEF Cybersecurity program & Others:

- Under direct guidance from the Chief, Information Security leads the execution of cybersecurity projects and initiatives, ensuring their alignment with organizational strategic goals and deliver high-quality outcomes.
- Strategic Cybersecurity Architecture and Engineering Capacity Building: In partnership with other members of the Information Security team and ICTD Sections, promotes adoption of latest technologies in the expertise area, such as Application Security Testing Platforms, Cloud Security posture Management, Modern Threat Detection and Response, Identity and Access Management, and AI.
- Stays updated with industry trends and best practices through various industry conferences and training events.
- Oversees the development and management of related IT standards within the context of the UNICEF enterprise IT architecture to ensure appropriate degrees of standardization. Coordinates regularly with other IT teams and IT Field officers to ensure that all UNICEF Cybersecurity Architecture and Engineering related standards are up-to-date and properly documented.
- Builds and sustain effective close working partnerships with the ICTD Digital Core, Digital Centre of Excellence, DAPM, field and other counterparts through active sharing of information and knowledge.
- Evaluates proposals and negotiates contracts for platforms and tools related to Cybersecurity
- Any other related duties as requested by the Chief of Section.

IV. Impact of Results (*Please briefly outline how the efficiency and efficacy of the incumbent impacts its office/division and how this in turn improves UNICEF's capacity in achieving its goals)*

The Cybersecurity Manager is pivotal in building cyber security credibility and trust among our stakeholders by driving a solid base of delivery of services, a consistent track record of security service delivery, and developing strategic partnership with the internal and external stakeholders.

The Cybersecurity Manager ensures that the organization's Digital Tools and Platforms align with its strategic goals and adheres to UN and industry standards on the Cybersecurity realm. The staff's work is curial for the identification and mitigation of risks in some of our most critical systems, including those handling sensitive data of donors and beneficiaries. This work not only safeguards the organization's digital assets, but the security of those working with or served by our organization. Furthermore, through successful delivery of Cybersecurity Architecture and Engineering related initiatives and strategic learning, the Cybersecurity Manager helps drive innovation and continuous improvement within the organization, reinforcing its reputation as a leader in its field.

V. Competencies and level of proficiency required (please base on UNICEF Competency Profiles)

Core Values

- Care
- Respect
- Integrity
- Trust
- Accountability
- Sustainability

Core competencies

- Builds and maintains partnerships
- Demonstrates self-awareness and ethical awareness
- Drive to achieve results for impact
- Innovates and embraces change
- Manages ambiguity and complexity
- Thinks and acts strategically
- Works collaboratively with others
- Nurtures, leads and manages people

Functional Competencies:

- Formulating Strategies & Concepts [II]
- Analyzing [II]
- Applying technical Expertise[III]
- Planning and Organizing [II]
- Leading & Supervising [II]

VI. Recruitment Qualifications

Education:	An Advanced University Degree in Computer Science or related field with a Strong Cybersecurity Focus is required. *A first University Degree in a relevant field combined with additional 2 years of professional experience may be accepted in lieu of an Advanced University Degree.
Experience:	A minimum of 8 years of progressively responsible work experience in an international development is required, including: • Experience leading software development teams in development / humanitarian contexts. • Experience with Agile practices and DevSecOps methodologies. • Strong working experience with Cloud environments, with a focus on Microsoft Azure and Cloud Native Foundation technologies (I.E. Kubernetes) • Experience successfully contributing to the security design in large, complex software development projects. • Experience working with and extending the Microsoft Security Stack (Defender XDR, Sentinel)

	• Experience supporting multiple stakeholders in a large context/geographically dispersed organization. • Understanding and experience with Information Management Systems in a humanitarian context. • Working experience in vendor and contract management. • Experience writing technical guidelines, procedures, and code samples.
Language Requirements:	Fluency in English is required. Knowledge of another UN language (Arabic, Chinese, French, Russian or Spanish) is desirable.
Other Skills and Attributes	• Knowledge and ability to perform information security and IT risks analyses, including conducting security assessments and code reviews to verify the effectiveness of security measures in custom developed applications. • Proficiency on the use of software development security tools such as static code analysis, dynamic code analysis, and dependency analysis (e.g., GitHub Advanced Security Tools, Fortify on Demand, Veracode). • Clear understanding of Information Security aspects in software development lifecycle and Application support • Ability to foster excellent work relationships and build alliances with key stakeholders and industry business partners. • Ability to support multiple projects and resources concurrently, including ability to assess benefits, risks, and costs. • Ability to learn the business unit's functions and understand the strategic business goals to identify opportunities for technology innovation and to analyze and propose technical strategies for the business units. • Ability to stay abreast of new technologies and their ability to support UNICEF innovation projects to improve efficiency and effectiveness of business units.

VII. Signatures- Job Description Certification

Sebastian Bana	Signature	Date
Chief, Information Security		
Name: Christian Larsson	Signature	Date
Title: Director, ICTD		