Job Description
Cost-Free Expert

Functional Title:	**Identity and Access Management Specialist**
Grade:	**P4**
Organizational Unit:	**Application Development Team**
	Development Section
	Office of Information and Communication Systems
	Department of Safeguards

Organizational Setting

The Department of Safeguards (SG) is the organizational hub for the implementation of IAEA safeguards. The IAEA implements nuclear verification activities for some 180 States in accordance with their safeguards agreements. The safeguards activities are undertaken within a dynamic and technically challenging environment including advanced nuclear fuel cycle facilities and complemented by the political diversity of the countries.

The Department of Safeguards consists of six Divisions: three Operations Divisions: A, B and C, for the implementation of verification activities around the world; three Technical Divisions: Division of Concepts and Planning, Division of Information Management, and Division of Technical and Scientific Services; as well as two Offices: the Office of Safeguards Analytical Services and the Office of Information and Communication Services.

Within the Department of Safeguards, the Office of Information and Communication Systems (SGIS) is the centre of competence for the specification, development and maintenance of Information and Communication Technology (ICT) systems and for the management of all ICT infrastructure and services to support safeguards. In partnership with other organizational entities, SGIS is responsible for planning and implementing an ICT strategy as well as enforcing ICT standards.

The Development Section provides ICT services to the Department of Safeguards and Member States, working cooperatively with staff in the Operations Divisions and the Technical Divisions to plan, establish and maintain information systems. The Section specializes in providing system analysis, software design, and implementation and maintenance services. The Section follows and implements best practices in the areas of software engineering, project management and quality management and continuously monitors the Department's information related needs so that they can be met through new or enhanced ICT solutions.

Main purpose

Under the general supervision of the Head of the Development Section, and reporting to the Team Leader for the Application Development Team, the Identity and Access Management Specialist provides specialized advice and guidance to the section in the area of information security and mitigating security vulnerabilities as well as manages the evaluation, implementation and maintenance of authorization systems for the Department of Safeguards.

Role

The Identity and Access Management Specialist is: (1) *an innovator*, developing new strategies and policies to securing our IT solutions; (2) *an expert* for IT identity and access management systems; (3) *a security analyst*, working with the development teams and user to establish and unify authorization approaches; (4) *a senior software engineer*, specifying, designing and ensuring implementation and enhancement to systems as well as customizing the identity and authorization systems.

Partnerships

The Identity and Access Management Specialist builds partnerships with various development teams and users to understand their requirements and assists in finding the most appropriate solution. The Identity and Access Management Specialist collaborates with colleagues in SGIS that are responsible for the infrastructure (middleware, service monitoring, networking, etc.), software engineering (standards, guidelines, etc.), and business analysis (business process).

Functions / Key Results Expected

- Develop innovative information security solutions to ensure that security risks are reduced or eliminated
- Provide specialised advice in information security to mitigate breaches and develop new policies, strategies, and tools to reduce security vulnerabilities
- Advocate and champion our security policies, procedures, and tools through clear communication initiatives and strategies
- Develop risk measurement criteria consistent with the Department's mission, which will enable the organization to determine where to effectively apply security controls
- Evaluate new IT technical architectures based on that risk measurement criteria and provide sound recommendations to ensure changes do not introduce vulnerabilities
- Provide advice and expertise in all aspects of application security to ensure standard compliance
- Build partnerships with various development teams to obtain consensus and appropriate solutions on information security initiatives.
- Perform all other related duties as assigned.

Knowledge, Skills and Abilities

- *Technical expertise:*
    - Strong expertise in the area of IT authorization technologies and standards.
    - Detailed knowledge of information security and secure coding techniques
    - Detailed knowledge of network configurations, security standards, and encryption.
    - Professional skills in software engineering tools, web service technologies, object oriented programming languages, web technologies, middleware, and database management systems.
    - Familiarity with international safeguards, nuclear material accounting, verification activities and State-supplied data handling is an asset.

- *Analytical skills and customer orientation:* Ability to analyse business processes and translate customer requests into ICT solutions.
- *Interpersonal skills:* Ability to establish and maintain good relationships with internal and external counterparts and to work harmoniously in a multicultural/multidisciplinary team with respect and sensitivity for diversity.
- *Communication skills:* Ability to write clearly and in a structured manner and to make effective oral presentations.
- *Knowledge management:* Openness to new ideas, technologies and tools in the IT industry and a willingness to learn and share skills and knowledge.
- *Teamwork:* Proven ability to work effectively as a member or leader of a multinational team with respect and sensitivity for diversity.

Education, Experience and Language Skills

- Advanced university degree (or equivalent) in computer science or a related field.
- Minimum of seven years of relevant practical experience in managing and customizing IT authorization solutions.
- Having advanced certifications in security, identity and access management is an asset (e.g. CISSP)
- Experience in all aspects of software engineering processes with demonstrated abilities in following formal software methodologies and a disciplined approach to software engineering.
- Fluency in written and spoken English. Knowledge of another official IAEA language (i.e. Arabic, Chinese, French, Russian, Spanish) an asset.