ROLE PROFILE

Position Title: Manager Tech Management & Security	**Reporting to:** Director Product Portfolio Management
Business Unit: Business	
Division: Product Hub	**Department:** Product Portfolio Management

A. ROLE AND CONTEXT

Purpose: This role is responsible to ensure that B2B products (ICT and Connectivity) are developed and maintained with the highest standards of security and data compliance. The role is also responsible for tech management and demand planning across the portfolio in close alignment with the technology teams and other external providers where relevant. Both areas of focus are meant to have a horizontal impact across product areas, realizing technical synergies and standards giving coherence to OQ B2B products portfolio and improving roadmap planning. The job holder will be responsible for integrating security standards and data compliance measures into the product development lifecycle, right from product security planning, architecture, implementation, operations and monitoring of each B2B product and service (ICT and Connectivity).	**Functional Context:** Ooredoo's Business BU is a critical part of the company's first line customer facing activities for all Business Accounts and has a significant role to play in long term business value creation through product design, achievement of sales revenue, profit and customer satisfaction, as defined in the annual business plans. The Product Hub focuses on productizing enterprise grade services for the B2B sector at Ooredoo Qatar covering core connectivity and ICT domains. It works closely with the Business Solutions unit specializing in delivering customized solutions, using products and services from the hub as foundational elements while forming direct partnerships for unique service integration and delivery. The B2B sector covers government, large enterprises as well as small to medium businesses.

B. ROLE ACCOUNTABILITIES

- Product Security Integration and Standardization
- Oversee the integration of security measures and standards throughout the B2B product development lifecycle right from development and launch upto decommissioning
- Plan security requirements, architecture, implementation, operations and monitoring and conduct regular security audits and assessments.
- Ensure privacy by design throughout the B2B product life cycle. Data privacy compliance needs to be maintained at all stages of product and solution design and operation until decommissioning.
- Implement advanced security features in products and technologies, such as encryption and identity management protocols (e.g., OAuth, SAML).
- Maintain security compliance throughout the product lifecycle, from design through deployment until decommissioning
- Keep up with the latest technology and security trends, including zero-trust architecture, blockchain, Artificial Intelligence and quantum cryptography, to drive innovation within the B2B product portfolio.
- Data Protection and Security Compliance and Governance
- Develop comprehensive security frameworks, policies, procedures, processes, architecture blueprints, and requirements to enhance OQ's technology and product security posture.
- Ensure that all OQ B2B products and technologies adhere to industrial security standards and regulatory requirements.
- Conduct regular data privacy and security audits/risk assessments for products' and technologies' Infrastructure
- Lead security incident responses and investigation to ensure rapid resolution and minimal impact on OQ operations and maintain an effective incident response plan.
- Technology Management and Demand Planning
- Provide guidance on end-to-end architectural considerations to effectively scale and evolve the product portfolio and features.
- Collaborate with product teams on roadmap planning, including the introduction of new services and the phasing out of legacy systems.
- Serve as the primary contact for internal technology demand planning (both BAU and quarterly), driving the realization of short- and long-term demand.

ROLE PROFILE

• Work with external partners (OEMs/Vendors) to ensure that B2B feature requirements are well-justified and integrated into partner roadmaps.
• Collaboration and Stakeholder Management
• Assess and manage relationships with internal technology teams and third-party vendors to ensure they meet OQ's security and data protection standards.
• Collaborate with Product Development teams to integrate security measures into B2B products, ensuring seamless security design and integration.
• Promote a culture of continuous improvement and professional development within the product team, enhancing awareness around security, data protection, and assurance.
• Work with compliance and legal teams to ensure products meet security regulatory and compliance requirements, addressing any legal implications related to security and data privacy.
• Support Sales and Customer Support teams by providing technical expertise and security guidance to OQ B2B clients, assisting in resolving complex security-related issues associated with OQ's product portfolio.

C. SCOPE AND INTERACTIONS

Direct Revenue Responsibility: No **Direct Budget Responsibility:** No **Direct People Management Responsibility:** No	**Primary Interactions (Internal/External)**	
	Internal Relationships: Cross Functional	**External Relationships:** Vendors Business Partners Customers

D. KEY PERFORMANCE INDICATORS (KPI)

• Compliance with security and data protection standards • Mean time to detect, contain and resolve • Incident response and investigation effectiveness • Customer satisfaction with security and data management handling • Roadmap planning and realization rate • Product performance

E. EXPERIENCE, QUALIFICATIONS AND SKILLS

Minimum Experience, Essential Knowledge & Skills	**Minimum Entry Qualifications**
10 years' experience in a similar role. Prior experience in technology management, IT demand planning, system security, compliance, and data privacy standardization, preferably in the telecom B2B sector. Deep understanding of technology architecture, Telco and ICT product know-how/management as well as information security Standards and best practices. Should be highly competent in deploying security and risk management tools and methodologies to protect and manage enterprise-level B2B products and services throughout the end-to-end product design, development, and deployment and decommissioning cycle. Hands-on experience in agile management of technology and demand planning across telecommunications and ICT product domains is required. Experience in product design and architecture is an advantage.	Bachelor's Degree in Computer Science or Technology or Engineering **Preferred Certifications / Other Qualifications** Relevant certifications in security, networking or systems architecture such as CISSP, CISM, cloud architecture, ITIL and TOGAF

ROLE PROFILE

Technical Competencies	Required Level	Behavioural Competencies	Required Level
Demand Management	Expert	Customer Focus	Basic
DATA PROTECTION	Advanced	Creative Thinking	Basic
SECURITY OPERATIONS	Expert	Quality and Continuous Improvement	Basic
AGILE/SCRUM	Advanced	Promoting Teamwork	Basic
TECHNOLOGY ARCHITECTURE	Advanced		
TECHNOLOGY ENABLEMENT	Advanced		

Competency Level (Reference Range)	Basic	Intermediate	Advanced	Expert
	Low >----------->----------->----------->High			