ROLE PROFILE

Position Title: Manager Incident Response & Investigation	**Reporting to:** Senior Manager Cyber Security Center
Business Unit: CEO	
Division: Corporate Information Security & Government Affairs	**Department:** Corporate Information Security

A. ROLE AND CONTEXT

Purpose: This role is responsible to ensure the security and integrity of Ooredoo's network and systems. This role also manages and leads dedicated professionals who monitor, detect, analyze, and respond to security incidents in real-time to minimize potential damage and maintaining the smooth functioning of our operations.	**Functional Context:** CEO's office works closely with Board of Directors, executive committee and audit committee members to facilitate & coordinate all of CEO's activities & functions. Job holder will be working closely with Board of Directors, executive committee and audit committee members to facilitate & coordinate all CEO's Office activities & functions. The Corporate Information Security division is responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected. It supports the department by identifying, developing, implementing and maintaining processes across the organization to reduce information and technology risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures as well as ensuring compliance. Securing information, technology and service availability through effective planning and management.

B. ROLE ACCOUNTABILITIES

- Oversee the daily CSC operations and ensure efficient incident response.
- Develop and maintain incident response plans, playbooks, and standard operating procedures (SOPs) to address various security incidents effectively.
- Collaborate with cross-functional teams within business units upon incident response and investigation e.g., Technology BU, Consumer BU, Business BU, Ooredoo Group (OG) and Ooredoo Financial Services (OFS).
- Monitor and analyse security event logs, network traffic, and system alerts to identify potential security incidents.
- Investigate security incidents promptly, employing industry -standard tools and techniques to determine the root cause, impact, and appropriate response.
- Coordinate incident response activities including containment, eradication, and recovery efforts to minimize the impact of security incidents.
- Work with CIS senior management to collaborate with external stakeholders such as law enforcement agencies, vendors and third-party for incident response and investigation as required.
- Stay updated on the latest cyber security threats, vulnerabilities, and industry best practices to enhance the capabilities of CSC.
- Conduct regular incident response drills and tabletop exercises to ensure preparedness and effectiveness of CSC team and other cross-functional teams as planned and arranged internally and externally.
- Produce comprehensive incident reports including post-mortem analysis, lessons learned and recommendations for improving incident response processes.
- Maintain and enhance security monitoring tools, ensuring their proper functioning and optimal performance.
- Drive continuous improvement initiatives within CSC, implementing advancements in technology as planned by the Security Architecture and Planning team in CIS, processes, and automation to enhance incident response capabilities.
- Act as a subject matter expert for security incidents in Ooredoo.

C. SCOPE AND INTERACTIONS

Direct Revenue Responsibility: No	**Primary Interactions (Internal/External)**

ROLE PROFILE

Direct Budget Responsibility: Yes **Direct People Management Responsibility:** Yes	**Internal Relationships:** Technology Business Consumer	**External Relationships:** Vendors Business Partners

D. KEY PERFORMANCE INDICATORS (KPI)

- Number of telecom and enterprise assets monitored.
- Number of incidents detected, responded, and investigated.
- Number of improvement plans implemented to enhance incident response.
- Instances of impact of security-related events on business operations identified.
- Impact of information security incidents identified.
- Information Security threats identified using threat hunting and intelligence tools and feeds.

E. EXPERIENCE, QUALIFICATIONS AND SKILLS

Minimum Experience, Essential Knowledge & Skills	**Minimum Entry Qualifications**
10 years' experience in a similar role. Expert in the field of: Incident response and digital forensic investigation for enterprise and telecom infrastructure. Strong knowledge of mobile and fixed networks and architectures including LTE & IMS. Knowledge of frameworks like eTOM, ITIL, COBIT.	Bachelor's Degree in Computer Science or Engineering or Telecom Engineering **Preferred Certifications / Other Qualifications** CISSP, CISM, GCIH, CHFI or SANS incident response certifications.

Technical Competencies	**Required Level**	**Behavioural Competencies**	**Required Level**
RISK MANAGEMENT	Advanced	Building Customer Value	Intermediate
CYBERSECURITY ARCHITECTURE & PLANNING	Expert	Delivering Results & Fostering Collaboration	Intermediate
SECURITY OPERATIONS	Advanced	Shaping Strategy	Intermediate
PLANNING + (P&L FIT)	Intermediate	Driving Change	Basic
		Networking and Influencing Collaboratively	Basic
		Leading Teams	Basic

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