|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – INCIDENT INVESTIGATION MANAGER** | | | | | |
| **Sector** | Infocomm Technology | | | | |
| **Track** | Cyber Security | | | | |
| **Sub-track** | Incident Response | | | | |
| **Occupation** | ICT Security Specialist | | | | |
| **Job Role** | **Incident Investigation Manager** | | | | |
| **Job Role Description** | The Incident Investigation Manager plans and oversees the performance of security response during the event of a cyber-incident or threat. He proposes mitigation techniques and countermeasures as well as develops cyber security solutions to prevent future attacks. He develops and implements cyber incident response strategies. He presents cyber-incident reports to senior leaders. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.  He is familiar with cyber security standards, protocols and frameworks, and ensures the organisation’s compliance to the Cyber Security Act 2018. He is knowledgeable in using various cyber security analysis tools and techniques to resolve incidents.  The Incident Investigation Manager is diligent and watchful in monitoring security operations, systems and activities. He is quick to provide solutions and fix issues when they arise. He is adept at dealing with complexity, and is an articulate and developmental leader in his team. | | | | |
| **Critical Work Functions, Key Tasks and Performance Expectations** | **Critical Work Functions** | **Key Tasks** | | | **Performance Expectations** |
| **Develop and implement cyber incident response strategy** | Develop contingency and disaster recovery plans tailored specifically for every security incident | | | In accordance with:     * Cyber Security Act 2018, Cyber Security Agency of Singapore |
| Establish incident response policies and standards for the organisation | | |
| Develop incident response processes and policies, refreshing them where required | | |
| Advise senior management on major information security-related risks and cyber incident response strategies | | |
| **Oversee cyber threat analysis** | Oversee the identification of security risks and exposures to internal systems | | |
| Optimise cyber security data analytics models to pre-empt and detect suspicious activities | | |
| Provide risk analysis and security design advice to internal software and system design teams | | |
| Oversee the sharing of cyber threat intelligence with security partners, vendors and law enforcement | | |
| Oversee the development of cyber security solutions to prevent future cyber incidents | | |
| **Manage people and organisation** | Review operational strategies, policies and targets across teams and projects | | |
| Develop strategies for resource planning and utilisation | | |
| Review the utilisation of resources | | |
| Oversee the development of learning roadmaps for teams and functions | | |
| Establish performance indicators to benchmark effectiveness of learning and development programmes against best practices | | |
| Implement succession planning initiatives for key management positions | | |
| **Skills and Competencies** | **Technical Skills and Competencies** | | | **Generic Skills and Competencies** | |
| Budgeting | | Level 5 | Communication | Advanced |
| Business Performance Management | | Level 5 | Developing People | Advanced |
| Cyber and Data Breach Incident Management | | Level 4 | Problem Solving | Advanced |
| Cyber Forensics | | Level 4, Level 5 | Resource Management | Advanced |
| Cyber Risk Management | | Level 5 | Sense Making | Advanced |
| Learning and Development | | Level 4, Level 5 |  | |
| Manpower Planning | | Level 4 |
| Networking | | Level 4 |
| People and Performance Management | | Level 4 |
| Security Assessment and Testing | | Level 4 |
| Security Governance | | Level 5 |
| Security Strategy | | Level 5 |
| Stakeholder Management | | Level 4, Level 5 |
| Strategy Implementation | | Level 4 |
| Strategy Planning | | Level 5 |
| Threat Analysis and Defence | | Level 4 |
| Threat Intelligence and Detection | | Level 4 |
| **Programme Listing** | For a list of Training Programmes available for the ICT sector, please visit: www.skillsfuture.sg/skills-framework/ict | | | | |
|  |  | |  |  |  |
| The information contained in this document serves as a guide. | | | | | |