|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – FORENSICS INVESTIGATION MANAGER** | | | | | | |
| **Sector** | Infocomm Technology | | | | | |
| **Track** | Cyber Security | | | | | |
| **Sub-track** | Forensics Investigation | | | | | |
| **Occupation** | ICT Security Specialist | | | | | |
| **Job Role** | **Forensics Investigation Manager** | | | | | |
| **Job Role Description** | The Forensics Investigation Manager plans and oversees the investigation processes and protocols after a cyber-threat or incident. He/She is responsible to ensure that the data is collected and analysed properly. He is also responsible for developing a forensics investigation strategy and overseeing the forensics investigations to ensure the threat is classified and future actions are recommended to the affected stakeholders.   He is familiar with different types of threats, cyber security standards, protocols and frameworks, and ensures the organisation’s compliance with the Cyber Security Act 2018. He is knowledgeable of hardware and software applications to analyse threat data from various sources.   The Forensics Investigation Manager is diligent and watchful in the investigation activities. He is also a confident leader who develops plans and solutions to address security incidents, and has a passion for engaging and developing others in his team. | | | | | |
| **Critical Work Functions, Key Tasks and Performance Expectations** | **Critical Work Functions** | **Key Tasks** | | | **Performance Expectations** | |
| **Develop a forensics investigation strategy** | Develop strategy to collect and analyse threat data after an incident | | | In accordance with:     * Cyber Security Act 2018, Cyber Security Agency of Singapore | |
| Establish digital forensic investigation policies and standards for the organisation | | |
| Develop threat mitigation processes and policies after analysing the root cause of the incident, refreshing them when required | | |
| Advise senior management on major information security-related risks and forensics investigations policies and procedures | | |
| **Oversee forensic investigations** | Lead forensic investigations and coordinate forensic teams post cyber-attacks to determine the root cause of the incident | | |
| Scrutinise forensic incident trends to ensure correct measures are taken during the investigation process | | |
| Determine the tactics, techniques and procedures used for cyber attacks | | |
| Manage the evidence and causal analysis of cyber threats, incidents and attacks | | |
| Present reports and outcomes in investigations or legal proceedings to senior management and key stakeholders | | |
| **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 Forensics | | Level 4, Level 5 | Problem Solving | | Advanced |
| Cyber Risk Management | | Level 5 | Resource Management | | Advanced |
| Emerging Technology Synthesis | | Level 4 | Sense Making | | Advanced |
| Failure Analysis | | Level 4 |  | | |
| Learning and Development | | Level 4, Level 5 |
| Manpower Planning | | Level 4 |
| Network Security | | Level 4 |
| Networking | | Level 4 |
| People and Performance Management | | Level 4 |
| Security Administration | | Level 4 |
| Security Assessment and Testing | | Level 5 |
| Security Governance | | Level 5 |
| Security Strategy | | Level 5 |
| Stakeholder Management | | Level 4, Level 5 |
| Strategy Implementation | | Level 5 |
| 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. | | | | | | |