|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – PRODUCT SECURITY ENGINEER** | | | | | |
| **Sector** | Infocomm Technology | | | | |
| **Track** | Product Development | | | | |
| **Sub-track** | Quality, Risk and Security | | | | |
| **Occupation** | Product Security Engineer | | | | |
| **Job Role** | **Product Security Engineer** | | | | |
| **Job Role Description** | The Product Security Engineer conducts cyber risk assessment in support of product development, existing product upgrades and new launches to help identify IT related risk and determines appropriate controls to mitigate risks. He/She monitors, identify recurring security issues in each product, tracks and manages risk mitigations and exceptions to ensure cyber security standards and policies are established. He applies a defined set of analytical or scientific methods and works independently. He is also responsible for documentation of cyber risk assessment reports.  He is also responsible for performing real-time analysis of products and trending of security log data from various security devices and systems on products. He responds to user incident reports and evaluates the type and severity of security events.  He is familiar with cyber security standards, protocols and frameworks, and acts in accordance with the Cyber Security Act 2018. He uses various cyber security monitoring and analysis tools and techniques depending on the organisation's needs and requirements.  The Product Security Engineer is vigilant and systematic in identifying cyber risks, and takes an analytical approach to performing real-time analysis and investigating issues. He communicates well both verbally and in writing. | | | | |
| **Critical Work Functions, Key Tasks and Performance Expectations** | **Critical Work Functions** | **Key Tasks** | | **Performance Expectations** | |
| **Establish cyber security standards and policies** | Conduct review of existing security policies, procedures, standards and exceptions | | In accordance with:     * Cyber Security Act 2018, Cyber Security Agency of Singapore | |
| Assist in the development of policies for conducting cyber security risk assessments and compliance audits | |
| Support implementation of information systems and cyber security policies | |
| **Manage cyber risks and assessments** | Perform cyber risk assessment activities based on risk assessment plans | |
| Assess third party security controls and internal security systems | |
| Establish scope of risk analysis for new technology initiatives | |
| Conduct research on emerging cyber security and risk management trends, issues, and alerts | |
| Monitor risks and incidents in accordance with the risk mitigation policies and guidelines | |
| **Mitigate cyber security risks**  **and respond to cyber security incidents** | Determine cause of security violations in products | |
| Assist in establishing procedures for handling detected cyber security incidents in products | |
| Recommend corrective actions or appropriate controls to mitigate technical risks in products | |
| Assist in the implementation of preventive measures against intrusion, frauds, attacks or leaks and correction of cybersecurity breaches in products | |
| Track remediation efforts for security and audit deficiencies in products | |
| **Skills and Competencies** | **Technical Skills and Competencies** | | **Critical Core Skills** | | |
| Audit and Compliance\* | Level 3 | Sense Making | | Intermediate |
| Cyber and Data Breach Incident\* Management | Level 3 | Transdisciplinary Thinking | | Basic |
| Cyber Risk Management\* | Level 4 | Problem Solving | | Intermediate |
| Data Analytics\* | Level 3 | Collaboration | | Intermediate |
| Data Governance\* | Level 4 | Decision Making | | Basic |
| Network Security\* | Level 4 |  | | |
| Security Administration\* | Level 3 |
| Security Education and Awareness\* | Level 3, Level 4 |
| Security Governance\* | Level 4 |
| Security Programme Management\* | Level 3 |
| Agile Software Development | Level 3 |
| AI Ethics and Governance | Level 2, Level 3 |
| Applications Development | Level 3 |
| Business Continuity | Level 4 |
| Business Needs Analysis | Level 3 |
| Cyber Forensics | Level 2 |
| IT Governance | Level 4 |
| Partnership Management | Level 3 |
| Process Improvement and Optimisation | Level 3 |
| Product Management | Level 3 |
| Quality Standards | Level 4 |
| Software Design | Level 3 |
| Software Testing | Level 2, Level 3 |
| Stakeholder Management | Level 2, Level 3 |
| Strategy Implementation | Level 3 |
| Strategy Planning | Level 4 |
| Test Planning | Level 2, Level 3 |
| Threat Analysis and Defence | Level 2 |
| Threat Intelligence and Detection | Level 2 |
| **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.  \*Note: Technical Skills and Competencies (TSCs) with an asterisk (\*) refer to Priority Skills (i.e., TSCs to be prioritised for this role). | | | | | |