|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Operations and User Support | | | | | |
| **TSC Title** | Cyber and Data Breach Incident Management | | | | | |
| **TSC Description** | Detect and report cyber and data-related incidents, identify affected systems and user groups, trigger alerts and announcements to relevant stakeholders and efficient resolution of the situation. | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  | **ICT-OUS-2003-2.1** | **ICT-OUS-3003-2.1** | **ICT-OUS-4003-2.1** | **ICT-OUS-5003-2.1** | **ICT-OUS-6003-2.1** |
|  | Provide real-time incident and status reporting, and identify affected systems and user groups | Troubleshoot incidents, escalate alerts to relevant stakeholder, and analyse root causes and implications of incidents | Develop incident management procedures and synthesise incident-related analyses to distil key insights, resolve incidents and establish mitigating and preventive solutions | Formulate incident response strategies and direct teams in the remediation, resolution, communication and post-mortem of large-scale, unpredictable cyber and data incidents | Drive cross-collaboration efforts to co-develop strategies to manage cyber and data incidents on an industry, national or international scale |
| **Knowledge** |  | * Incident detection and reporting protocols * Types of security incidents * Types of data breaches * Categorisation guidelines for incidents * Impact of incidents on systems and users * Personal Data Protection Act 2012 | * Prioritisation criteria for incidents * Tools and processes used to remedy incidents * Root cause analysis procedures * Security implications of incidents * Personal Data Protection Act 2012 | * Mechanics of incident alert triggers * Incident remediation solutions and strategies * Incident mitigation strategies * Personal Data Protection Act 2012 | * Industry standards and best practices in incident management * Key components of an incident management playbook * Criteria and requirements of an incident response team * Cyber incident mitigation strategies * Data breach mitigation strategies * Key stakeholder groups * Post-mortem processes related to cyber incidents * Personal Data Protection Act 2012 | * Political, national and international sensitivities regarding cyber crimes, incidents and breaches * Potential impact of incidents to the organisation and stakeholders * Types of cyber and data incident management strategies * Best practices in cyber incident management * Risk mitigation strategies for cyber and data breach incidents * Communication strategies and protocols for cyber and data incidents * Procedures to manage cyber and data incidents on an industry, national or international scale * Personal Data Protection Act 2012 |
| **Abilities** |  | * Maintain a tracker or log of incidents to provide real-time status reporting on affected systems * Report incidents, in line with incident management protocols * Gather relevant information about incidents * Categorise the importance of incidents based on established guidelines * Identify the systems and user groups affected by the incident based on information gathered * Assist in mitigation of repeat incidents as directed * Document the modifications made to troubleshoot and resolve problems or incidents in the system | * Review categorisation of an incident, and determine its priority and need for escalation * Escalate alerts to relevant stakeholder groups upon the occurrence of incidents * Perform first responder troubleshooting on cyber-related, data-related or security incidents, by following pre-determined procedures * Analyse incident reports, log files and affected systems to identify threats and root causes of incidents * Perform incident triage to assess severity of incidents and security implications * Implement approved processes or technologies to mitigate future incidents | * Develop mechanisms or threat signatures that trigger incident alerts to relevant parties and systems * Integrate cyber- and data-related information, alerts and analysis from detection system logs to develop a holistic view of incidents * Distil key insights and impact from analyses of incidents * Manage the containment of cyber and data incidents within the organisation * Lead recovery of contained security incidents * Establish mitigation and prevention processes and policies * Drive implementation of mitigation processes and policies | * Establish incident management procedures for the detection, reporting and handling of incidents * Develop a playbook for cyber and data incident management * Lead an incident response team * Lead the remediation and resolution of cyber and data incidents at the organisational level * Resolve large-scale, unpredictable incidents * Make key decisions on when and how to communicate incidents to different critical stakeholders * Direct post-mortem activities following critical incidents * Develop organisation-wide cyber and data incident mitigation strategies | * Direct the management of cyber and data incidents on an industry, national or international scale * Manage incidents to minimise significant reputational risk to the organisation * Lead collaboration across industries to manage large-scale cyber and data security incidents * Co-develop cyber and data incident management strategies on a national level with external experts and stakeholders * Lead critical communications to the public, authorities, internal and external stakeholders |
| **Range of Application** | For Data Protection-related programmes, please refer “Guide to Develop Training Courses for Data Protection Officer (DPO)”, Personal Data Protection Commission (PDPC), <http://www.pdpc.gov.sg/dp-competency> [March 2020] | | | | | |