|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Governance and Compliance | | | | | |
| **TSC Title** | Data Protection Management | | | | | |
| **TSC Description** | Develop and implement a Data Protection Management Programme to comply with the Personal Data Protection Act 2012 | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  |  | **ICT-CGP-3020-1.1** | **ICT-CGP-4020-1.1** | **ICT-CGP-5020-1.1** |  |
|  |  | Collect, use or disclose personal data in accordance with the organisation’s Data Protection Management Programme (DPMP) | Develop the organisation’s Data Protection Management Programme (DPMP) in accordance with legal requirements | Formulate the organisation’s data protection strategy and ensure effectiveness of Data Protection Management Programme (DPMP) |  |
| **Knowledge** |  |  | * Definition of personal data * Organisation’s processes, procedures and guidelines of DPMP * Personal Data Protection Act 2012 (PDPA) * PDPA and the data lifecycle * Obligations under the PDPA * Accountability under the PDPA * Best practices in operationalising PDPA | * Components of a DPMP * Data lifecycle * Personal Data Protection Act 2012 (PDPA) * DPMP and its relationship to the data lifecycle * Dynamic and iterative consent approaches to comply with the consent requirement under PDPA * Circumstances that may allow for exemptions from all or any of the PDPA provisions * Methods to document personal data flows * PDPA Assessment Tool for Organisations (PATO) | * Data Protection by Design (DPbD) approach * Data Protection Impact Assessment (DPIA) * Best practices in data protection * Principles in data protection policy * Personal Data Protection Act 2012 (PDPA) |  |
| **Abilities** |  |  | * Obtain consent to collect, use or disclose individuals’ personal data * Allow individuals to withdraw consent * Collect, use or disclose personal data only for the purpose for which consent was obtained * Notify individuals of the purposes for the collection, use or disclosure of their personal data * Correct errors or omissions in individuals’ personal data upon request * Ensure accuracy and completeness in the collection of personal data * Cease retention or anonymise personal data when it is no longer necessary for business or legal purposes | * Document the flows of personal data within the organisation * Create content registry to record consent provided by individuals to the organisation * Identify key gaps and areas for improvement in data protection * Develop processes to handle data breach incidents * Publish information on the organisation’s data protection policies, practices and compliant-handling process * Determine the circumstances under which organisations must seek fresh consent for the use of personal data * Designate data protection roles and responsibilities within the organisation * Adopt innovative processes and methods to comply with PDPA requirements * Submit reports of data protection measures to senior management | * Review the organisation’s DPMP to determine gaps and areas for improvement * Formulate the organisation’s regional DPMP * Conduct a DPIA to identify, assess and address personal data protection risks based on the organisation’s functions, needs and processes * Assess if the handling of personal data complies with the PDPA or data protection best practices * Introduce technical or organisational measures to safeguard against data protection risks to individuals * Designate regional data protection roles and responsibilities within the organisation |  |
| **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] | | | | | |