ANNEX A

OVERVIEW OF CERTIFICATION REQUIREMENTS

The certification requirements are based on four key principles, each framed by a set of assessment criteria and controls. They are:

Principle 1: Governance and Transparency

Appropriate Policies and Practices
An organisation will be assessed on its data protection policies and practices; queries, complaints and dispute resolution handling processes; and data breach management plan.

Openness
An organisation will be assessed on its data protection policies and practices such as the appointment of a Data Protection Officer (DPO), the establishment of an appropriate data protection governance and support structure, and providing information on personal data protection policies to external stakeholders.

Internal Communication and Training
An organisation will be assessed on its communication of data protection policies and practices to all employees, and implementation of data protection training for all employees.

Principle 2: Management of Personal Data

Appropriate Purpose
An organisation will be assessed on its policies and practices in ensuring the collection of personal data is for purposes that are clear and appropriate in the circumstances.

Appropriate Notification
An organisation will be assessed on its policies and practices in ensuring notification of individuals of the purposes for the collection of their personal data, and ensuring notification of new purposes before the use or disclosure of their personal data.

Appropriate Consent
An organisation will be assessed on its policies and practices in ensuring that consent of individuals has been obtained for the purposes for the collection of their personal data, and ensuring that consent for personal data with special considerations (e.g. minors' personal data) has been obtained.

Appropriate Use and Disclosure
An organisation will be assessed on its policies and practices in ensuring the use and disclosure of personal data is for purposes for which consent of the individuals has been obtained.

Compliant Overseas Transfer
An organisation will be assessed on its policies and practices in ensuring appropriate personal data transfer policies are implemented as required under the PDPA.

Principle 3: Care of Personal Data

Appropriate Protection
An organisation will be assessed on its policies and practices in ensuring reasonable security policies and practices are implemented, including by third parties handling personal data on its behalf, and ensuring regular testing of security safeguards.

Appropriate Retention and Disposal
An organisation will be assessed on its policies and practices in ensuring appropriate personal data retention policies are implemented, including for the disposal, destruction or anonymisation of personal data when there are no longer legal or business purposes to retain the personal data.

Accurate and Complete Records
An organisation will be assessed on its policies and practices in ensuring personal data for use or disclosure is accurate and complete, and ensuring personal data disclosed to a third party organisation is accurate and complete.

Principle 4: Individuals' Rights

Effect Withdrawal of Consent
An organisation will be assessed on its policies and practices in ensuring provision for withdrawal of consent for the collection, use or disclosure of individuals' personal data.

Provide Access and Correction Rights
An organisation will be assessed on its policies and practices in ensuring provision for individuals' access to and correction of their personal data in the organisation's possession or under its control on request.