DATA PROTECTION POLICY

1. INTRODUCTION

1.1 The Data Protection Policy (the "**Policy**") sets the standards of conduct and operating procedures that MOHH staff are to comply with in connection with data in the possession or under the control of the MOHH Group.

1.2 This Policy demonstrates the Company's commitment to develop and implement policies and practices to meet its obligations in respect of the following:

(i) **managing personal data** under the Personal Data Protection Act 2012 ("**PDPA**"); and

(ii) **managing all types of data** in compliance with the HealthTech Instruction Manual – Data Management Chapter ("**HIM-DM**") released by MOH. This Policy supplements the HIM-DM which shall be deemed incorporated as part of this Policy to the extent that it applies to MOHH and, in particular, incorporates the HIM-DM's requirements in respect of security classifications for data.

1.3 This Policy shall apply to MOHH staff including permanent employees, fixed term employees, contracted staff, temporary staff, secondees, interns, authorised third-party representatives or sub-contractors or agents engaged by MOHH.

2. OBJECTIVE

2.1 To strengthen the culture of care and responsibility for handling data in MOHH.

2.2 To develop, manage and maintain a robust data protection infrastructure in MOHH.

3. SCOPE

Information in General

3.1 This Policy is applicable to all activities in MOHH that involve the collection, use, disclosure and processing of data, including personal data, and information refers to such data in processed form. The classification and treatment of information as set out within this Policy applies to all information within MOHH and handled by MOHH staff whether received from external organisations or not. For clarity, the terms "data" and "information" cover data and information in any form.

Personal Data under the PDPA

3.2 Personal data refers to data, whether true or false, about an individual, whether living or deceased, who can be identified from that data; or from that data and other information that MOHH has or is likely to have access to. Examples of "personal data" include an individual's name, age, weight, height, NRIC/FIN number, medical records, income, race, blood type, fingerprints, marital status, religion, education, home address and telephone number(s).

4. CLASSIFICATION & TREATMENT OF INFORMATION

4.1 Information is classified into 2 categories, **Restricted** and **Unclassified**. Restricted category is further classified into 3 subsets based on impact of unauthorised disclosure.

Information Sensitivity Classification	Impact of Unauthorised Disclosure	
	On Individuals	**On Business Entities**
Restricted, Sensitive (High)	Causes **serious** physical, financial, or sustained emotional injury or social stigma	Causes **sustained** financial loss
Restricted, Sensitive (Normal)	Causes **temporary and minor** emotional distress or disturbance	Causes **reduction** in competitiveness or a compromise of business interests
Restricted, Non-Sensitive	**Does not** cause physical, financial, or emotional injury to the individual	**Does not** impact a business process or operations

Storage and Sharing Restrictions

4.2 All documents that contain sensitive and restricted information must be securely stored within office environment, on the office computers, or in locked cabinets.

4.3 MOHH staff may only disclose restricted information to another MOHH staff member who has a genuine and legitimate need for access to the data in order to carry out his/her job function.

4.4 Restricted information may be disclosed to authorised external parties only on a need-to-know basis. In addition to the aforesaid requirement, in disclosing Restricted, Sensitive (Normal) or Restricted, Sensitive (High) information to external parties, MOHH staff shall obtain the approval of the respective Director or Head of Department ("HOD").

4.5 MOHH staff shall ensure that the relevant measures, safeguards and security standards associated with the respective classification categories as may be issued pursuant to HIM-DM from time to time are complied with.

Document Labelling

4.6 Documents are to be labelled clearly and prominently in accordance with the Information Sensitivity Classification as per sub-paragraph 1 i.e. "Restricted, Sensitive (High), "Restricted, Sensitive (Normal)" and "Restricted, Non-Sensitive". The classification to be marked on restricted information should be the highest classification of information contained in the document.

4.7 Within each Division, the approval of the HOD is required to upgrade, downgrade and declassify any information category. Where MOHH is acting as agent or under a data sharing arrangement, the consent of the originating entity providing the information shall be obtained before performing any declassification, downgrade or upgrade. Pending the decision of the originating entity, the information should be handled and protected at the higher classification.

4.8 Where data has been upgraded, downgraded or declassified, MOHH staff shall:

(a) maintain proper records and prominent marking of the revised classification on the material where required;

(b) notify the parties acting as MOHH's agent or under a data sharing arrangement who have received the information previously, so that consistent handling procedures can be applied;

(c) not reclassify information after it has been declassified and officially released to the public.

Clean Desk Policy

4.9 Where directed by their respective HODs, who shall have the authority to so direct to ensure security and privacy control, MOHH staff shall apply Clean Desk Policy which may entail any or all of the following:

(a) printed documents that contain sensitive and restricted information and laptops, tablets, and other hardware devices that are not secured by cable lock must be removed from the workstation and locked in cabinets when a workstation is not in use or unattended or unoccupied for an extended period of time.

(b) keys for accessing drawers or cabinets must not be left unattended at workstation.

(c) printed materials containing sensitive and restricted information must be retrieved immediately from the printer after printing. All printed materials left unclaimed at the printer at the end of the work day must be properly disposed of.

Disposing Requirement

4.10 When physical documents containing restricted information are no longer required, MOHH staff shall dispose of them using the company provided equipment on premises. MOHH staff shall ensure that the restricted information in physical documents remain securely stored in accordance with its classification pending completion of disposal. For bulk disposal at off-site premises by third-party service providers, MOHH staff shall observe the destruction process and record the declarations by the destruction personnel and witness.

5. MANAGING PERSONAL DATA: OBLIGATIONS UNDER THE PDPA

5.1 All MOHH staff shall ensure that the practices and processes in the handling of personal data comply with the obligations under the PDPA listed below.

(a) **CONSENT OBLIGATION**
An organisation must obtain the consent of the individual before collecting, using or disclosing his/her personal data for a purpose.

- MOHH staff must ensure that consent from the individual has been expressly given or deemed given by law, before collecting, using or disclosing his/her personal data for the specified purpose(s).
- If MOHH staff receive a request from an individual to withdraw his/her consent, staff are to inform the individual about the likely consequences of withdrawing consent, and comply with his/her request and stop retaining his/her personal data.
- Where personal data is obtained from external sources, MOHH staff must exercise appropriate due diligence to ensure that the external source can validly give consent for MOHH's collection, use and disclosure of personal data on behalf of the individual, or that the source had obtained consent from that individual for disclosure of his/her personal data to MOHH.

(b) **PURPOSE LIMITATION OBLIGATION**
An organisation may collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned.

- Each division dealing with personal data must identify the list of business purposes for collection, use or disclosure of personal data and inform the individuals concerned of these business purposes.

- MOHH staff may collect, use, or disclose personal data that are relevant for the business purposes, and only for purposes that a reasonable person would consider appropriate in the circumstances.

(c) **NOTIFICATION OBLIGATION**

An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

- MOHH staff must inform individuals of the business purposes for collecting, using or disclosing their personal data before collecting the data. If a new purpose arises for the use of personal data previously collected, such individuals must be informed of the said new purpose.

- As a good practice, MOHH staff should inform individuals in writing, such that the individual is clear about the purpose of usage/collection/disclosure and for easy reference in the event of any dispute.

(d) **ACCESS AND CORRECTION OBLIGATION**

An organisation must, upon request, (i) provide an individual with his/her personal data in its possession / control and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in its possession / control.

- If requested, MOHH must provide, to an individual, his/her personal data, and information about the ways in which the individual's personal data has been used or disclosed within a year before the date of the request.

(e) **ACCURACY OBLIGATION**

An organisation must make a reasonable effort to ensure that personal data collected by or on its behalf is accurate and complete if the personal data is likely to be (i) used by it to make a decision that affects the individual concerned or (ii) disclosed by it to another organisation.

- Where personal data is collected from an external source, MOHH staff must obtain written confirmation from the said source that he has verified the accuracy and completeness of the personal data. Otherwise, MOHH staff must conduct their own independent verification.

(f) **PROTECTION OBLIGATION**

An organisation must protect personal data in its possession / control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

- MOHH must protect personal data in its possession / control by taking appropriate administrative (eg. clear desk policy), physical (eg. keeping hard copies under lock and safe) and technical measures (eg. access control) to prevent unauthorised access, collection, use, disclosure, copying,

modification and disposal of such data.

- MOHH must ensure adequate, effective and appropriate security arrangements commensurate with the sensitivity of the data in question.

(g) **RETENTION LIMITATION OBLIGATION**

An organisation must stop retaining personal data once the purpose for collecting the personal data is no longer valid and the retention is no longer necessary for legal or business purposes.

- MOHH staff must stop retaining personal data as soon as such data is no longer required for legal or business purposes.

- MOHH staff must erase or anonymise the abovementioned personal data. Anonymising refers to removing the means by which personal data can be associated with particular individuals.

(h) **TRANSFER LIMITATION OBLIGATION**

An organisation must not transfer personal data outside Singapore except in accordance with the requirements prescribed under the PDPA.

- If MOHH's business purposes require personal data to be transferred overseas, ensure that –

  - such personal data is only transferred to organisations in overseas jurisdictions that have a comparable standard of data protection as the PDPA and the Personal Data Protection Regulations ("PDP Regulations"); or failing which,

  - the overseas recipients are contractually required to implement protective measures for personal data comparable to those in the PDPA and the PDP Regulations.

(i) **ACCOUNTABILITY OBLIGATION**

An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available.

- Divisions dealing with personal data are expected to document personal data flows in their respective business processes and review the flow of such data on a periodic basis. The purpose of such periodic reviews includes but is not limited to: (i) checking for compliance with obligations under the PDPA, (ii) identifying and assessing any data protection and information security risks (actual or potential), and (iii) taking appropriate remedial action.

- Any variations and supplements to this Policy shall be communicated to all MOHH staff via electronic means or through postings on MOHH's intranet homepage.

- This Policy may be supplemented by parameters set by HODs and data owners according to the circumstances and purposes the personal data serve.

- There shall be external data protection notice/s containing information on this Policy. External data protection notice/s shall be made publicly available online at the company's websites.

- The contact details of the MOHH Data Protection Officer ("DPO") shall be listed on the MOHH website. This is to allow members of the general public to inform MOHH, via the DPO if they:

  (a) Wish to rectify any incorrect or out-of-date personal data previously provided to MOHH;

  (b) Intend to withdraw any consent previously given to MOHH to collect, use, disclose and retain any such personal data;

  (c) Have any questions relating to any personal data shared with MOHH.

- MOHH divisions shall communicate to stakeholders in MOHH's projects / services / activities the ways in which their personal data is collected, used, disclosed, stored and safeguarded through appropriate notices.

6. MANAGING ALL TYPES OF DATA: BREACH AND INCIDENT HANDLING

6.1 All MOHH staff shall report any potential or actual leak of personal data to their HOD immediately. This is to enable procedures for containment of the breach to be initiated as soon as possible. In order to meet any incident reporting timelines stipulated in the PDPA or any other laws/regulations, the HOD shall make an assessment of the severity of the breach and, if necessary, escalate the matter to the DPO.

6.2 Particulars of the incident and measures taken in response to the incident shall be recorded and reported to the DPO as soon as possible, but in any case no later than 2 calendar days after any MOHH staff member becomes aware of the incident. The rationale for this is that the PDPA requires all organisations to notify the PDPC of all significant data breaches no later than 3 calendar days after the data breach is assessed to be of significant impact.

6.3 In the event that any vulnerabilities, gaps and/or data protection risk exposures are discovered by MOHH staff, the MOHH staff member should make a report of this to the HOD immediately for the HOD to take the appropriate remedial action.

6.4 In the event that any MOHH-issued electronic data storage device is lost, such an incident must be reported to (1) Division ICPC member (who will inform IT Admin and the HOD), and (2) the Police if the HOD deems necessary.

7. MANAGING ALL TYPES OF DATA: OBLIGATIONS UNDER THE HIM-DM

7.1 All MOHH staff shall be responsible in the use of all types of data in their possession. The principles relating to the use of personal data apply to the use of data generally.

7.2 MOHH staff must also acknowledge and agree to the Personal Undertaking: MOHH Group Policy on Data Protection and Data Security, administered via MOHH's Annual e-Declaration Exercise.

7.3 The failure of an employee to observe confidentiality of information in any MOHH Group entity is a breach of the terms and conditions of employment. The employee may be

subject to internal disciplinary action, including termination of employment.

7.4 The failure of an employee to comply with any MOHH Group entity's policies, terms and conditions for the use and access of IT systems, contractual obligations and/or obligations to applicable laws, may also render the employee liable to disciplinary action and legal action in the event of a data breach, and termination of access to any MOHH Group entity's information.

8. AUDIT AND RISK REPORTING STRUCTURE

8.1 Internal audits shall be conducted periodically to monitor and evaluate the implementation of this Policy and the practices at the division level.

8.2 DPO shall work together with MOHH's Enterprise Risk Management team in managing data protection risk.

* * * * *