APPENDIX – Requirements regarding handling of data breaches

Section A - Background

1. Some examples of Data Breach are illustrated below:

   (a) Loss of physical means on which CRIS' Personal Data is stored (collectively referred to as "**Storage Devices**"). Examples of such Storage Devices include computer notebooks, mobile devices such as mobile phones or tablets, data storage devices such as thumb drives, and paper records of CRIS' Personal Data.

   (b) Unauthorised access or disclosure of CRIS' Personal Data by employees of the Vendor.

   (c) Sending and/or disclosing of CRIS' Personal Data to wrong recipients e.g. through email or to physical address.

   (d) Improper disposal of CRIS' Personal Data.

   (e) Hacking of electronic Storage Devices.

   (f) Theft of Storage Devices.

   (g) Exploitation of errors or bugs in programming code of the Vendor's websites and/or databases by unauthorised third parties resulting in unauthorised access of CRIS' Personal Data.

Section B - Obligations

2. The Vendor agrees to handle Data Breaches in compliance with the relevant guidelines issued by the Personal Data Protection Commission ("**PDPC Guidelines**"), the relevant requirements set out in the policies relating to data breaches as may be issued by the Ministry of Health from time to time (the "**MOH Policies**"), and any and all policies, guidelines, notices and circulars relating to data breaches which CRIS may from time to time notify in writing to the Vendor ("**CRIS Circulars**"). The PDPC Guidelines have been taken in consideration in the drafting and implementation of the CRIS Circulars.

3. Parties also agree to comply with the requirements set out below in relation to the handling of Data Breaches. In the event of a conflict between the obligations set out below, the PDPC Guidelines applicable at the time of the Data Breach, and the MOH Policies applicable at the time of the Data Breach, the conflict shall be resolved in the following order of priority: (1) the MOH Policies; (2) the CRIS Circulars; (3) PDPC Guidelines; (4) the obligations set out below.

   (a) NOTIFICATION TO CRIS

   In the event that the Vendor is aware of a Data Breach in respect of CRIS Personal Data, the Vendor shall immediately notify CRIS .

   Such notification should be made to CRIS no later than twenty-four (24) hours from the time the Vendor first becomes aware of the Data Breach. The notification form template is provided in Annex A below. For the avoidance of doubt, CRIS reserves the right to amend the notification form template in Annex A from time to time PROVIDED ALWAYS that the notification form template complies with and is subject to the MOH Policies, including but not limited to the HealthTech Instruction Manual. Any amendments to the notification form template made by CRIS shall be notified in writing to the Vendor.

   (b) CONTAINMENT OF DATA BREACH

   The Vendor should take immediate steps to contain the Data Breach. This typically means that any further access to or disclosure of CRIS' Personal Data affected by the Data Breach should

be limited to authorised persons who need such access or disclosure to rectify or mitigate the Data Breach. Examples of steps which may be taken to contain the Data Breach include:

a) Shutting down and/or isolating the system(s) which was involved in the Data Breach; and
b) Stopping practices and processes that led to the Data Breach.

The Vendor shall notify CRIS as soon as practicable regarding the steps it has taken to contain the Data Breach.

(c) PROVIDING ASSISTANCE AND COOPERATION

The Vendor shall work closely with CRIS to remedy and mitigate the Data Breach, and shall provide relevant updates to CRIS regarding its response to the Data Breach as soon as practicable.

The Vendor shall also provide all necessary assistance and cooperation to CRIS in relation to any investigation of the Data Breach conducted by CRIS and/or any claim, allegation, action, proceeding or litigation involving CRIS which arises out of or in connection with the Data Breach.

(d) EVALUATION AFTER RESOLUTION OF THE DATA BREACH

After the Data Breach has been resolved, the Vendor and CRIS shall share findings with one another regarding how to prevent future Data Breaches. Such findings may include:

(a) assessment of the need to implement or to continue with any remediation actions and/or correction actions;
(b) identification of areas of weakness and the actions needed to strengthen such areas; and
(c) assessment of the effectiveness of the response(s) to the Data Breach.

Annex A – Data Breach Notification Form template

IMPORTANT NOTE: Please ensure that the completed form is submitted via email to the Data Protection Officer(s) of CRIS.

Report Date:	Report Time:
Notifying Party:	

1. Particulars of representative of Notifying Party ("Reporter")	
Name:	Designation:
Telephone No:	Department / Division:
Email Address:	
2. Details of Data Breach Incident	
Date Noted: (observation)	Time Noted:
Date Occurred: (earliest known occurrence)	Time Occurred:

Description of Incident:

Section A – Critical Information regarding the Incident

*Instructions: Please provide answers to **all** of the following questions in order for the Affected Parties to conduct their initial assessment of the risks arising from the Incident.*

(i) What was the cause(s) / suspected cause(s) of the Data Breach? *(Please refer to paragraph 2 of the Appendix for examples of possible causes, and provide as much information as possible regarding the cause(s) / suspected cause(s)).*

(ii) Is the Data Breach still ongoing?

(iii) How many individuals were affected by this Incident?

(iv) What types of CRIS Personal Data was involved in this Incident? Please indicate all data fields exposed as a result of this Incident.

(v) Were any CRIS Platforms affected by the Incident? If so, please indicate which CRIS Platforms were affected.

Section B – Other relevant information regarding the Incident

Instructions: Please provide answers to as many of the following questions as possible.

(vi) Who was / were the recipient(s) of the data involved in the data breach incident?

(vii) Were there any consequences and / or impact on the affected individuals? If so, do elaborate them here.

(viii) Were there any consequences and / or impact on CRIS? If so, do elaborate them here.

(ix) Were there any efforts taken by the Vendor to contain and investigate the incident? If so, do elaborate them here.