**Data Retention and Disposal Policy for Student and Staff Data in the Banner ERP System**

**Version 2: January 17, 2020**

1. **Purpose**

The purpose of this policy is to ensure personal data stored in the Banner ERP System are protected and maintained properly and to ensure the data that are no longer needed by the University or are of no value are discarded within a proper period of time. This policy is set up based on the guidelines provided by the Privacy Commissioner for Personal Data (PCPD) of HKSAR.

1. **Scope**

This policy covers all student and staff records and data stored in the Banner ERP System.

**2.1** **Out of Scope**

This policy does not cover data stored in either digital or paper forms outside of the Banner ERP Sysem. Examples include but are not limited to data on non-ITSC managed systems, data stored in user PCs, file servers, mobile storage, e-mail, SharePoint, Network share drives, etc.

1. **Review**

This policy must be reviewed regularly to keep pace with work practices of the University, technology developments, and regulatory changes.

1. **Data Retention and Disposal Principle**

The principle of “Need to know” shall be applied to retain or dispose the student and staff records as they are all personal data and should be kept in the Banner ERP System for maintaining the operation of the University only. Data owners should review the necessity and accuracy of the data that are stored in the system from time to time. All unnecessary personal data should not be kept in the system.

1. **Retention of Data**

At the coordination by the Chief Data Protection Officer (DPO), all data owners of the student and staff records discussed and agreed to retain the different data fields of these records as specififed in **Appendix 1**. In any data field where different departments have different retention periods for their operational needs, the principle of using the longest retention period is adopted to determine the retention period for that particular data field. Data owners are required to review and re-define the retention period of the data according to their operational needs and legal requirements. If data are accessible by multiple parties, the respective data owner should establish agreement with all data users the longest period of time that the data should be retained.

1. **Disposal of Data**

Records and data should be removed from the systems as soon as they have exceeded the retention period defined by the data owners together with the data users as specified in Appendix I.

**6.1 Data disposal schedule**

**6.1.1** **Immediate Deletion (I)** – Those data fields marked with “I” in Appendix 1 will be deleted after the data subject has left the University. It will be carried out annually on or before December 31. All staff with status “TERMINATED” (PEAEMPL status as terminated) and students that have become inactive will be included.

**6.1.2** **Permanent (P)** – Those data fields marked with “P” will be kept permanently and thus will not be deleted.

**6.1.3** **Number of years (1,2,3 or more)** – Those data fields marked with a number indicate the specified years they will be kept. Deletion will be carried out 1 year after the expiry of the retention period. The "7 tax years" is defined as 7 tax years calculated from the last working day of the staff, meaning that the data field will be deleted annually in January in the 8th year from the departure of the staff.

The first batch of deletion to be conducted will be March 2020. The annual deletion process will be carried out in January every year.

Any request for changes in the disposal schedule should follow the procedure specified in Section 8 below.

In order to maintain the integrity of Banner ERP System data, the data fields of staff ID and name will be kept even all other data fields have been deleted.

**6.2 Suspension of Disposal**

Data disposal action should be suspended in case the data is involved in any governmental investigation, audit concern, litigation or for any solid reasons raised by Chief DPO, data owner, data user or senior management of the University. The suspension request should be submitted in an official written format with reasons and evidence provided to the system administrator with copies to the data owner and Chief DPO of the University. The suspension of disposal action should be maintained until the advice of the requester determines otherwise.

**6.3 Disposal Action**

Once a record or data has reached its designated retention period, the designated administrator in ITSC should execute the disposal action that is defined in the disposal schedule. The system administrator need to send a notification to the data owner before and after the disposal action to alert the changes in the data.

The disposal of data should be non-reversible. Besides deletion of data in databases or systems, those traces in any systems log, archives and backup should be cleared as far as possible.

Data removal from backup media or archives can be deferred for a maximum of 1 year from the retention period if there are any technical constraints. Backup media and archives in such case need to be stored or locked in a secure place, an access log should be maintained to keep track of any access of the backup media or archives. Restoration of such data should be restricted with written approval from both data owners and Chief DPO. The destruction of the backup media or archive should also be recorded with date, handler and the method of destruction.

1. **Data Disposal Log**

A “Data Disposal Log” should be maintained for audit purpose. The log should document which set of data has been deleted or destroyed, when, by whom and by what method. Care should be taken to ensure that the log record itself does not contain any personal identifiers.

1. **Exceptions**

Data may be retained for a longer period to fulfil contractual or legal obligations or for other reasons. Any request for exceptions to this policy should be submitted in writing to CIO and Chief DPO of the University for review and endorsement. ITSC and Chief DPO will assess the impact, security and risk measure of the request before submitting recommendation to the Personal Data Privacy Committee for approval.

Exception requests must include the following information:

* Reasons for non-compliance
* Proposed alternative protection methodology
* Reasons for using a different approach
* Risk and impact assessment with the proposed methodology