The Chinese University of Hong Kong, Shenzhen

Policy on Protection of Personal Data (Privacy)

1. General

1) The University is committed to safeguarding the privacy of its students, alumni, faculty, and staff, as well as protecting the confidentiality, integrity, and availability of personal data that are important to the University's mission.
2) All Unit heads of the University are requested to critically review and improve the procedures and other relevant internal arrangements that are within their purview, in accordance with the following policy published by the University.

2. Scope of Policy

1) This policy covers the personal data, not only limited to the Computer and Digital Data Resources (its definition is as at Appendix 1), but also the data in any other forms relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual.
2) This policy applies to the individuals that control the collection, holding, processing or use of personal data at the University. The resources of personal data include, but not limited to students, alumni, faculty and staff, those working on behalf of the University, guests, tenants, contractors, consultants, visitors and/or individuals authorized by affiliated institutions and organizations.
3) Personal data created or transmitted in the University's business processes includes, but not limited to, National ID, University ID, location data, online identifier, and factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity; application data such as for admissions, activities, scholarship and financial aid; academic data such as grades, scores, records of attendance and observations; data from journals, research publications or other platforms through which employees or students publish academic content; employment data such as employment history, education, professional certifications, health, personal profile, and those of family members.

3. Purpose of Data Collection

1) Personal data created or transmitted in the University's business processes is owned by the University, and, as such, all members of the University community and affiliates are responsible for appropriately using and safeguarding that data.
2) Personal data the University collects is to
   - administer and manage University programmes, services and facilities,
   - make strategic decisions,
   - file required reports with applicable governmental authorities,
   - enforce policies and applicable laws.

4. Data Protection

1) The individuals that use the personal data are responsible for safeguarding their access privileges, for the use of the personal data in conformity with all applicable University policies, and for securing such data.
2) The individuals should take all practicable security steps to ensure that personal data is protected against unauthorized or accidental access, processing or erasure having particular regard to the kind of data and the harm that could result if any of those things should occur.
3) Personal data should be safeguarded to maintain the confidentiality and privacy of personally identified and personally identifiable information. Access to University's personal data should be based on the business needs of the units and should enhance the ability of the University to achieve its mission. The individuals shall have access to the data needed to perform their responsibilities. Individually identifiable data shall be available to the extent necessary to perform administrative duties.
4) To protect Computer and Digital Data Resources, unit heads should make sure that an effective mechanism is in place within their respective Department/School/Unit to determine whether it is really necessary to use mobile computing devices (e.g. notebook computers and PDAs) and portable storage devices (e.g. external hard drives, memory cards, USB storage devices, memory sticks and thumb drives) to handle identifiable personal and sensitive data, and to make sure that such devices are securely kept and the data carried therein are properly encrypted and/or password protected. When required, unit heads should consult with Information Technology Services Office (ITSO) for further advice.
5) To avoid the loss or unauthorized use or disclosure of personal and sensitive data, it is recommended that a Non-Disclosure Agreement (as at Appendix 2) be signed in all situations with contractors when acquiring third-party service that may need to access personal and sensitive data in the University.
6) Engaging cloud storage providers is considered as one form of outsourcing arrangements. The individuals are ultimately responsible for the protection of the personal data collected and held by them. The outsourcing of any processing or storage of personal data to the third-parties does not relieve the individuals' responsibility for the protection of the personal data they collect and hold. The individuals should be aware of the risk that the cloud storage provider is able to unilaterally change conditions in the agreement it has with its customers to a lower protection standard or limit its liability.
7) While using cloud storage service, the individuals should ensure they have the obligations that enable them to access their personal data, request corrections, and resolve issues and complaints. Accordingly, the individuals must ensure that their

contract with the cloud storage provider allows them to meet these obligations. Furthermore, the individuals should ensure there are the following obligations imposed in their contract with cloud storage providers:

- Limit the use of personal data,
- Set out how personal data is to be erased or returned to the individuals upon requests, contract completion or contract termination,
- Take security commitment to the data protection,
- Maintain business continuity,
- Handle data breaches.

8) If required, the individuals should consider implementing an end-to-end, comprehensive and properly managed encryption system for the transmission and storage of personal data. If the individuals are not able to have direct oversight over all the obligations necessary for the protection of personal data, they should consult with ITSO for further advice.

5. Data Sharing

1) Personal data may be shared among University employees according to well-defined business processes approved by the University. It may be released publicly only according to well-defined business processes, and with the permission of the unit heads.
2) Sharing data between academic and/or administrative units within the University should be facilitated where appropriate, subject to appropriate security restrictions as established by the University.
3) Integration of data across the University should be encouraged to foster data accuracy and uniformity, consistent with the University's institutional complexity, various data systems, and differing data formats. This should result in reduced duplication of data and greater data accuracy.

6. Data Retention

1) The University preserves the personal data of all resigned staff, leavers, and graduates. The University stores their personal data in accordance with the Lifecycle of Data Retention as at Appendix 3.

7. Data Disposal

1) The University retains the ownership of personal data created and transmitted in the University business processes. The University units keep the right to dispose personal data in line with the data retention schedule in Appendix 3. While performing data disposal, unit heads should ensure there are no relevant proceeding in progress concerning with individuals identified in the data, for instance, internal disciplinary action, contract disputes or court actions.

2) Resigned staff's, leavers' and graduates' portable storage devices can only keep their individual information, such as resume, salary forms, payroll slips, performance appraisal, reference letter and transcripts. Unit heads should ensure the sensitive data concerning with administrative, academic, and research records of the University is properly disposed from the portal storage devices owned by resigned staff, leavers, and graduates. To dispose the data stored in the portable storage devices, unit heads should ensure the data are deleted completely. When required, unit heads should consult with ITSO for further advice of data wiping operated on the portable storage devices.
3) ITSO is responsible for the data disposal residing at the University network storage. Aligning with the data retention schedule, ITSO will perform routine maintenance on personal data linking with these items as listed in the Lifecycle of Data Retention. ITSO will no longer keep or do backup of personal digital data which is out of its retention period.
4) To dispose of the data stored on paper, the University units should use paper shredder or other paper disposal devices. When necessary, a massive shredding work should be contracted to a professional disposal operator upon a written agreement to dispose of the materials to the necessary standard.
5) To dispose of the data stored in the tapes, on the films, and in other non-electronic forms, the University units should consult with the professional data disposal contractor for further advice to ensure the operation of data disposal is complete and safe.
6) The data disposal procedure does not apply to the data archiving operation necessarily performed by the University or its administrative units, such as the President's Office, nor does its retention schedule apply to any data in any forms that need to be archived in light of business needs. The University and its administrative units maintain separate data archiving mechanism to preserve data for future reference and historic needs.

8. Rights of Employees and Students

1) Employees and students have the following rights with respect to personal data.

- The right to request access to personal data, such as salary forms or payroll slips, performance appraisal, reference letter, transcripts or other individual academic record that the University has, as well as the right to request rectification of any personal data that is inaccurate or incomplete, provided that such requests shall be practically in connection with his or her own profile.
- The right to request a copy of personal data, such as salary forms or payroll slips, performance appraisal, reference letter, transcripts or other individual academic record, in electronic format so that employees and students can transmit the data to third parties, or to request that the University directly transfer personal data to one or more third parties. Such requests should be specific and practically in connection with his or her profile.

- The right to object to the processing of personal data for marketing or other commercial purposes.

9. Provision of Sanction

1) All the misconducts that violate this policy will be reported to the Personal Data Controlling Committee, whose members shall review and propose sanction advice in light of the relevant regulations of the University.

10. Right of Interpretation

1) The University reserves the right of interpretation for all terms as stated in this policy. All terms, including the Appendixes, are subject to further revision from time to time conducted by the Personal Data Controlling Committee.

Oct, 2019

Appendix 1: Definition of Computer and Digital Data Resources

Computer and digital data resources are defined for the purpose of this policy as follows:

- Desktop, laptop, or server computers running general purpose operating systems such as Windows, Mac OS, Unix/Linux, and mobile applications.
- Network server applications, such as an SFTP-server application.
- Applications and web applications, such as Student Information System, Human Resources System, Finance system, Learning Management System, websites, and other administrative systems for Students Affairs, Schools, Colleges and Research operation.
- Databases, Data Warehouse, APIs, and other data exchange systems.
- Mobile devices, such as tablets and smartphones where data can be stored.
- Authentication and authorization systems such as Single Sign-On, Active Directory, and LDAP, etc.
- Other computing devices, systems, and applications if the above items don't include.

Appendix 2: Non-Disclosure Agreement

Information Security and Confidentiality Agreement

Party A: The Chinese University of Hong Kong, Shenzhen

Address: No. 2001, Longxiang Blvd., Longgang District, Shenzhen

Party B:

Address:

Whereas:

1. The Parties hereto are currently working on XX project.
2. This Agreement is made for protecting sensitive data (hereinafter referred to as "confidential information") already or to be provided or disclosed by Party A to Party B for the purpose of project cooperation. Party B is the information technology service provider, as such it may come into contact with and obtain Party A's confidential information when providing technical services to Party A.
3. The Parties hereto agree that, except for use of confidential information in ways otherwise agreed in writing by and between both Parties, they shall use confidential information in ways specified herein and assume the obligation of confidentiality.

In order to ensure the successful performance of the XX project contract (hereinafter referred to as the "original contract") entered into by and between both Parties, the Parties hereto agrees as follows.

I. Confidential Information

1. Confidential information includes but is not limited to the following: XXXX
2. The above-mentioned confidential information may take the form of data, texts that are contained in tangible media such as documents, CDs, software, books, etc., and transmitted by oral and other audiovisual methods.

II. Rights and Obligations of the Parties

1. As the provider of information technology service, Party B shall not disclose Party A's confidential information to any third party during the provision of service to Party A and shall endeavor to prevent inadvertent disclosure of such confidential information to any third party.
2. Without the written consent of Party A, Party B shall not use Party A's confidential information or distribute such information within its own organization, except for any information required for negotiation and discussion with Party A's personnel or for assistance provided to Party A or for any other purposes approved by written authorization of Party A after the execution hereof. Party B shall be held liable for any breach of confidentiality by its own personnel who may come into contact with Party A's confidential information.
3. Party B shall not use any confidential information related to Party A for its own interests or for the benefit of any other party other than those specified in this Agreement.
4. Party B's confidentiality obligation doesn't apply to information : (a) that is already in the public domain upon Party A's disclosure thereof; (b) that enters the public domain due to reasons other than Party B's fault after Party A's disclosure thereof; (c) that is already disclosed to Party B without attaching any confidentiality obligation upon Party A's disclosure thereof; (d) as proven by written proof, any information that is independently developed by Party B without using any confidential information of Party A; (e) Any information that is required to be disclosed according to a court order or government order.
5. This Confidentiality Agreement, the disclosure of confidential information and negotiations between the Parties thereafter do not give rise to any obligations other than those specified herein. The execution of this Agreement or the disclosure of confidential information to Party B thereafter shall not be deemed to confer to Party B any intellectual property rights or any other right of any kind to said information.

6. All confidential information is provided on an "as is" basis and neither Party gives any warranty (express, implied or otherwise) as to its accuracy, completeness or performance.
7. All materials provided by Party A to Party B and Party A's confidential information obtained by Party B when providing information technology services to Party A, including but not limited to documents, data, designs and lists, shall remain the property owned by Party A. Upon written notice from Party A, Party B shall promptly return said materials and information (the original copy thereof and other copies made thereon) and delete any relevant information stored on Party B's computer, server or other storage media.
8. Party B's confidentiality obligations shall survive the expiration of the technical service period agreed by both Parties, and Party A has the right to hold Party B liable for any breach of such confidentiality obligations in accordance with the *Contract Law* and the *Tort Liability Law of the People's Republic of China*.

III. Liability for Breach of Contract

1. Where Party B or its personnel (including those who have left the company after coming into contact with Party A's confidential information) have violated the confidentiality obligations stipulated herein, Party B shall stop such violation immediately and bear the liability for compensation of any loss caused by such violation to Party A; if Party B fails to rectify the violation in time, it shall be held liable for compensation of any further loss arising therefrom;
2. Where Party B violates this Confidentiality Agreement, Party A may unilaterally terminate this Agreement, and Party B shall pay liquidated damages (in the amount of 30% of the actual loss arising therefrom, said loss shall be assessed and determined by Party A or a third-party appraisal agency (the expenses shall be borne by Party B) engaged by Party A and the liquidated damages shall be paid within 30 days after the issuance of the appraisal report) and compensate Party A for any loss arising therefrom.

IV. The Governing Law and Dispute Resolution

1. This Agreement is governed by *the Laws of the People's Republic of China*.
2. All disputes arising out of or in connection with this Agreement shall be resolved through friendly negotiation between both Parties. If the friendly negotiation fails, either Party may submit the dispute to the Shenzhen International Court of Arbitration (Shenzhen Arbitration Commission) for arbitration to be conducted in Shenzhen in accordance with then effective and applicable arbitration rules of the Commission.
3. During the course of the arbitration, both Parties shall continue to perform parts of this Agreement that are not related thereto.

V. Entry into Force and Miscellaneous

1. This Agreement and any amendments, attachments, changes or additions hereof shall take effect upon execution by the Company and the acceptance and signature of the authorized representatives of both Parties.
2. This Agreement is made in duplicate, with each Party holding one copy and both copies having the same legal effect.
3. This Agreement shall enter into force on the date of signature and seal of both Parties, and shall remain effective until _____ (generally the expiration date of the Contract, but could be dates otherwise agreed upon for major projects).

Party A:	Party B:
Seal:	Seal:
Authorized representative:	Authorized representative:
Date:	Date:

信息安全保密协议

甲方：香港中文大学（深圳）

地址：深圳市龙岗区龙翔大道 2001 号

乙方：

地址：

鉴于：

1. 甲乙双方正在进行 XX 项目。
2. 本协议旨在保护因项目合作，甲方已经或将要向乙方提供或披露的敏感数据（以下统称“保密信息”）。乙方作为甲方的信息技术服务提供商，在提供技术服务过程中会接触和获得甲方的保密信息。
3. 双方协商依照本协议使用保密信息，承担保密义务，除非双方书面签署文件同意以其他方式使用保密信息。

为保证甲乙双方订立的 XX 合同（以下简称“原合同”）能够顺利履行，经双方协商，达成本协议。

一、保密信息

1. 保密信息包括但不限于以下内容： XXXX ；
2. 上述保密信息可以以数据、文字及记载上述内容的文档、光盘、软件、图书等有形介质体现，也可通过口头等视听方式传递。

二、双方权利义务

1. 乙方作为甲方的信息技术服务供应商，在为甲方提供服务时，乙方不得将甲方的保密信息透露给任何第三方，而且应尽力避免由于疏忽将甲方的保密信息披露给任何第三方。
2. 未经甲方书面同意，乙方不得使用甲方的保密信息，也不应在自己的组织内部流通，但乙方与甲方人员商谈、讨论和协助之需或在本协议签署后经

甲方书面授权的使用除外。乙方应为自己组织内有可能接触甲方保密信息的人员的泄密行为后果承担责任。

3. 乙方不应为除本协议规定的目的之外的自身利益或任何其他方的利益而使用任何关于甲方的保密信息。
4. 乙方对以下方面的信息没有义务：（a）在甲方向乙方告知信息时，该信息已处于公众领域中；（b）在甲方向乙方告知信息后，该信息非因乙方过错而进入公众领域；（c）在甲方向乙方告知信息时，该信息系乙方拥有且无任何保密义务的信息；（d）根据书面而记录证明，该信息系乙方独立开发，没有借助于甲方任何保密信息；（e）该信息被法院或政府命令要求披露。
5. 本保密协议，保密信息的披露和双方之间其后的商议并不产生除本协议规定之外的义务。本协议或向乙方披露的保密信息均不得视为向乙方授予任何知识产权或与之有关的任何性质的权利。
6. 所有保密信息是基于“可能是”而提供，任何一方都不通过明示、暗示或其他方式对其准确性、完整性或性能做出保证。
7. 所有由甲方提供给乙方的材料和乙方在为甲方提供信息技术服务过程中获得的甲方的保密信息，包括但不限于文件、数据、设计和清单，保密信息应仍为甲方的财产。经甲方书面通知后，乙方应立即归还原件和据此制作的副本，并删除存储于乙方电脑、服务器或其他存储介质的有关信息。
8. 乙方承担的保密义务不随乙方为甲方提供技术服务期限的届满而终止，且乙方如有违反保密义务之处，甲方有权依据中华人民共和国《合同法》、《侵权责任法》等法律追究乙方责任。

三、违约责任

1. 乙方或乙方人员（包括获知甲方保密信息的乙方已经离职人员）违反本约定规定的保密义务，应立即停止侵害，乙方应承担对甲方由此造成损失的赔偿责任；如因乙方未及时处理，而造成损失扩大的，乙方应承担赔偿责任；
2. 乙方违反保密协议的约定，甲方可以单方解除本协议，乙方应支付违约金（甲方评估实际损失的金额或者找第三方鉴定机构鉴定（鉴定费用乙方承

担），违约金为损失金额的30%），于鉴定报告后30天内支付，并赔偿甲方因此而遭受的损失。

四、法律适用和争议解决

1. 本协议适用中华人民共和国法律。
2. 所有因本协议引起的或与本协议有关的任何争议将通过双方友好协商。双方不能通过友好协商解决争议，则双方均可提交深圳国际仲裁院（深圳仲裁委员会）依照该会现行有效的仲裁规则适用简易程序在深圳仲裁。
3. 仲裁进行过程中，双方将继续履行本协议未涉及仲裁的其他部分。

五、协议生效及其他

1. 本协议及其任何修改、附件、变更或补充经公司签署并经双方授权的代表接受和签署方才生效。
2. 本协议一式两份，甲乙双方各执一份，两份协议具有同等法律效力。
3. 本协议自甲乙双方签字、盖章之日起生效，有效期至（一般为合同有效期限，如重大项目再另行约定）。

甲方：	乙方：
盖章：	盖章：
授权代表：	授权代表：
日期：	日期：

Appendix 3: Lifecycle of Data Retention

Category	Description	Retention Period
Academic Affairs and Student Records	Official Transcripts, Degree, Grades, and Enrollment Statistics	Permanent
	Course Offerings, Class Lists, Schedule of Classes	Permanent
	Scholarship Records	Permanent
	Student Admissions Records	Permanent
	Students' Profile and Identifiable Information	Permanent
	Alumni and Alumni Associations Records	Permanent
	Student Activity Records	Permanent
	Blackboard Discussion Board, Course Materials, Assignments, Exams, Grades and Evaluations	Permanent
	Students' Employment Information	Permanent
	Teaching and Learning Videos	Permanent
Finance Records	Annual Payment Records	15 Years
	Record of Payments and Deductions (payroll registers, deductions lists, adjustments)	15 Years
	Students' Financial Information	15 Years
	Expense Claims	15 Years
	Fixed Asset System Data	15 Years
Human Resources Records	Employee Personnel Files (including application, resume, appointment/salary forms, benefits enrollment and application forms, beneficiary designations)	15 Years
	Employee Benefits Plan Files (Applications and Correspondence) and Benefits Handbook	15 Years
	Performance Appraisals	3 years after resignation
	Payroll Deduction Authorizations, Pay Slips	15 Years
	Employees Benefits Records	15 Years

	Attendance, and Leave Records	3 years after resignation
Records of Information Technology Services	Records of Borrow and Return of IT Equipment	Permanent
	ITSM System Data	Permanent
	Network Authentication Records	6 months
	Internet Records	6 months
	Email Records	1 year after resignation
Records of Research Administration	Personnel Files	Permanent
	Research Project initiation Documents	Permanent
	Research Project Budget and Expenditure	Permanent
	Research paper, Thesis and Publications	Permanent
Records of Security and Safety	Data of Surveillance System	3 months
	Access Control Records	3 months
	Data of Campus ID Card Services	1 year