

Operational Outline to Establish and Use the Database of Institutional Research of Asia University, Taiwan

July 20, 2016 Issued through the 12th administrative council in Academic Year 2015

1. To promote the value-added application of institutional information, strengthen the function of statistics, support and decision-making and enhance the academic research energy, the Center of Institutional Research & Development (hereinafter referred to as “the center”) of Asia University (hereinafter referred to as “the university”), Taiwan shall make the data to the public and stipulate criteria for the use and release of data. The “Operational Outline to Establish and Use the Database of Institutional Research of Asia University, Taiwan” (hereinafter referred to as “the outline”) is set referring to *Openness of Government Information Act* and *Personal Information Protection Act*.
2. Related personnel in the university who use the institutional research data and data released to the public shall handle it by the regulations of the outline and based on related laws and regulations including *The Freedom of Government Information Law* and *Personal Information Protection Act*.
3. The content in the outline includes establishment standards for database of institutional research, definitions of related terms in institutional research, the qualification to apply for using the institutional research data, procedure to apply for using the institutional research data, procedures of institutional research data review, spread and application of institutional research, etc.

The establishment and management of database shall be handled by the Office of Information and Communication Technology (OICT) in the university based on related regulations about information security. For the use of data, issuance of analysis and subsequent execution for tracing results, the center shall take charge of it.

4. Establishment criteria of institutional research data:

- (1) Data collection and encryption:

For the data files collected by the university, sensitive data shall be encrypted and processed necessary review first.

- (2) Data examination:

Examine collected data and the examination scope includes: sum of data, year, definition, logics, property and column form.

1. The lengths, properties and codes of the same data columns in different database shall be the consistent.
2. Every examination result shall be recorded in “Index in Database of Institutional Research of Asia University”(IR Index).

(3) Data storage and verification:

When the data files with encryption are collected to the data storage, the data files and decoding tables in different classifications shall be established respectively, as required. After that, the data verification shall be processed and recorded. If it's necessary, notes for mending or explaining shall be added and recorded in “Index in Database of Institutional Research of Asia University” (IR Index).

1. Data files in different classifications shall be stored respectively without encrypting comparison.
2. Select a number of common columns to build data sub-files, as use frequency and needed.

(4) Provide to download data:

The applicants apply it by the database usage procedures in the university. After approval, the Office of Information and Communication Technology (OICT) shall provide for the applicants to use after articulating and connecting the data. Only after OICT receives the confirmation notice can the data be edited, downloaded and processed. Basically, one application shall be provided within 2-10 days, but the specific handling time interval in terms of special case or other situation cannot be reasonably anticipated shall be further noticed based on actual situation.

5. Definitions of related terms in institutional research data:

- (1) Personal data: The name, date of birth, student number, ID number, family background, educational background, job, health examination and other data which can directly or indirectly identify the individual of teachers, students and staff in the university.
- (2) Data encrypting: The personal identification code of personal data file is encrypted after reorganization and the data after encrypting shall be obscured again or a number of columns shall be added or deleted.

- (3) Comparison of added values of data: Combine more than two kinds of databases file, taking the same columns as key values.
 - (4) Database of Institutional Research: The database integrating all data of units in the university provided by the OICT is established to operate the data by standard procedures.
 - (5) Procedures to establish: The procedures to collect, encrypt, examine, storage, verify, compare, deliver out and support the data by institutional integrated database.
 - (6) Procedures to use: The application for using data shall be approved by certain procedures and providing of documents. In addition, through the review and approval of the OICT and IR of the university, the identification procedure can be exempted.
 - (7) Results of statistics analysis: The statistics results after organization and computation excluding personal data for users to analyze.
 - (8) Data grading: Personal data is graded based on the error detection program, encrypt or not, sensitivity and so on.
6. Qualification to apply for using the institutional research data as following:
- (1) All directors and colleagues of administrative units and departments in the university.
 - (2) Teachers, students and staff who are interested in institutional research in the university.
 - (3) Cross-school cooperating personnel or personnel not belongs to the university who would like to process the institutional research project shall be signed and checked additionally.

Above applicants shall provide supporting documents to prove that applicants have been experienced the IR-IRB related educational trainings more than 4 hours. If the applicant does not provide the documents when applying but make it up after the application is passed, the OICT shall offer required data for application.

7. Procedures to apply for using the institutional research data:
- (1) Make an application (as annexed Table 1) to IR-IRB and get approval.
 - (2) Fill the online Application Form for Using Data of OICT.
8. Procedures of institutional research data review:

The applicants apply to the OICT by application procedures and the results will be noticed after the applications are inspected.

9. Spread and application of institutional research:
 - (1) Applicants who apply for institutional research data to analyze shall submit and transfer the analysis reports to the center to archive and examine, in order to provide references and applications for service executions of all units and other institutional developments.
 - (2) Applicants who apply for institutional research data to do research paper and publish to the public shall not use the data related to institutional sensitive issues (as annexed Table 2). It can be implemented after the applicants sign the petitions with approval.
10. The applicants shall apply for and use the institutional research data based on the regulations of the outline.
11. The data files as required by the applicants provided by the center shall confirm to the purpose to collect, except one of following situations:
 - (1) For improving public interests.
 - (2) For necessary academic research without harming to the vital interests of the interested parties.
12. Related regulations about service data provided by the center as following:
 - (1) For data requested to be provided, if it is necessary to get the consent of data supplier in advance, the center or OICT shall request the applicant to get consent first and then apply by the application procedures.
 - (2) For data requested to be provided, the applicant shall file the application to the OICT online and specify all data needed.
13. The personnel in the center and the users and applicants for institutional data shall sign the confidentiality affidavit (as annexed Table 2) and keep the secret. In addition, they shall submit the result reports and return the data file back at the same time. The offenders shall be handled by related decrees.
14. The unaccomplished matters in the outline shall be handled by related decrees and regulations. The outline shall be implemented or revised with the approval of executive council and the authorization of the President.

Annexed Table 1 Application Form for Research Project of IR-IRB, Asia University, Taiwan

All applicants who apply for the institutional research data in the university to research shall fill the form and submit it to the committee to check. Only it is approved can the research be operated. If the applicant would like to cooperate with other organizations, it shall be agreed by the committee and related committee of cooperative organization.

1. Name of applicant: College: Department:
2. Collaborative presenter: College: Department:
3. Research topic
4. Research purpose
5. Research subject
6. Data for research
7. Methods for research design and process
8. Research duration and schedule
9. Supporting documents to prove that applicant has been experienced the IR-IRB related educational trainings more than 4 hours
The supporting documents have been submitted when application
The supporting documents have not been submitted when application and the applicant will hand in the required analysis data after submitting
10. Confidentiality affidavit for applicant
11. Contact of the project: Telephone: e-mail:

Through my confirmation, all data listed in the application project are true. I shall operate it by the criteria made by IR-IRB in the university. If not, I volunteer to undertake any responsibility.

Signature of applicant: Date:

Director of application unit:

Department head:

;Dean:

Date:

Annexed Table 2 Data grading and public usage principles of IR Database in Asia University, Taiwan

The data is graded in following four classes based on the principles of error detection program, encrypt or not and sensitivity; Data of first grade to third grade involve institutional sensitive issues and cannot be used in paper research and published to the public.

1. First-grade data:

Complete data which can identify the individual original plain code, including student number, ID number and related sensitive data(such as the natural person's name, telephone, address and so on. Hereafter referred to as sensitive data).

2. Second-grade data:

Data which may identify the individual or specific organization, encrypting the identification code of first-grade data and eliminating the sensitive data which can identify the individual.

3. Third-grade data:

Data which takes part columns of second-grade data to obscure distinguishable data and take secondary encryption for different purposes.

4. Fourth-grade data:

Data used publicly.

