Data Access Guidelines
for Business Intelligence (BI) System

Revision History

Version	Prepared By	Approved By	Date	Revision
1.0	ITSC	TLIS / UAPC	May 2016 / July 2016	Initial version
2.0	ITSC	ISMB	March 2023	Revised the text in various sections, examples quoted and the Roles and Privileges Matrix for Business Intelligence System in Appendix I as highlighted

Guidelines

Institutional data covering all data and records held in any format or medium by any University department are key information assets owned by the University that supports the central mission of the University. In order to support effective decision-making and enable the University to align resources and projects with strategic priorities, institutional data must be represented accurately in the corresponding data formats. It must be easily integrated across the University's centralized systems, as well as be accessible by all legitimate university members.

The use of institutional data shall be:

- Used solely for legitimate university purposes.
- Granted to all eligible university employees for legitimate university purposes.
- Accessible to centralised systems for legitimate university purposes. Any systems containing institutional data must maintain at least the same level of security protection and data integrity as the data source.
- Observing ethical restrictions and abiding applicable laws and policies with respect to access, use or disclosure of information.

Access and control of institutional data containing personal data must comply with the Personal Data (Privacy) Ordinance of HKSAR, the University's "Code of Practice for Handling Personal Data" and the "Information Security Policy".

Categories of Institutional Data

I. Aggregated Institutional Data

Aggregated institutional data will generally be available and accessible to all eligible full-time staff members. Examples include:

- Number of students and graduates
- Number of research outputs, publications and journals
- UGC funding amount and departmental expenditures

- Other summary data that does not identify a specific individual and do not allow any specific individuals or their data to be identified.

II. Disaggregated Institutional Data
Disaggregated institutional data are restricted to individuals with a legitimate reason in accessing the data to perform the functions of one's job or for handling University's approved projects. Examples include:

- Data maintained by the University that identifies specific person.
- Personally identifiable information that is unique or traceable to a specific person will not be displayed. These data are protected by law, and includes ID or Passport numbers, contact information and medical records.
- Aggregated data for very small populations that might indirectly allow an individual to be identified.

Access to Institutional Data

1. Eligible university staff members are allowed access to aggregate institutional data in support of university business.
2. All individuals with access to institutional data must comply with all applicable university rules, policies, procedures and standards as well as all applicable laws, regulations and ordinances.
3. The roles and privileges matrix for BI listed in Appendix I describes how default access to data is administered.
4. The roles and privileges matrix for BI listed in Appendix I is subject to change in the future corresponding with the addition or deletion of any source information.
5. Exceptional access to authorised institutional data can be granted subject to the approval of corresponding data owners such as Deans, Department Heads or senior university administrators based on a proper user request with valid justification.

Institutional Data and Systems Integration

Institutional data are permitted to be exported or integrated among the University's centralized computer systems, which support the administration, operation or governance of the University.

Systems, databases, applications, etc. that access confidential and sensitive data must be maintained with security protection at least the same as the data source. The integrity and quality of the data must be accurately maintained across systems. Information security demands that only necessary data sufficient to provide accurate data analysis should be kept and maintained in the Business Intelligence System.

Reference:

Lingnan University. (2022, December 5). *Information Security Policy*. https://www.ln.edu.hk/secure/f/upload/50187/InformationSecurityPolicy.pdf

Appendix I

The Roles and Privileges Matrix for Business Intelligence (BI) System

Group	Members	Scope of Institutional Data using in Analytics			
		University-wide (e.g. CDCF, University Accountability Agreement, QS Ranking Statistics, etc)	Cross-departmental (Academic-related) (e.g. Data Repository System)	Cross-departmental (Non-Academic-related)	Specific Department's Interest (e.g. BI Reports for OGE)
Senior Management	President, Vice President, Associate Vice-Presidents	✓	✓	✓	✘
Deans	Faculty Deans, Dean of Graduate Studies	✘	✓	✘	✘
Academic Heads	Heads of Academic Units, Programme Directors	✘	✓	✘	✘
Administrative and Services Heads	Heads of Administrative and Service Units	✘	✘	✓	✘
Authorized Staff^	Authorized staff including both Administrative and Academic Units	✓	✓	✓	✓

Notes:

^Authorized Staff refers to any staff member of both administrative and academic units authorized by Heads, Deans or University management to access relevant data in the BI system.