Sabaragamuwa University of Sri Lanka

Policy Title – Data Management Policy -SUSL

Policy Number – Policy / SUSL / Gov & Mgmt / 23

Effective Date – 27.11.2023

Revised Dates – NA

Approving Authority – The Council, Sabaragamuwa University of Sri Lanka

Administrative Responsibility – Council

Overview

The University operates in an environment that is increasingly complex and data-driven. It is the responsibility of the University to ensure the availability, confidentiality, and integrity of all information entrusted to it. The data generated and held by the University, whether stored on personal devices, managed by a third party or business partner, or outsourced to a service provider, are a valuable asset that must be managed, governed, protected, and appropriately safeguarded to support the strategic development, essential functions, and academic integrity of the University.

Purpose

Inappropriate use of the university's data may damage the institution, its faculty, staff, students, and alumni. This damage could have an effect on the university's mission of education, research, and service. It poses criminal, financial, and reputational hazards to the university. Members of the university community are responsible for the proper use, maintenance, and protection of university data.

This policy will provide a framework to safeguard and secure the university's data while allowing for flexibility to support a vast array of academic, research, and administrative endeavors.

Scope

All the students (internal, external and postgraduates students), employees, alumni, service providers, contractors, authorized visitors, and persons or organizations acting on behalf of or for the university.

Definitions

- **University data** – Data that is created, collated, and stored (either electronically or in physical copy) in support of academic, research, and administrative activities by units and members of the university community. University data may include (but are not limited to) the following:
    - **Institutional data** – Data generated, collated, and stored by all university entities and members in support of academic and administrative activities. Institutional data includes administrative information about teaching, learning, research, and scholarly activity, such as grades, attendance, research grants held, and publications produced.
    - **Research data** - Data generated or derived from research, academic, or artistic endeavors.
    - **Personal data** – Data containing personally identifiable information about an individual. If these data were compromised or used improperly, the privacy of an individual would be compromised.
    - **Third-party data** - Data created or owned by a third party and used to support academic, research, and administrative endeavors. If these data were compromised or used improperly, the third party would be affected. This includes data such as licensed software or software components, as well as content protected by intellectual property laws.
- **Derived data** – Data that has been modified from the original data using a mathematical formula, composition, or aggregation.
- **Data Access**
    - **Internal Data**: Internal data can be accessed by all internal staff without restriction

- **Confidential and Highly Confidential**: Data will be categorized as Confidential or Highly Confidential by the DMC and can be accessed by only authorized staff members.
- **Public**: Data will be categorized as Confidential or Highly Confidential by the DMC and can be made freely available without restriction.

- **Data managemen**t – Includes activities associated with the creation, collection, storage, maintenance, cataloging, use, distribution, and disposition of university data.
- **University community** - All students, employees, faculty, postdoctoral fellows, alumni, agents, contractors, authorized visitors, and persons or organizations acting on behalf of or for the university.
- **University-owned assets** – Assets acquired with university funds, including research grants administered by the university, or through a contractual agreement.
- **IT services** - Technology-based services managed or hosted by a member of the university community, the university, or third-party vendors/contractors.
- **IT infrastructure** – IT assets such as servers, databases, data, software, end-point devices, the university network, Internet connections, central authentication, the telephone system, and data centers, whether provided directly by Information and Communications Technology or contracted.
- **IT outsourcing** - entails the utilization of external service providers to deliver IT-enabled business process, application service, and infrastructure solutions. Outsourcing can include utility services, software as a service, and cloud-enabled outsourcing, among others.
- **University** - Sabaragamuwa University of Sri Lanka

Policy statements

1. This policy focuses on the activities related to all sorts of data management of the University.
2. University data are the property of the University and are regarded as corporate assets.
3. University can gather relevant data from different sources depending on the requirements in accordance with its vision and mission.
4. Data being collected and processed should be treated as confidential and it must be accurate, up to date, safeguard and protected.
5. Responsibility of maintaining data integrity is with the Data Management Committee (DMC)

6. Data shall be handled by the data management committee /DMC appointed by the council.
7. This committee shall be chaired by the Vice Chancellor of the University.
8. This committee shall work according to the policies, laws, acts and any other necessary legal framework of the University and the Government of the Democratic Socialist Republic of Sri Lanka.
9. When collecting data, wherever necessary, the data provider shall give the consent to the DMC. This can be done by using a written document or it can be given as email or any digital form.
10. Access to data will be granted to Data Users for all legitimate University purposes, subject to any limited access restrictions that may be determined from time-to-time by DMC. While maintaining the confidentiality of any kind of data DMC must take necessary measures to avoid unauthorized or unlawful processing of data, destruction of data, and loss of data.
11. DMC members should use only the official mails for communicating with relevant parties but not with their personnel mails.
12. University shall have a data management plan /Data Management Standards which is approved by the council.
13. Data management plan of the university should be incorporated into the University strategic management plan and action plan.
14. Any data should be collected only for specific purposes and they should not be used for other purposes which were not stated. With the consent of the data owner data can be used for other purposes which was not stated at the beginning of the data collection.
15. Types of data: Personnel data; This policy will enable protection of personal data of students and employees of SUSL, in line with “Personal Data Protection Act no: 09 of 2022.
16. Research data; responsibility of managing research data during any research project is with the Principal Investigators (PIs) or individual researchers (academic staff, undergraduates and postgraduate research students).
17. Data must be stored in an official University data repository or place determined by DMC
18. Data must be available to all Data Users with legitimate University operations need through an easily accessible platform
19. Data should be defined consistently across the University, and names, formats and codes must be consistent across all the units that use the data and consistent with any agreed University standards
20. Data collection, generation, and processing should, wherever possible, be automated.
21. Data updating processes should be standard across the University

22. Data can be managed appropriately under strict change control and need to be recorded in an auditable and readable under any agreed change control processes
23. Data should not be duplicated. If duplication is essential, then the data owner can approve. However, a robust process must ensure copies are not modified.
24. Whenever possible, international or national standards for data models must be adopted

25. Data Owners;

- Data Ownership will be given to the Vice Chancellor, Deans, head of the departments, directors, registrar, librarian, DR, SAB, Bursar, head of divisions Unit or other Officer with primary responsibility for the University operations to which the Dataset relates
- The owner is responsible for the data quality, security, reliability and availability of the data for which they are the Data Owner

26. Data operators

Data operators, under the guidance of the pertinent data owner, are accountable for the following:

Overseeing the operational aspects of the designated university data;

- implementing the University's established data management protocols and guidelines
- ensuring clear communication with technical specialists overseeing the data storage systems as well as the associated applications and reporting mechanisms
- conducting data evaluations
- supplying critical information to bolster University's decision-making processes
- ensuring the Data Dictionary is understandable to its users
-

27. Data Users

Data Users are required to

- access and use data only in their conduct of University operations
- consider the confidentiality and privacy of individuals whose records they may access
- consider any ethical, security or other restrictions determined by the DMC
- obey all relevant legal requirements
- work within only the data that they have been granted

28. This Policy should be evaluated periodically (amendments shall be done when there is a need) and it can be amended with the recommendation of the Senate Standing Committee on QA and followed by the Senate and Council approval (Policy on formulating and regulating policies of SUSL, Policy / SUSL / Gov & Mgmt / 14)

Legislative context:

1. Personal Data Protection Act No: 09 of 2022
2. RIT

Supporting Documents:

Annex 1: Composition of the Data Management Committee, SUSL

Policy on formulating and regulating policies of SUSL, Policy / SUSL / Gov & Mgmt / 14

ICT policy, SUSL

Responsibility: The Council of the University

Promulgation:

This policy will be circulated among all the students and staff of the University

This will be placed in the University website and in the University policy repository

Implementation:

This policy will be implemented by the Data Management Committee and the data owners as stated in the 25th line of the policy statement

Centre for Quality Assurance,

Sabaragamuwa University of Sri Lanka,

August 2023

******This has been approved at the 278th Senate held on 10.10.2023 and at the 302nd Council held on 27.11.2023***

ANNEX: COMPOSITION OF THE DATA MANAGEMENT COMMITTEE, SUSL

The Vice Chancellor (Chairman of the Committee)

All the Deans of the Faculties

Registrar

Bursar

Librarian

Deputy Registrars

Registrar /SAR, Examination