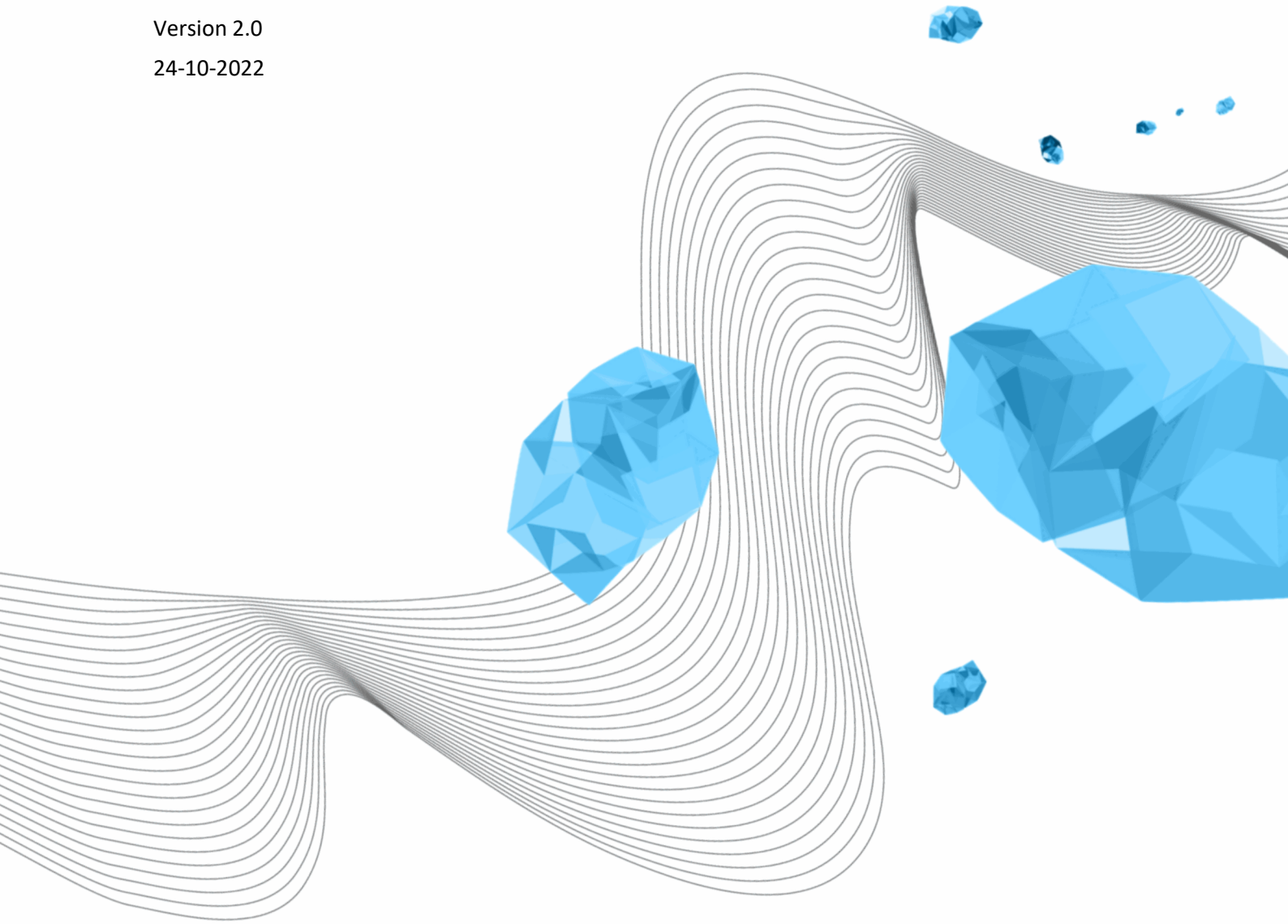
Status: final
Approved by the Executive Board on
24 October 2022

OWNERSHIP OF ENTERPRISE SYSTEMS

Erik van den Bosch

Version 2.0

24-10-2022



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Ownership of enterprise systems

SUBJECT
Agreements on the ownership of an enterprise system

ATTRIBUTE
LISA-0361

VERSION (STATUS)
2.0

DATE
24-10-2022

AUTHOR(S)
Erik van den Bosch

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
1.9	12-10-2022	Erik van den Bosch	Translation of the Dutch policy document *Eigenaarschap van een instellingssysteem,* version 1.83, Erik van den Bosch, 28-09-2022. Version 1.83 was approved by the CDO on October 11, 2022.
2.0	24-10-2022	"	Approved by the Executive Board in the EB meeting of 24 October 2022

DISTRIBUTION

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
1.9	12-10-2022	Erik van den Bosch	EB, for approval
2.0	24-10-2022	"	Publication on the Utwente Service Portal website

TABLE OF CONTENTS

INTRODUCTION

The UT has placed ownership of enterprise systems with the directors of the service departments. This memorandum clarifies what this role entails. In particular, this concerns control over the functionality of and the data in the systems and responsibility for security and privacy. This memorandum is intended for the owners of enterprise systems and their representatives in the I-Council. Service department directors are administrators (in Dutch: *beheerder*) according to Article 29(3) of the BBR (Administrative and Management Regulations, *Bestuurs- en Beheersreglement*). According to Article 30, paragraph 3 of the BBR, the Executive Board may issue regulations and instructions regarding the powers and duties of the administrator. This memorandum on ownership of enterprise systems can be considered such a regulation.

In addition, the target group consists of colleagues working in the IT chain: functional administrators, application managers, project managers and others involved.

WHO OWNS AN ENTERPRISE SYSTEM?

Every enterprise system has an owner who is responsible for that system. An enterprise system is a system that is of interest to a large part of the UT community and can be used by the entire UT. Precisely because the system is for general use, it is important to place responsibility for it clearly and in one place. The owner of an enterprise system is always a director of a service department. It is usually obvious which service department director is the owner. Generally speaking, the main person responsible for the business processes supported by the system is also the owner of the system. For example, the director of HR owns the HR system.

Usually, the daily direction of use and management of the enterprise system is delegated by the director to a team or department head from the service department. This person sits on the I-Council, a regular consultation of owners of Enterprise systems, chaired by the head of university information management. However, the director remains ultimately responsible.

The list of enterprise systems is kept up to date by UIM and published on the website utwente.nl/uim.

SYSTEM OWNER IS RESPONSIBLE FOR SYSTEM AND DATA

The owner of an enterprise system is responsible for the functionality and use of the system as well as the data stored in that system. This means that the owner deals with changes in functionality and renewal of the system.

The system owner, in coordination with the line management of the user organisation, determines who has access to (parts of) the system and who has access to the data in the system and takes care of granting access and authorisations. The system owner applies the UT's Authorisation Policy to manage access rights.

The system owner determines whether another system can access data in its system. Data integrations are important for user-friendliness and avoiding having to enter data twice. Aspects of privacy legislation and security should be considered here. See also the following section on source data.

To determine which security measures are needed for the system, the owner follows the UT Classification Guideline, which can be found at utwente.nl/cyber-safety.

The owner is responsible for designing the business processes within which the system is used, setting up the system appropriate to the process and providing appropriate information, training and training materials.

The owner is also responsible for managing the data in the system throughout their life cycle. The owner is thus also responsible for the mandatory periodic cleansing of obsolete data, in coordination with line management.

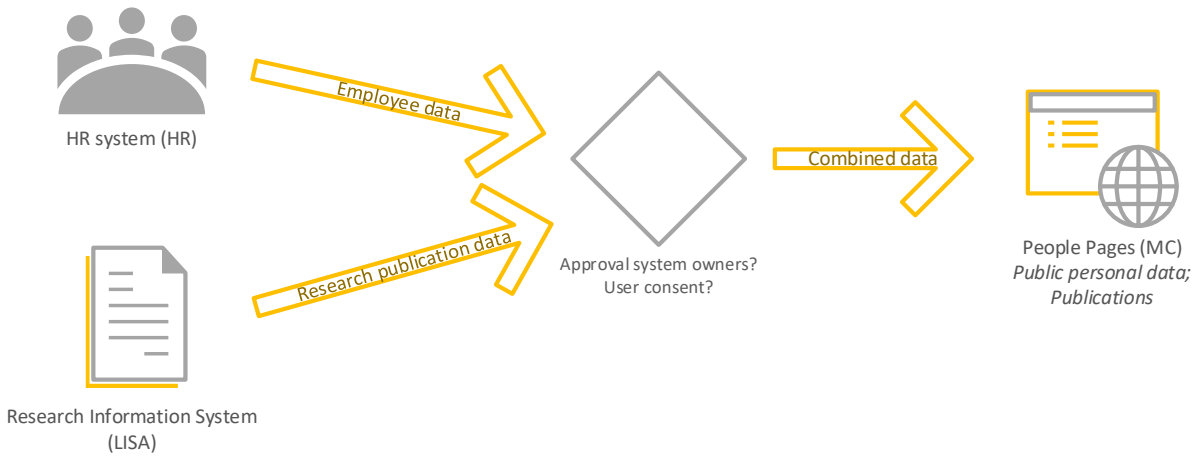
An important part of owners' responsibility is to draw up continuity plans: what should be done if the system is not available, perhaps for longer periods of time? These plans should integrate well with LISA's more infrastructure-focused continuity plans.

SOURCE DATA AND OWNERSHIP

According to UT architecture principles, we register all data only once, at the place where the data originates. This ensures that we work according to “a single version of the truth" and avoids confusion and unnecessary discussion. The system in which we initially register the data is called the source system. If this data is needed in other places, the owner of the source system must give permission based on established agreements. The owner of the system with source data also remains the owner of any copied data and retains control over the data.

However, a system owner is responsible for classification of all data in the system and for taking appropriate security measures (or having them taken).

In the example below, director HR as owner of the employee data and director LISA as owner of Pure determine whether employee data and publications respectively may be copied in People Pages (of M&C). In this specific case, the user can then specify what may be shown publicly. However, M&C should classify all data in People Pages, as combinations of data and a different context may lead to a different classification.



FUNCTIONAL MANAGEMENT

The owner of the enterprise system organises the establishment of functional management for the enterprise system. Functional Management represents the voice of the user. Functional Management ensures that the functions of the institution system and the business processes to be supported are well aligned. To this end, Functional Management organises good coordination with users (demand-driven). This includes making agreements on communication about maintenance and malfunctions and where end users can report incidents.

Functional management implements the UT's authorisation policy. Line management specifies who can access the data/system and with what rights, while functional management monitors the implementation of the authorisation policy. Furthermore, functional management supports users, communicates with them, provides manuals or other instructional materials and ensures that the system is properly embedded within the UT. University information management promotes and supports a coherent uniform way of working of the different functional management teams.

Functional management is responsible for the data quality of data created or modified within its managed system, and makes agreements with end users to this end. Data is delivered to receiving systems and to the UT data warehouse, and data quality works its way up this information chain.

CHANGE MANAGEMENT

Due to the integration of systems, changes in systems can have far-reaching consequences for the availability of other systems and for the quality of reports. In order to coordinate this properly, the UT uses the change management process, of which LISA is the process owner. All functional management departments must follow the central agreements in this process; the system owner is responsible for this. The I-Council is the body where agreements and working methods are discussed and recorded.

FUNCTIONAL MANAGEMENT, APPLICATION MANAGEMENT AND TECHNICAL MANAGEMENT

Functional management, as described above, is organised by the owner of the system. For systems where licences and hosting are not part of the same contract, hosting, application and technical management is placed with LISA and/or an external supplier. Functional management refers to managing the provision of information on behalf of a user organisation. Hosting refers to providing the hardware and infrastructure to 'run' and access an application. Application management includes managing, setting up, updating and installing the application, as assigned by functional management. Technical management concerns managing the underlying infrastructure (e.g. servers, databases, operating systems).

In the case of SaaS contracts, on which a large part of UT systems are now based, the software, hosting, application management and technical management are provided by an external party. Here, functional management often has direct contact with the supplier to discuss changes.

Systems can often be extensively configured through functionality available to functional management. This can include changing a field name, configuring a workflow, up to and including configuring complete data integrations with other systems. With these direct contacts and

functionalities, functional management has possibilities that were often reserved for the IT organisation in the past, and can make changes that can have far-reaching consequences for integrated systems, consistency in the application landscape and quality of reports.

To prevent problems arising elsewhere in the chain, all changes must be assessed for impact. Functional management has the responsibility to adhere to the change management process and central agreements. The LISA change manager is manager of this process. Changes in change management are discussed in the I-council.

Control over application and technical management always lies with LISA, even if external suppliers carry it out.

CONTRACT AND SUPPLIER MANAGEMENT

Procurement and making the right substantive agreements with suppliers is a highly specialised process that requires a lot of substantive knowledge. It involves, for example, conclusively recording agreements within the framework of the AVG, security agreements, technical agreements on data exchange, exit strategies, intellectual property, etc. The risk for UT of incorrect or incomplete contractual agreements is high.

For these reasons, for all enterprise systems (including SaaS) and all systems linked to them, procurement and contracting runs through LISA contract and supplier management. In this, LISA works closely with Procurement when it comes to procurement procedures and procurement compliance.

AUDIT STATEMENTS

If the system is a SaaS service, LISA Contract Management - if this is part of the contract - requests the audit statements annually and ensures that the owner receives a copy of these. If necessary, the owner coordinates with Operational Audit Department, which issues an opinion on the audit statement. If there are findings, the holder can discuss them with LISA contract management and the supplier. The system owner makes the final decision on the report.

SECURITY

The owner of the enterprise system is ultimately responsible for taking and complying with the measures needed to ensure an adequate level of security. The basis for determining what measures are needed is the classification of the data in the institution system according to the UT guideline (found utwente.nl/cyber-safety). The classification of data on the aspects of Availability, Integrity and Confidentiality is used to determine the level of security required. Which measures are needed at a certain classification level is determined by LISA's Information Security Officer.

The owner must report observed or suspected security incidents to CERT-UT. This is in order to be able to take the appropriate (technical) measures as quickly as possible, and to keep track of these incidents at UT level. LISA's Computer Emergency Response Team (CERT-UT) plays an important role in this. CERT-UT cooperates in a national network of CERTs. Security incidents can also be discovered by security managers or reported through the responsible disclosure procedure. Security managers assess the seriousness of a security incident and can independently decide to (temporarily) shut

down an information system if the seriousness of the incident makes this necessary. This is of course done in coordination with the responsible functional management department as much as possible.

PRIVACY

The owner of a system is responsible for respecting privacy laws. For the processing of personal data, the purpose and means of processing must be properly defined. If personal data are processed by third parties, a data processing agreement is needed. The data processing agreement should include an agreement on the life cycle of the data (retention period and ensuring that data is physically removed and can no longer be found via the internet). LISA contract management takes care of drafting data processing agreements that meet all requirements and coordinates this with the service department's Privacy Contact Person and UT's Data Protection Officer (DPO). The owner signs the agreement and is responsible for compliance.

Data breaches should be reported immediately to the Data Protection Officer. The DPO has a statutory role in this and, together with the Executive Board, considers whether a data breach should be reported to the AP (Personal Data Authority).