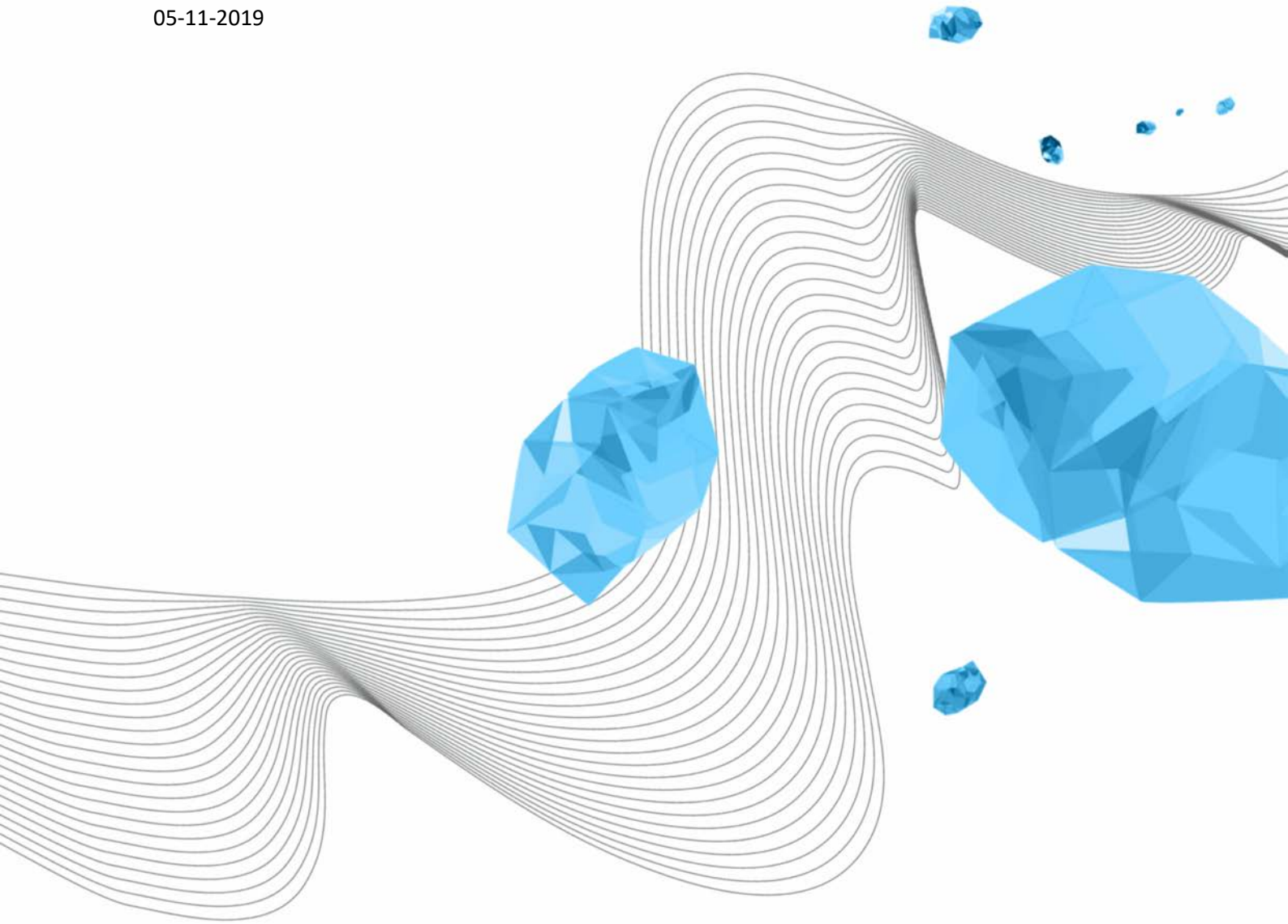
Status: Final
Date of adoption by Executive Board: 25-11-2019
Author: Harry Renting

UNIVERSITY OF TWENTE AUTHORISATION POLICY

Renting H. (LISA)

Version 2.2

05-11-2019



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
University of Twente Authorisation Policy

REFERENCE
[xx/xx/xx]

VERSION (STATUS)
2.2

DATE
05-11-2019

AUTHOR(S)
Renting H. (LISA)

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
1.0	2013	Wim Koolhoven	Final version
2.0	07-10-2019	Harry Renting	Adjusted for new authorisation procedure. Discussed with the Authorisation Policy project steering committee Minor textual adjustments
2.1	31-10-2019	Harry Renting	Discussed in the I-Consultations
2.2	05-11-2019	Harry Renting	Comments from the I- Consultations processed. 25-11-2019 Adopted by Executive Board (CvB)

DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
2.0	07-10-2019	Harry Renting	Authorisation Policy project steering committee
2.1	31-10-2019	Harry Renting	Members of the I-Consultations for discussion in the meeting of 31-10-2019
2.2	05-11-2019	Harry Renting	For adoption to CvB of 25-11-2019

TABLE OF CONTENTS

1 INTRODUCTION

The University of Twente uses information systems to consult and record relevant data. Integrity is paramount for all systems, as we do not want anyone to change data without any reason. Confidentiality plays a part with many systems: not everyone is allowed to consult personal data or otherwise confidential information[1]. For compliance with the GDPR it is necessary that the authorisation policy of the systems containing data about persons has properly been arranged.

The awarding of rights regarding who is entitled to do what is called authorisation. Checking whether someone is the person who he claims to be is called authentication and is set out in further detail in the Identity Management Policy Rules[2].

The Authorisation Policy is an instruction on how to deal with authorisations.

2 AUTHORISATION IN ACCORDANCE WITH THE ROLE-BASED ACCESS CONTROL PRINCIPLE

Authorisations for certain rights of access to an application are requested on the basis of one or several roles the person fulfils for that application. For this purpose, each application has a number of pre-defined roles. One or several rights within the application have been linked to each of these roles (RBAC: Role-Based Access Control). For each role, the connection between roles and rights has been set out in an authorisation matrix. The roles are not important for an application: in the end, it is all about recording the rights within the application. A person can have one or more roles for each application.

3 RESPONSIBILITY

The holder or owner of the information system also has the responsibility for the proper set-up of the authorisation procedure. In the Information Security Policy[3], this official is called the System Holder.

For the more complex systems, the party responsible for the data is not the same as the holder of the system. Usually, the responsibility for the system lies with a central unit and the responsibility for the data lies with an institute or a faculty. The party responsible for the process is responsible for the data in the system. The System Holder is responsible for the authorisation policy of the relevant system and for the coordination with the various parties responsible for the process.

[1] for further information, see Information and Information Systems Classification Guidelines http://www.utwente.nl/sb/uim/informatiebeveiliging/classificatierichtlijn_ut.pdf
[2] University of Twente Identity Management Policy Rules, reference SB/UIM/13/0213/khv
[3] http://www.utwente.nl/sb/uim/informatiebeveiliging/informatiebeveilingsbeleid_ut.pdf § 4.6.5, page 12

4 SEPARATION OF DUTIES

The UT applies a separation of duties for authorisations. In general, the following roles can be distinguished here:

Applicant: this person applies for these authorisations and changes of authorisations on behalf of the party responsible for the process. The applicant is usually the head of a department or a team leader.

Authorisation Matrix Owner: is responsible for the authorisation data and checks the authorisation matrix on a regular basis. This person must be appointed per application. The authorisation matrix owner is usually the same person as the system holder.[4]

Functional management: this department checks the applications and supervises the authorisation procedures on behalf of the system holder.

Application management: is tasked with the implementation of the changes of authorisations.

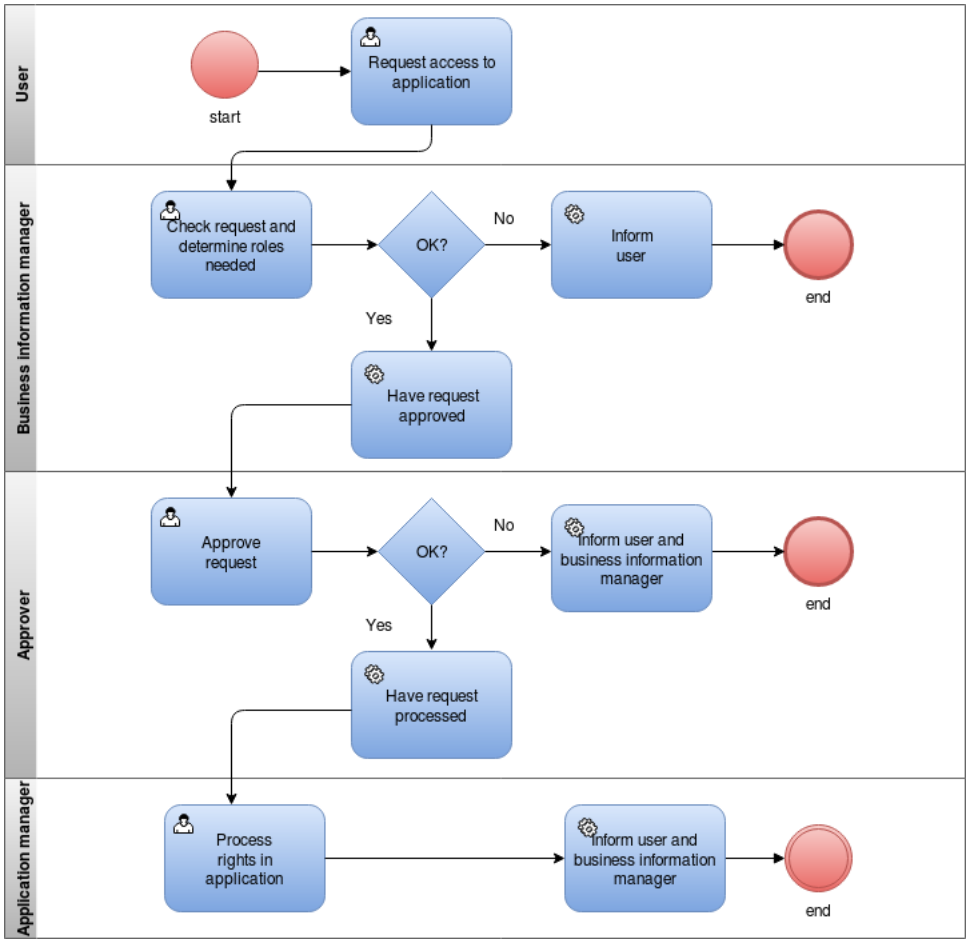
5 AUTHORISATION MATRIX CHANGE PROCESS

The authorisation matrices have been designed in such a way that they will not often require adjustments or changes to the authorisation matrix per application. If a change is desired, because of a changed situation, it is recommended that any change is made no more often than once or twice per year. The owner of the authorisation matrix determines the changes after advice from an advisory council he composes from users of the application in question, supplemented with a functional manager and the functional manager of the TACS authorisation management application.

[4] For each application, the job titles have been specified in the appendix.

6 PROCEDURES

Authorisation application procedure



This procedure is followed for applications for new staff authorisations as well as for changes in existing staff authorisations. All relevant details are stated in the application; these details are different for each system. When the application is checked, it is checked not only whether the application is complete and clear, but also whether the applicant is authorised to make the application.

The application for access rights is not directly made by the end user, but by the manager (or his substitute), through the functional manager of the application. It is often clear in advance which roles a new staff member needs within the applications to be used. The aim is therefore to have this arranged before the start of the employment.

The end user himself does not play an active part in the authorisation process.

6.1 PROCEDURE FOR WITHDRAWAL OF AUTHORISATIONS

If a staff member leaves the UT or takes up another position, authorisations will have to be withdrawn. The applicant is primarily responsible for communicating this to the functional manager in good time.

6.2 PROCEDURE FOR PERIODIC CHECKS ON AUTHORISATIONS

As mistakes are always made in practice, it is important to check on a regular basis whether the authorisations assigned are still correct. Usually, it is quickly acknowledged that a user has been awarded too few rights, because as a result, the work cannot be carried out properly. However, too many rights may result in undermining of the principle of separation of duties and entail risks that are bigger than necessary.

Twice a month, the functional manager of the relevant system runs a report that provides an overview of the rights awarded to each staff member. After a check performed by the functional management department, this report will be sent for validation to the relevant persons responsible for the process. Any errors detected will be rectified as soon as possible.

6.3 PROCEDURE FOR LOGGING AND PERIODIC AUDIT

In order to establish in retrospect what actions were taken in the authorisation process, it is important that these actions are recorded. As from 1 November 2019, an application (TACS, *Twente Authorisation Control System*) has become available, using which the application for an authorisation is recorded.

For systems that have been classified as critical in terms of Integrity or Confidentiality, it is necessary that the applications as well as the execution are recorded and that an audit is conducted at regular intervals.

7 IMPLEMENTATION AND EVALUATION

University Information Management publishes this guideline and brings it to the attention of the system holders. After this, UIM will make regular enquiries with the holders into its implementation. Next year (2020), this policy and its implementation will be evaluated in the I-Consultations.

8 APPENDIX 1

This appendix is a 'living' document. Whenever applications are added to TACS, these applications will be included into this appendix.

8.1 OVERVIEW OF OWNERS OF AUTHORISATION MATRICES

Application	Position	owner
Oracle Finance	Head of Financial Services	R.P. Ree
Oracle HR	Head of HR Services	A.G.M.J. Holterman
Osiris	Head of Information Management	J. Pasman
BO	Projects & Development Department Head	E.A. van den Bosch N.J.C. Letteboer (SP)
JOIN*	Head of University Information Management	J.L. Evers

* Ad interim situation.