Identity & Access Policy

TILBURG UNIVERSITY

Commissioner	:	Corné van Nispen

Revision History

Document Management				
Version	**Date**	**Distribution**	**Status**	**Changes on key points**
0.1	July 6, 2022	IAM project team: Frank van den Tillaart, Jurgen van Dijk, Niek Vrijssen, Remco Nijkamp, Peter Kleijnjan	draft	First version
0.2	July 22, 2022	Peter van Empel, Edwin Groenenberg, Emile Petit, Tessel Stoppelenburg, Ton Aben	draft	After review by Jurgen van Dijk, Remco Nijkamp, Niek Vrijssen, Frank van den Tillaart
0.3	Sept. 19, 2022	Jolanda Peters, Paul Geerts, Patrick Rozema, Tessel Stoppelenburg, Ton Aben, Eric Peeters, Maurice Driessen	draft	After review by ISOs: several paragraphs were removed, which will be included in a separate access policy
0.4	Oct. 21, 2022	Jolanda Peters, Paul Geerts, Patrick Rozema, Eric Peeters, Maurice Driessen, Emile Petit, Peter Kleijnjan, Frank van den Tillaart	draft	Reviews processed; list of open items prepared for discussion; Authorization Committee added in 3.5
0.9	Nov. 16, 2022	IAM steering committee	draft	After discussion of outstanding items; final draft.
1.0	Nov. 30, 2022		Final	After approval by steering committee. Minor changes to Sections 1.5 and 2.6 at the request of CISO.
1.1	Dec. 6, 2022	MUS and BoM	Final	Composition of Authorization Committee added in 3.5
1.2	Nov.29, 2023	EB	Final	Bulk registration guests expires (2.2.3.1) and no further changes after drafting IAM processes and recalibration project

Content

1. About the Identity & Access Policy

1.1 Purpose and scope

This document describes the policies and business rules that apply within Tilburg University (TiU) for processes and functionalities related to identities: who are you? What is your relationship with our organization? - And with access: what are you allowed to do? And why are you allowed to do that?

The policy in this document applies to all employees, external employees (*PNIL*), students, and guests of Tilburg University and to situations related to work or study and/or activities taking place on campus.

Within TiU, we strive for an integrated approach to information access (logical access) and physical access. Therefore, the rules for both areas come together in this document.

Despite its size, the purpose of this document is that it is readable and understandable in its entirety by directors, managers, and information managers of the Divisions and Schools, and that they are able to commit themselves to it in practice: after all, it provides the "rules of the game" that apply to our business processes.

1.2 Principles

The design of access and entitlement management is governed by these principles:

i. **Regulations & standards are leading**: our processes and systems for identity & access management ensure that we structurally comply with applicable laws and regulations, such as ISO27001, GDPR, and the SURF Standards Framework.

ii. **No access without registration**: the person's identity and relationship with TiU is verified and recorded in a reliable process.

iii. **Traceability**: all access is traceable to a natural person. All access rights are traceable to policies and/or decisions made by a responsible person, such as a manager and/or process or system owner.

iv. **Secure where necessary, freedom where possible:** broad access enables flexible collaboration. Therefore, we regulate access as broadly as possible, although the higher the risk, the more limited the access.

v. We respect the responsibility of **specific stakeholders** such as owners/managers of particularly sensitive information systems and areas with specific security requirements.

vi. **Simplicity, speed, and predictability:** access management is designed so that employees, external employees, students, and guests are quickly provided with the access resources they need and that this is done in a process that is understandable and predictable to the manager.

vii. **Financial efficiency:** access to facilities is increasingly dependent on person-based licenses or licenses with maximum numbers. To control costs for TiU, access to such facilities is intricately facilitated.

1.3 Related standards and documents

This policy can partly be seen as a fulfillment of a measure in accordance with the information security policy and partly as an extension of it:

- Information Security Policy Tilburg University with associated:
- Baseline Information Security[1]

TiU's facility user regulations and code of conduct are also relevant in this context:

- Code of conduct for the use of E-mail, Internet and Telephone Facilities Tilburg University
- Code of Conduct, specifically "Processing Information"

Also, this policy touches on the following TiU regulations:

- Tilburg University Mandate and Authorization Regulations;
- Administration and Management Regulations; (in Dutch)

TiU aims to achieve a higher maturity level in the area of identity and access management. To this end, the SURF Standards Framework is used to periodically test this maturity level:

- SURF Standards Framework

In addition, there are policies, which provide further detail on aspects that are relevant to this policy:

- Policy providing facilities *PNIL* and Post-active staff (April 2022);
- TiU access policy (physical and logical for non-regular accounts).

1.4 Terminology

This Tilburg University Identity and Access policy is also referred to as the TiU IAM policy.

In this policy, the following terms are defined and used as follows:

- **Identification**
  Disclosing the identity of individuals, organizations, or digital facilities. This can be done in the physical sense through the use of an identity document or certificate. In the digital world, a digital identity is used for this purpose, usually in the form of an account or digital certificate.

[1] See TiU Baseline final Version 1.0 dated October 2021.

- **Authentication**
  The verification of a claimed (digital) identity so that it can be shown that the person who identifies himself or herself is actually the person who pretends to be such. Authentication is also referred to as: verification of identity. Authentication is usually done on the basis of something that only the user can know or have at his/her disposal.

- **Entitlement**
  Granting permission (an entitlement) to an authenticated party to access a particular service and/or perform a particular action. Except for public information and freely accessible services, this means giving the user the appropriate authority to perform work or to study at the University.
  A further detailing of the generic term “entitlement” reads as follows:

i. A **role** is a classification of persons that is meaningful to the organization and says something about the relationship between the person and the organization.
ii. An **authorization** represents the right to access a particular area, system, functionality, or information or the right to perform a particular action. An authorization is requested, granted, and then issued (and eventually revoked and then taken away).
iii. Authorizations take shape in an application or system as **permissions**.

1.5 Life cycle of this policy

This Policy is adopted by the Executive Board. The chief information officer (CIO) and system owners are responsible for the implementation and compliance with measures. This Policy also applies to services provided by TiU to TIAS.

The chief information security officer (CISO) provides solicited and unsolicited advice on this policy and its compliance.

Following the management cycle of the Information Security Policy, the Identity and Access Policy will be reviewed and, if necessary, updated at least once every two years. Also after a substantial change in institutional policy or significant cybersecurity developments, the Policy will be reviewed and re-adopted by the Executive Board.

2 Identity Management

2.1 Types of identities

The University grants access to (part of) TiU's physical and digital facilities only to identified, authenticated, and authorized persons who need such access for their studies, work, or another valid reason. A distinction is made between the following categories:

1. Staff
   In this document, "employee" means anyone, who is registered by TiU's personnel administration as a salaried employee (*personen in loondienst* (*PIL*)).

2. Persons not employed
   Here a distinction can be made between:
   a. External employees (*personen niet in loondienst* (*PNIL)*);
   b. Post actives; this category will be phased out from the second quarter of 2022 and henceforth registered as *PNIL*.

   Depending on the registration, it is possible to distinguish between subgroups within the *PIL* and *PNIL* categories.

3. Students
   In this document, "student" means anyone who attends TiU and is registered as such in the TiU Student Information Systems. A distinction can be made among:
   a. applicants;
   b. students;
   c. course participants.

   Depending on the registration, it is possible to distinguish between subgroups within these categories.

4. Guests
   “Guest” in this document means anyone who receives temporary access to specific digital facilities at the invitation and under the responsibility of a University employee and is registered in a guest system of record. A distinction can be made here among:
   a. guests general;
   b. guests with Wi-Fi access only;
   c. guest borrowers, individuals who only use the Library facility and/or Brabant Collection.

5. TIAS Users
   Tilburg University provides IT services for the TIAS School for Business & Society, the business school of Tilburg University and the University of Technology Eindhoven. It concerns non-funded education. TIAS has its own system of record distinguishing among the following types of users:
   - salaried Employees (*PIL*);
   - staff, lecturers employed on a self-employed basis (*ZZP*) (*PNIL*);

- full-time students;
- part-time students, divided into two groups:
  - students attending an NVAO accredited program;
  - students attending short programs, not accredited.

6. Externals
   “External” in this document means anyone, who does not appear in any of the other categories and therefore is not registered in any of the TiU system of records. A distinction can be made between:
   a. TiU alumni;
   b. students, lecturers, researchers, or guests who need access to TiU's digital facilities and get this with their own (institutional) identity and account;
   c. employees of external partner organizations, such as suppliers and management parties. For this, we rely on the identity management of the organization involved.

2.2 Registration of persons

2.2.1 Registration of employees and persons not employed

Salaried personnel (*PIL*) are recorded[2] in the employee system of record with a copy of an identity document stored. The date of employment and end date of the employment contract are also recorded. If the end date of an employment contract changes (including termination of an open-ended employment contract), the manager is responsible for notifying HR in a timely manner.

Persons not employed (*PNIL*) are recorded[3] in the HR system of record, where a copy of an identity document is requested, checked, but not stored. The start and end date of the contract are also recorded. If the end date changes, the manager is responsible for notifying HR in a timely manner.

TIAS staff and guest lecturers are registered by TIAS in their system of record.

2.2.2 Registration of students

Participants in regular education (Bachelor's, pre-Master's, Master's) enroll through Studielink, and thus enter the student system of record and are registered as "student.”

Participants in non-formal education are recorded through various processes and systems and then entered into the student systems of record as "course participants.”

Full-time TIAS students and participants or course participants are registered by TIAS in their system of record.

Identity verification takes place with all these users.

[2] In accordance with HR's work instructions "Instruction on Submitting PIL," "Instruction on Submitting Student Assistants," and "Instruction on Submitting Trainees."

[3] In accordance with HR's work instruction "Entering PNIL."

2.2.3 Registration of guests

2.2.3.1 Guests in general

It is possible to register guests with IT Support. For this purpose, a Guest Form is available to provide the necessary data. IT Support generally enters these guests into the guest system of record, registering the applicant as the responsible party.

Identity verification also takes place with this type of user.

Note: It is possible to register yourself separately as a guest for the printer/scanner/copier. This registration is located with the supplier of this equipment and not with the University. Users with a TiU account can use this to log in to this equipment.

2.2.3.2 Guests with Wi-Fi access only

To provide network access to guests we use eduroam Visitor Access (eVA); this is a service offered by SURF. EVA supports guest access by invitation of TiU staff or via self-service. Registration of this type of guests takes place directly in eVA where identification is based on text messages and, thus, the guest's mobile number. In the event that a guest is guilty of committing crimes while using our network, the justice system can find out the guest's identity through the guest's telecom provider.

2.2.3.3 Guest borrowers

Like regular guests, guest borrowers are registered in the guest source system. However, they receive a pre-produced—still anonymous—Tilburg University card, to which the guest's data are later linked by the identity management system.

Verification of identity also takes place with this type of user.

2.2.4 Registration of TIAS users

TIAS has its own CRM system in which all users are registered, which serves as the system of record for TiU.

Verification of identity also takes place with this type of user.

2.3 Digital identity, TiU account, and basic rights

2.3.1 Identity, Account and Naming

Based on the registration in one of the systems of record, the identity management system creates a digital identity and a Tilburg University account. A single digital identity and TiU account is created per natural person. If a natural person appears multiple times in the systems of record, for example both as an employee and as a student, a matching process is performed to link the source data to the same digital identity. In this matching process, match candidates are presented to specifically designated individuals, who may approve the match or decide that a new identity and account will be created.

An administration number (ANR) is assigned to all individuals who are given a TiU account. The ANR is a 6-digit number that uniquely identifies a person. Every effort is made to provide returning individuals with their old ANR whenever possible. A person may be assigned a new ANR, but the ANR is never reused for another person.

The naming of accounts is based on the person's name or ANR. In principle, the user name is never changed because it has consequences for a user's profile in applications. Exceptions are submitted to the CIO for approval.

Note: This Identity & Access Policy covers regular user accounts. Other types of accounts, including management, test, and vendor accounts, are the subject of a more in-depth access policy.

2.3.2 Basic Rights

Depending on the type of user, an initial set of access rights is assigned to the account, and it is determined whether the user will have access to a campus card.

The TiU self-service portal publishes the current overview of basic rights ("account facilities").

2.3.3 Joining, moving, leaving

A TiU account is automatically created upon **joining** the organization after registration in one of the systems of record. An account is initially created at the following time:

- Employees: once the new employee is entered into the source system and the contract is signed;
- Persons not employed: once the new person is entered into the source system;
- Students: after enrollment in a study program and up to three months before the start of the study program;
- Guests: once the specified effective date is reached;
- TIAS: once the effective date of the contract/study is reached.

Upon a mutation of name information, organizational unit, and/or position or study (**moving**) in the system of record, the account and basic privileges are updated on the effective date of the mutation. For employees and external employees, the manager is responsible for timely notification of mutations to HR.

If a user receives an additional registration of another type, that new type is added to the account. From this point on, all authorizations (facilities) from all assigned types are made available to that person. It is also possible that a user type ends in the interim. At that time, access to the facilities of that specific type is removed from the account according to the leaving procedure that leads to withdrawal of facilities per type. Facilities granted from other types remain granted on the account.

If a person no longer has a relationship with Tilburg University, the person's account will be terminated. The **leaving procedure** starts at the following time:

- Employees: once the end date of the contract has passed;
- Persons not employed: once the end date of the contract has passed;

- Students: once the end date of a study program is processed or if a student has not met all enrollment requirements by October 1 of the current academic year;
- Guests: once the guest registration end date is processed;
- TIAS: once the end date of the relationship is processed.

Removal of facility access is still subject to the following phasing:

- on the end date: access to the account and facilities remains intact.
- After 32 days: access to the account and therefore the facilities are closed.
- Up to 60/90 days: if the account is reactivated, access to email is restored. After 60/90 days (depending on the email provider), the email recovery period expires.
- Up to 90 days: if the account is reactivated: access to the account and facilities is restored.
- After 90 days: accounts in facilities are cleared, as much as possible.
  The account itself is cleared. For applications, where accounts are created via automatic links to the identity management system, the account is also cleared automatically. For other applications, the functional administrator is responsible for the clearing process, for example, based on the date of the last login.
  The exception to this term is for the learning management system, where accounts are only cleared after two years due to legal obligations.
- Up to 2 years: if personal data is re-entered and matching takes place: The ANR can be reused in a new account.
- After 2 years: if the personal data is re-entered, a new ANR is used in a new account unless the person is recognized in the system of record based on retained data.

Finally, there is an **emergency button**. In the event of a labor dispute, instant dismissal, serious misconduct, etc., the user's access can be blocked with immediate effect at the initiative of the Managing Director of the School or Division concerned.

2.4 Authentication tools

2.4.1 Campus card

The campus card (Tilburg University card) can be applied for by *PIL*, *PNIL,* and students. The card is not issued automatically. After loss or (at a person's own request) if the name has changed, a replacement card can be requested after the old card has been blocked. The card has a photo, name, and student or administration number[4].

Prior to being issued, the person's ID is checked. No record is made of this check.

Each user always has a single valid card, even in the case of multiple appointments, roles, or studies.

The card is blocked after the end of contract/end of study program date, so it cannot be used for access anymore.

[4] See Tilburg University card | Tilburg University.

2.4.2 Passwords (First factor)

Upon registration, a user will receive an email containing the TiU account information and a link to a page to set the password. The password must comply with the password policy (see below under password rules).

The rules for the password, recovery, lockout, etc. are defined in the Access Policy.

2.4.3 Second factor

TiU has a policy of second factor account protection. This means that when logging into applications, in addition to a password, a second means of authentication (an app or token) is required. For this the following applies: “a second factor unless,” where the CISO advises on the exceptions based on a risk analysis.

If a user does not have access to the second factor, a procedure is set up for the provision of a temporary solution. Thus, the second factor is not switched off.

2.4.4 TiU as identity provider

When accessing applications, *single sign-on* is preferably used through TiU-managed facilities or through SURFconext, the national federation for secondary and higher education and research. In this process, users log in with their TiU identity and means of authentication provided to them. The application first leads the user past the TiU identity provider where the user logs in—usually with password and a second factor. Then the user is provided with the appropriate attributes (for authorization purposes) and returned to the application.

For eduroam, RADIUS is used as the identity provider for TiU.

2.5 Other account types

In addition to regular TiU user accounts, management, service, vendor, and functional accounts are also used within TiU. The rules for these are described in a separate Access Policy.

2.6 Accounts in applications

An application must use the central TiU authentication facility or TiU identity provider (see 2.4.4) according to the "comply or explain" principle.

If an application is not connected to the IAM platform, the person responsible for the application must ensure that connection to the process of joining, moving, and leaving is guaranteed, in particular that accounts are blocked and deleted in a timely manner after leaving service or after the end of the contract.

If the use of local accounts is unavoidable, the Access Policy describes the rules for these types of accounts.

2.7 Accounts in equipment

The rules for local accounts in equipment such as network, telephony, AV, and laboratory equipment are also detailed in a separate Access Policy

2.8 Archiving and retention of identity data

Identity data is deleted from the IAM platform after two years. The purpose of retaining data is to be able to re-issue the administration number, username and e-mail address if a user is re-registered in one of the systems of record within this period. This period is short enough to avoid keeping redundant data in the system and long enough to provide returning users with their old account and e-mail address in practice.

Different rules may apply to supplying systems of record.

3 Access Management

3.1 General

This chapter applies to logical entitlement management (access to information systems) and also physical access (access to areas within the university).

For definitions of entitlement, role, authorization, and permission, see in Section 1.4.

A **role** contains one or more authorizations; an **authorization** is translated into one or more **permissions** in a system.

Granting (or *revoking*, as appropriate) refers to the decision to issue or deny the entitlement; it is an administrative process. If multiple parties must give approval, it is part of the granting process.

By contrast, *issuing* (or *withdrawing*) is an operational task with no decision element: the management actions necessary to set up granted entitlements for the user in question; these may be partially automated.

In other words, granting and revoking relate to the norm (the "**Soll**"). Issuing and withdrawing have the purpose of bringing the current situation (the "**Ist**") in line with the norm.

3.2 Grant and revoke entitlements (soll).

Tilburg University opts for pragmatic role-based access management with recording in the IAM facility. This includes:

i. Each user is automatically assigned one or more roles based on employment, organizational unit, and position, or study program. These roles vary from organization-wide (student) via general organizational unit or education roles (Tilburg Law School) to very detailed (Functional Administrator LIS). Thus, roles can be assigned or taken away when the relationship changes, also for multiple relationships.

    a. Each role includes the relevant authorizations to different systems and spaces.

ii. In addition, flexible roles and authorizations can be assigned to users on an individual basis based on a particular relationship with the University.

iii. By "pragmatic" we mean that we do not try to assign all entitlements with roles but accept that the automatically assigned roles comprise on average about 60-80% of the total access profile—and that the rest must still be assigned separately.

Automatically assigned roles are based on policy. For automatically assigned roles, both the role definition (what entitlements) and the role assignment rules are organization-wide and reviewed periodically. Access granted based on these automatically assigned roles is thus based on policy, not an individual decision.

The TiU Authorization Committee is responsible for managing this role logic and ensuring that it is periodically reviewed, approved, and published (see Section 3.5).

The assignment of **individual authorizations**, in addition to the roles model but within its frameworks, is a **management decision**. The manager in line is responsible for all individually assigned employee entitlements. The manager decides on granting and revoking these, possibly after approval by process and/or authorization owner.

A manager can grant or revoke individual entitlements with direct entry in the IAM facility or via notification in the service management system to IT Support.

Supplemental, not restrictive. Authorizations granted as part of an automatic role cannot be revoked for individual employees.

Traceability. Any user authorization can be traced to a policy decision or to the decision of a responsible manager or the process or authorization owner.

Authorization owner. Some authorizations have such a risk profile that, in addition to the manager, the "owner" of the room or data must also be involved in the access decision. The ground rules for this are:

i. The authorization owner reports to the IAM Gatekeeper (see Section 3.5) of his/her organizational unit and is recorded by IAM management in the IAM facility as such with the authorization.
ii. The manager who wishes to grant the authorization in question on an individual basis to an employee agrees in advance with the authorization owner.
iii. The authorization owner receives an automatic notification as soon as the authorization is granted on an individual basis. He/she can revoke the authorization immediately by notifying the IAM Gatekeeper.
iv. If an authorization owner objects to the inclusion of an access right or authorization in an automatically assigned role, he/she can have the role definition modified by the Authorization Committee. This then applies to everyone who has or receives the role.

3.3 Entitlements and the life cycle

Automatic role assignment for future users occurs at the time of registration as soon as this is passed to the IAM facility, see also Section 2.3.3.

In case of progression, that is, mutations in the organizational unit, position, or study program, the automatically assigned role package for the respective relation is adjusted as of the date the mutation takes effect.

There is no "overlap," no period where the user keeps the old rights and acquires the new rights “in advance.” If needed for transfer or preparation, for example, additional authorizations can be granted on an individual basis—preferably immediately including an end date.

On the end of contract or end of study program date, all automatically assigned roles are revoked subject to the deadlines mentioned in Section 2.3.3.

Individually assigned roles and authorizations remain in effect until the end date of those authorizations (if indicated) and otherwise until 90 days after the end of contract or end of study program date, that is, on the same date when the TiU account is deleted. The majority of re-entrants within this period consist of users whose contract renewal or registration (and payment) for a course was not processed in a timely manner and in this way we minimize the impact of this. If a re-entrant has another position or training within this period, then this is (still) progression.

3.4 Entitlement management in applications (soll to ist)

Each authorization that can be granted has a name and description in which the purpose and scope of the authorization is described for managers. These definitions are maintained in the IAM facility by functional management IAM.

Mapping of permissions to authorizations. The application's functional administrator is responsible for the correct mapping of "logical" authorizations in the IAM facility to the "technical" permissions or profiles in the application.

Provisioning of permissions. The functional administrator is also responsible for ensuring that the assignment of authorizations (as recorded in the IAM facility) in the application results in the proper issuing of permissions.

For applications with an automated link to the IAM facility, this mainly means: monitoring that the link works properly at the functional level.

For applications linked to the IAM facility with a work order process, this means: monitoring that the actual permissions match the assigned authorizations, supported for example by Soll/Ist comparisons from IAM.

For **permissions that are not included in authorizations in the IAM facility**, the functional administrator is responsible for registering the entire process of granting, issuing, revoking, and withdrawing. Each permission granted must be traceable by the functional administrator to the specific decision of a responsible party.

In some applications--for example, in SharePoint, Teams, Canvas--the management of permissions for certain data areas (teams, sites, groups) can be delegated to their owner.

3.5 Authorization Committee and IAM Gatekeepers.

Composition. At least twice a year, university wide, the various stakeholders in access rights management meet in the Authorization Committee:

	policies and procedures	role model and authorization matrix	case study
permanent members			
Owner domain IAM (CIO).	V	optional	optional
Head of Internal Audit & Compliance	V	V	V
Internal audit / privacy officer	optional	V	optional
Chief info security officer (CISO)	V	optional	optional
Central IAM Gatekeeper(s).	optional	V	optional
LIS/Process specialist IAM	optional	optional	optional

Additionally, insofar as they have an interest in the agenda:

- of the organizational unit involved: the privacy officer, IAM Gatekeeper(s), and/or information manager;
- involved heads of organizational units, process owners, and project leaders;
- functional managers of affected systems.

The Authorization Committee's **duties and mandate** are:

- Review and approve **policies and procedures** regarding authorization management, possibly leading up to formal adoption by the EB. The current document serves as the framework for this.
- Review and establish the **roles model**. This includes:
  - role definitions: what groups do we know, how do we recognize them?
  - role assignment: who is assigned (automatically or manually) to which roles?
  - authorizations: what profiles are there, are they recognizable to the business?
  - authorization matrix: which authorizations can be provided automatically or additionally per role?
  - segregation of duties: which authorizations should not be combined?

  The Authorization Committee focuses on the level of roles and authorizations, each of which has a name and description recognizable to the business. Correct mapping of authorizations to the system-specific permissions is a responsibility of the functional administrators involved (see Section 3.4).
- **Case studies**. In some cases, the parties involved cannot agree on the design or definition of roles and authorizations. There is a lack of clarity as to who is authorized to decide, or

there is a need for an exception to the established rules and frameworks. Such cases are then submitted to the Committee for review and decision-making.

The "V" in the Committee composition table indicates which members must be present to make decisions on the given items.

The **IAM Gatekeepers** are jointly responsible for maintaining the roles model, where:

- **entitlement rules** require the approval of the managers and/or process owners involved;
- **role authorizations** and the **authorization matrix** require the approval of managers and/or process owners involved as well as the functional administrators of the systems involved;
- the IAM Gatekeepers are responsible for **delineating, naming, and documenting** roles and authorizations in such a way that managers and the Authorization Committee can base decisions on them;
- new or changed roles and authorizations are submitted to the Authorization Committee **for adoption** at least twice a year; until then, IAM Gatekeepers are responsible for the accuracy of roles and authorizations.

4 Monitoring and Protection

4.1 Logging

Per application/per system. The application owner is responsible for ensuring that logging is set up properly:

- log files must be created, retained, and reviewed regularly in accordance with the TiU Baseline Information Security;
- security and availability incidents must be able to be analyzed retrospectively and traced to data/position, place, time, and person (who/what/where/when);
- access to and handling of logs complies with the TiU Baseline Information Security.

Systems preferably connect to TiU's SIEM facility; applications do not.

Retention periods. Application logging should be retained for a set period of time.

In case of a (suspected) information security incident, the retention period of logged incident information is at least three years.

4.2 Attestation by managers

Once a year, functional management IAM asks or facilitates all managers to verify that the data as known in IAM is correct and complete.

This attestation includes:

- Is the list of employees (*PIL* and *PNIL*) reporting to the manager correct?

- Are the assigned individual authorizations correct for these employees?

As part of the attestation process, the manager is also offered insight into automatically assigned roles so that any errors in role assignment can be identified. However, the manager is not primarily responsible for this part.

For attestation of elevated rights accounts, see the separate Access Policy.

4.3 Management and control of roles book and authorization matrix

Twice a year, the (by the) Authorization Committee (designated employee) performs random Ist/Soll checks on the roles book and authorization matrix:

- Are the actual authorizations of the selected employees in line with the matrix?
- Is the translation of IAM roles to authorizations (access to applications) correct for the chosen employees?
- If deviations from the matrix have occurred, can these deviations be explained by previous decisions of the Authorization Committee?

5 Documented Exceptions to this Policy

This final section briefly describes known exceptions to this Policy. After all, this Policy describes the desired ground rules in the IAM domain, and they may not yet be standing practice.

- Re Section 2.3.1: In principle, the account created for each person concerns a Microsoft Active Directory (AD) account. Until further notice, it is accepted that this account is also included in OpenLDAP.
- Re Section 2.2: Identity verification does not always take place upon registration.
- Re Section 2.2.3.1: The applicant is not recorded as responsible in the registration of guests but the person from IT Support who handles the registration is.
- Re Section 2.6: Not all applications use the TiU account; some still have their own account: Planon, SAP, Business Objects, and xFlow, among others.
- Miscellaneous sections: Still to be drafted is the Access Policy for non-regular TiU user accounts.