Beleid Identiteiten & Toegang

Opdrachtgever : Corné van Nispen

Revisiehistorie

Documentbeheer				
Versie	**Datum**	**Distributie**	**Status**	**Wijzigingen op hoofdpunten**
0.1	06-07-22	IAM projectteam: Frank van den Tillaart, Jurgen van Dijk, Niek Vrijssen, Remco Nijkamp, Peter Kleijnjan	concept	Eerste versie
0.2	22-07-22	Peter van Empel, Edwin Groenenberg, Emile Petit, Tessel Stoppelenburg, Ton Aben	concept	Na review door Jurgen van Dijk, Remco Nijkamp, Niek Vrijssen, Frank van den Tillaart
0.3	19-09-22	Jolanda Peters, Paul Geerts, Patrick Rozema, Tessel Stoppelenburg, Ton Aben, Eric Peeters, Maurice Driessen	concept	Na review door ISO's: diverse paragrafen verwijderd, die in apart toegangsbeleid komen
0.4	21-10-22	Jolanda Peters, Paul Geerts, Patrick Rozema, Eric Peeters, Maurice Driessen, Emile Petit, Peter Kleijnjan, Frank van den Tillaart	concept	Reviews verwerkt; lijst van openstaande punten opgesteld ter bespreking; autorisatiecommissie toegevoegd in 3.5
0.9	16-11-22	Stuurgroep IAM	concept	Na bespreking openstaande punten; finaal concept.
1.0	30-11-22		Definitief	Na goedkeuring door stuurgroep. Kleine wijzigingen in par. 1.5 en 2.6 op verzoek CISO.
1.1	06-12-22	MUS en CvB	Definitief	Samenstelling Autorisatiecommissie toegevoegd in par. 3.5
1.2	29-11-23	CvB	Definitief	Bulkregistratie gasten vervalt (2.2.3.1) en verder geen wijzigingen na opstellen IAM-processen en herijking project

Inhoud

Revisiehistorie 2
1. Over het beleid Identiteiten & Toegang 4
1.1 Doel en reikwijdte 4
1.2 Uitgangspunten 4
1.3 Gerelateerde normen en documenten 5
1.4 Terminologie 5
1.5 Levenscyclus van dit beleid 6
2 Identiteitenbeheer 7
2.1 Soorten identiteiten 7
2.2 Registratie van personen 8
2.2.1 Registratie van medewerkers en personen niet in loondienst 8
2.2.2 Registratie van studenten 8
2.2.3 Registratie van gasten 9
2.2.4 Registratie van TIAS-gebruikers 9
2.3 Digitale identiteit, TiU-account en basisrechten 9
2.3.1 Identiteit, Account en naamgeving 9
2.3.2 Basisrechten 10
2.3.3 Instroom, doorstroom en uitstroom 10
2.4 Authenticatiemiddelen 12
2.4.1 Campus card 12
2.4.2 Wachtwoorden (Eerste factor) 12
2.4.3 Tweede factor 12
2.4.4 TiU als identity provider 12
2.5 Andere account-types 13
2.6 Accounts in applicaties 13
2.7 Accounts in apparatuur 13
2.8 Archiveren en bewaren identiteitsgegevens 13
3 Toegangsbeheer 14
3.1 Algemeen 14
3.2 Bevoegdheden toekennen en intrekken (‘soll’) 14
3.3 Bevoegdheden en de levenscyclus 16
3.4 Bevoegdhedenbeheer in applicaties (‘soll naar ist’) 16
3.5 Autorisatiecommissie en IAM Poortwachters 17
4 Bewaking en bescherming 18
4.1 Logging 18
4.2 Attestatie door leidinggevenden 19
4.3 Beheer en controle rollenboek en autorisatiematrix 19
5 Gedocumenteerde uitzonderingen op dit beleid 19

1. Over het beleid Identiteiten & Toegang

1.1 Doel en reikwijdte

Dit document beschrijft de beleids- en bedrijfsregels die binnen Tilburg University (TiU) gelden voor processen en functionaliteiten die met identiteiten te maken hebben: wie ben je? Wat is je relatie met onze organisatie? – en met toegang: Wat mag je? En waarom mag je dat?

Het beleid in dit document is van toepassing op alle medewerkers, personen niet in loondienst (PNIL), studenten en gasten van Tilburg University en op situaties die verband hebben met werk of studie en/of activiteiten die plaatsvinden op de campus.

Binnen TiU streven we naar een integrale benadering van toegang tot informatie (logische toegang) en fysieke toegang. Daarom komen de regels voor beide terreinen samen in dit document.

Ondanks de omvang is het doel van dit document dat het in zijn geheel leesbaar en begrijpelijk is voor directeuren, leidinggevenden en informatiemanagers van de divisies en scholen en dat het door hen in de praktijk kan worden gedragen: het geeft immers de 'spelregels' die gelden voor onze bedrijfsprocessen.

1.2 Uitgangspunten

Bij de inrichting van het toegangs- en bevoegdhedenbeheer gelden deze principes:

i. **Regelgeving & standaarden zijn leidend**: onze processen en systemen voor identiteiten & toegangsbeheer zorgen ervoor dat wij structureel voldoen aan geldende wetten en regels, zoals ISO27001, AVG en het SURF Normenkader.

ii. **Geen toegang zonder registratie**: de identiteit van de persoon en de relatie met TiU wordt in een betrouwbaar proces gecontroleerd en vastgelegd.

iii. **Herleidbaarheid**: alle toegang is herleidbaar naar een natuurlijk persoon. Alle toegangsrechten zijn herleidbaar naar beleid en/of door een verantwoordelijk persoon, zoals een leidinggevende en/of proces- of systeemeigenaar, genomen beslissingen.

iv. **Veilig waar dat nodig is, vrijheid waar dat kan:** brede toegang maakt flexibel samenwerken mogelijk. We regelen de toegang daarom zoveel mogelijk op hoofdlijnen, waarbij wel geldt: hoe hoger het risico, hoe meer de toegang wordt beperkt.

v. We respecteren de verantwoordelijkheid van **specifieke belanghebbenden** zoals eigenaars/beheerders van bijzonder gevoelige informatiesystemen en ruimtes met specifieke beveiligingseisen.

vi. **Eenvoud, snelheid en voorspelbaarheid:** het toegangsbeheer wordt zó vormgegeven dat medewerkers, personen niet in loondienst, studenten en gasten snel worden voorzien

van de toegangsmiddelen die zij nodig hebben en dat dit gebeurt in een voor de leidinggevende begrijpelijk en voorspelbaar proces.

vii. **Financiële efficiëntie:** toegang tot faciliteiten is steeds vaker afhankelijk van persoonsgebonden licenties of licenties met maximale aantallen. Om de kosten voor TiU te beheersen wordt toegang tot dergelijke faciliteiten fijnmazig gefaciliteerd.

1.3 Gerelateerde normen en documenten

Dit beleid kan gedeeltelijk worden gezien als een invulling van een maatregel conform verbijzondering van het informatiebeveiligingsbeleid en gedeeltelijk als een uitbreiding daarop:

- Informatiebeveiligingsbeleid Tilburg University met de daarbij horende:
- Baseline Informatiebeveiliging

Ook het gebruikersreglement voor de faciliteiten van TiU en de gedragscode is in dit kader relevant:

- Gedragscode e-mail, internet en telefoonfaciliteiten Tilburg University
- Code of Conduct, met name “Omgaan met informatie”

Tevens raakt dit beleid aan de volgende reglementen van TiU:

- Regeling mandaat en volmacht Tilburg University;
- Bestuurs- en Beheersreglement;

TiU streeft naar een hoger volwassenheidsniveau op het gebied van identiteiten- en toegangsbeheer. Daartoe wordt het SURF Normenkader gebruikt om periodiek deze volwassenheid te toetsen:

- SURF Normenkader

Daarnaast zijn er beleidsstukken, die een nadere detaillering bevatten van aspecten, die voor dit beleid relevant zijn:

- Beleid verstrekking faciliteiten PNIL en Postactieven (april 2022);
- Toegangsbeleid TiU (fysiek en logisch voor niet-reguliere accounts).

1.4 Terminologie

Dit beleid voor identiteiten en toegang voor Tilburg University wordt ook aangeduid als het TiU IAM-beleid.

In dit beleid worden de volgende begrippen als volgt gedefinieerd en gebruikt:

- **Identificatie**

Het bekend maken van de identiteit van personen, organisaties of digitale voorzieningen. Dat kan in fysieke zin door gebruik van een identiteitsbewijs of certificaat. In de digitale wereld wordt hiervoor een digitale identiteit gebruikt, meestal in de vorm van een account of digitaal certificaat.

- **Authenticatie**
  De controle van een geclaimde (digitale) identiteit zodat kan worden aangetoond dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft. Authenticatie wordt ook wel aangeduid als: verificatie van de identiteit. Authenticatie gebeurt meestal op basis van iets dat alleen de gebruiker kan weten of tot zijn beschikking kan hebben.

- **Bevoegdheid**
  Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst en/of een bepaalde actie uit te voeren. Behalve voor publieke informatie en vrij toegankelijke diensten betekent dit dat de gebruiker de juiste bevoegdheden moet krijgen om werk of studie op de universiteit te kunnen uitvoeren. Een verdere detaillering van de generieke term bevoegdheid luidt als volgt:

  i. Een **rol** is een voor de organisatie betekenisvolle classificatie van personen en zegt iets over de relatie tussen de persoon en de organisatie.
  ii. Een **autorisatie** staat voor het recht op toegang naar een bepaalde ruimte, een bepaald systeem, bepaalde functionaliteit of informatie of het recht een bepaalde handeling uit te voeren. Een autorisatie wordt aangevraagd, toegekend en dan verstrekt (en uiteindelijk ingetrokken en dan afgenomen).
  iii. Autorisaties krijgen in een applicatie of systeem gestalte als **permissies**.

1.5 Levenscyclus van dit beleid

Dit beleid wordt vastgesteld door het College van Bestuur. De Chief Information Officer (CIO) en de systeemeigenaren zijn verantwoordelijk voor de uitvoering en naleving van maatregelen. Dit beleid is ook van toepassing op de diensten die door TiU worden verleend aan TIAS.

De Chief Information Security Officer (CISO) geeft gevraagd en ongevraagd advies over dit beleid en de naleving ervan.

Aansluitend op de beheercyclus van het informatiebeveiligingsbeleid zal het beleid identiteiten en toegang minimaal eenmaal per twee jaar geëvalueerd en zo nodig bijgesteld worden. Ook na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en door het CvB opnieuw vastgesteld.

2 Identiteitenbeheer

2.1 Soorten identiteiten

De universiteit verleent alleen toegang tot (een deel van) de fysieke en digitale voorzieningen van TiU aan geïdentificeerde, geauthentiseerde en geautoriseerde personen, die voor hun studie, werk of andere geldige reden deze toegang nodig hebben. Hierbij wordt onderscheid gemaakt tussen de volgende categorieën:

1. Medewerkers
   Onder 'medewerker' wordt in dit document verstaan iedereen, die door de personeelsadministratie van TiU wordt geregistreerd als zijnde in loondienst (PIL).

2. Personen niet in loondienst
   Hierbij kan onderscheid gemaakt worden tussen:
   a. Personen niet in loondienst (PNIL);
   b. Postactieven; deze categorie wordt vanaf het tweede kwartaal van 2022 uitgefaseerd en voortaan als PNIL geregistreerd.

   Afhankelijk van de registratie is het mogelijk om onderscheid te maken naar subgroepen binnen de categorieën PIL en PNIL.

3. Studenten
   Onder 'student' wordt in dit document verstaan iedereen, die onderwijs volgt aan de TiU en als zodanig geregistreerd staat in de Studentinformatiesystemen van de TiU. Hierbij kan onderscheid gemaakt worden tussen:
   a. Aanmelders;
   b. Studenten;
   c. Cursisten.

   Afhankelijk van de registratie is het mogelijk om onderscheid te maken naar subgroepen binnen deze categorieën.

4. Gasten
   Onder 'gast' wordt in dit document verstaan iedereen, die op uitnodiging en onder verantwoordelijkheid van een medewerker van de universiteit tijdelijk toegang krijgt tot specifieke digitale voorzieningen en is geregistreerd in een bronsysteem voor gasten. Hierbij kan onderscheid gemaakt worden tussen:
   a. Gasten algemeen;
   b. Gasten met alleen wifi-toegang;
   c. Gastleners, personen die alleen gebruik maken van de Bibliotheek voorziening en/of Brabant-Collectie.

5. TIAS-gebruikers
   Tilburg University verzorgt IT-diensten voor de TIAS School for Business & Society, de business school van Tilburg University en University of Technology Eindhoven. Het betreft

niet-bekostigd onderwijs. TIAS heeft een eigen bronsysteem, waarin onderscheid wordt gemaakt tussen de volgende typen gebruikers:

- Medewerkers in loondienst (PIL);
- Staf, externe docenten die op ZZP-basis onderwijs verzorgen (PNIL);
- Voltijd studenten;
- Deeltijd studenten, onder te verdelen in twee groepen:
  - Studenten die een NVAO geaccrediteerde opleiding volgen;
  - Studenten die een kortlopend programma volgen, niet geaccrediteerd.

6. Externen
   Onder 'externen' wordt in dit document verstaan iedereen, die niet in een van de andere categorieën voorkomt en dus niet in een van de bronsystemen van de TiU wordt geregistreerd. Hierbij kan onderscheid gemaakt worden tussen:
   a. Alumni van TiU;
   b. Studenten, docenten, onderzoekers of gasten, die toegang nodig hebben tot digitale voorzieningen van de TiU en die dat met een eigen (instellings)identiteit en -account krijgen.
   c. Medewerkers van externe partnerorganisaties, zoals leveranciers en beheerpartijen. Hierbij vertrouwen wij op het identiteitenbeheer van de betrokken organisatie.

2.2 Registratie van personen

2.2.1 Registratie van medewerkers en personen niet in loondienst

Personeel in loondienst (PIL) wordt geregistreerd[1] in het bronsysteem voor medewerkers, waarbij een kopie van een identiteitsbewijs wordt opgeslagen. Ook de datum in dienst en einddatum van de arbeidsovereenkomst worden vastgelegd. Als de einddatum van een arbeidsovereenkomst verandert (daaronder inbegrepen het opzeggen van een arbeidsovereenkomst van onbepaalde duur) is de leidinggevende verantwoordelijk voor de tijdige melding daarvan bij HR.

Personen niet in loondienst (PNIL) wordt geregistreerd[2] in het HR bronsysteem, waarbij een kopie van een identiteitsbewijs wordt opgevraagd, gecontroleerd, maar niet wordt opgeslagen. Ook de start- en einddatum van de overeenkomst worden vastgelegd. Als de einddatum verandert is de leidinggevende verantwoordelijk voor de tijdige melding daarvan bij HR.

Medewerkers en gastdocenten van TIAS worden door TIAS in hun bronsysteem geregistreerd.

2.2.2 Registratie van studenten

Deelnemers aan het reguliere onderwijs (bachelor, premaster, master) schrijven zich via Studielink in en komen zo in het bronsysteem voor studenten en worden als 'student' geregistreerd.

Deelnemers aan het niet-reguliere onderwijs worden via verschillende processen en systemen geregistreerd en vervolgens in de bronsystemen voor studenten opgenomen als 'cursist'.

[1] Conform de werkinstructies "Instructie Indiensttreding PIL", "Instructie Indiensttreding Student-assistenten" en "Instructie Indiensttreding Stagiairs" van HR.
[2] Conform de werkinstructie "Opvoeren PNIL" van HR.

Fulltime studenten en deelnemers of cursisten van TIAS worden door TIAS in hun bronsysteem geregistreerd.

Bij al deze gebruikers vindt verificatie van de identiteit plaats.

2.2.3 Registratie van gasten

2.2.3.1 Gasten algemeen

Het is mogelijk om gasten aan te melden bij IT Support, daarvoor is een Gastformulier beschikbaar om de benodigde gegevens aan te leveren. IT Support voert in de regel deze gasten op in het bronsysteem voor gasten, waarbij de aanmelder als verantwoordelijke wordt geregistreerd.

Ook bij dit type gebruiker vindt verificatie van de identiteit plaats.

N.B. Het is mogelijk om jezelf apart als gast te registreren voor de printer/scanner/kopieerapparaat. Deze registratie bevindt zich bij de leverancier van deze apparatuur en niet bij de universiteit. Gebruikers met een TiU-account kunnen hiermee inloggen op deze apparatuur.

2.2.3.2 Gasten met alleen wifi-toegang

Voor het verlenen van netwerktoegang aan gasten maken wij gebruik van eduroam Visitor Access (eVA); dit is een service die door SURF wordt aangeboden. EVA ondersteunt toegang voor gasten op uitnodiging van medewerkers van de TiU of via selfservice. Registratie van dit type gasten vindt rechtstreeks plaats in eVA waarbij de identificatie plaatsvindt op basis van sms-berichten en daarmee het mobiele nummer van de gast. In het geval dat een gast zich bij het gebruik van ons netwerk schuldig maakt aan het plegen van strafbare feiten kan justitie de identiteit van de gast achterhalen via de telecomprovider van de gast.

2.2.3.3 Gastleners

Net als reguliere gasten worden gastleners in het bronsysteem voor gasten geregistreerd. Zij krijgen echter een vooraf geproduceerde—op dat moment nog anonieme—Tilburg University card, waaraan later de gegevens van de gast worden gekoppeld door het identity management systeem.

Ook bij dit type gebruiker vindt verificatie van de identiteit plaats.

2.2.4 Registratie van TIAS-gebruikers

TIAS heeft een eigen CRM-systeem waarin alle gebruikers worden geregistreerd en dat geldt als bronsysteem voor de TiU.

Ook bij dit type gebruiker vindt verificatie van de identiteit plaats.

2.3 Digitale identiteit, TiU-account en basisrechten

2.3.1 Identiteit, Account en naamgeving

Op basis van de registratie in een van de bronsystemen wordt door het identity management systeem een digitale identiteit en een Tilburg University account aangemaakt. Er wordt per natuurlijk persoon één digitale identiteit en TiU-account aangemaakt. Komt een natuurlijk persoon meerdere keren voor in de bronsystemen, bijvoorbeeld zowel als medewerker als student, dan wordt een matching proces uitgevoerd om de brongegevens aan dezelfde digitale identiteit te

koppelen. Bij dit matching proces worden de match-kandidaten voorgelegd aan specifiek hiervoor aangewezen personen, die de match kunnen goedkeuren of besluiten dat er een nieuwe identiteit en account wordt aangemaakt.

Aan alle personen die een TiU-account krijgen wordt een administratienummer (ANR) toegekend. Het ANR is een 6-cijferig nummer waarmee een persoon uniek te identificeren is. Er wordt zoveel mogelijk getracht om terugkerende personen te voorzien van hun oude ANR. Het is mogelijk dat een persoon een nieuw ANR toegewezen krijgt, maar het ANR wordt nooit hergebruikt voor een andere persoon.

De naamgeving van accounts is gebaseerd op de naam van de persoon of op het ANR. De gebruikersnaam wordt in principe nooit gewijzigd, omdat dit consequenties heeft voor het profiel van een gebruiker in applicaties. Uitzonderingen worden aan de CIO voorgelegd voor goedkeuring.

N.B. Dit beleid voor identiteiten & toegang betreft de reguliere gebruikersaccounts. Andere soorten accounts, waaronder beheer-, test- en leveranciersaccounts, zijn het onderwerp van een verdiepend toegangsbeleid.

2.3.2 Basisrechten

Afhankelijk van het type gebruiker wordt een initiële set aan toegangsrechten aan het account toegekend en wordt bepaald of de gebruiker de beschikking krijgt over een campuscard.

In de TiU selfservice portal wordt het actuele overzicht van de basisrechten ("account-voorzieningen") gepubliceerd.

2.3.3 Instroom, doorstroom en uitstroom

Een TiU-account wordt bij **instroom** automatisch aangemaakt na registratie in een van de bronsystemen. Een account wordt initieel aangemaakt op het volgende moment:

- Medewerkers: zodra de nieuwe medewerker ingevoerd is in het bronsysteem én het contract is ondertekend;
- Personen niet in loondienst: zodra de nieuwe persoon ingevoerd is in het bronsysteem;
- Studenten: nadat een inschrijving voor een studie is gedaan en maximaal drie maanden voor de start van de studie;
- Gasten: zodra de opgegeven ingangsdatum bereikt is;
- TIAS: zodra de ingangsdatum van het contract/studie bereikt is.

Bij een mutatie van naamgegevens, afdeling en/of functie, of studie (**doorstroom**) in het bronsysteem worden het account en de basisrechten op de datum van ingang van de mutatie bijgewerkt. Voor medewerkers en personen niet in loondienst is de leidinggevende verantwoordelijk voor de tijdige doorgifte van mutaties aan HR.

Indien een gebruiker een aanvullende registratie krijgt van een ander type, dan wordt dat nieuwe type toegevoegd aan het account. Vanaf dit moment worden alle autorisaties (voorzieningen) uit alle toegewezen typen aan de persoon ter beschikking gesteld. Het is ook mogelijk dat er tussentijds een gebruikerstype eindigt. Op dat moment wordt toegang tot de voorzieningen van dat specifieke type van het account verwijderd volgens de uitstroom-procedure die per type tot het

intrekken van voorzieningen leidt. De voorzieningen die zijn toegekend vanuit andere typen blijven toegekend op het account.

Als een persoon geen relatie meer heeft met Tilburg University, dan wordt het account van de persoon beëindigd. De **uitstroom**-procedure start op het volgende moment:

- Medewerkers: zodra de einddatum van het contract is verstreken;
- Personen niet in loondienst: zodra de einddatum van de overeenkomst is verstreken;
- Studenten: zodra de einddatum van een studie verwerkt wordt of als een student op 1 oktober van het lopende academische jaar niet aan alle inschrijfvoorwaarden voldaan heeft;
- Gasten: zodra de einddatum van de gast-registratie verwerkt wordt;
- TIAS: zodra de einddatum van de relatie verwerkt wordt.

Voor het verwijderen van toegang tot faciliteiten geldt nog de volgende fasering:

- Op de einddatum:
  Toegang tot het account en de voorzieningen blijft nog intact.
- Na 32 dagen:
  Toegang tot het account en daardoor de voorzieningen wordt afgesloten.
- Tot 60/90 dagen:
  Indien het account opnieuw geactiveerd wordt: toegang tot email wordt hersteld. Na 60/90 dagen (afhankelijk van de emailprovider) is de hersteltermijn van e-mail verstreken.
- Tot 90 dagen:
  Indien het account opnieuw geactiveerd wordt: toegang tot het account en de voorzieningen wordt hersteld.
- Na 90 dagen:
  Accounts in de voorzieningen worden, zoveel mogelijk, opgeruimd.
  Het account zelf wordt opgeruimd. Voor applicaties, waarbij de accounts via automatische koppelingen met het identity management systeem worden aangemaakt, wordt het account ook automatisch weer opgeruimd. Voor andere applicaties is de functioneel beheerder verantwoordelijk voor het opschoningsproces, bijvoorbeeld op basis van de datum van laatste inlog.
  Uitzondering op deze termijn geldt voor het learning management systeem, waar accounts pas na twee jaar worden opgeruimd in verband met wettelijke verplichtingen.
- Tot 2 jaar:
  Indien de persoonsgegevens opnieuw ingevoerd worden en er matching plaatsvindt: Het ANR kan hergebruikt worden in een nieuw account.
- Na 2 jaar:
  Indien de persoonsgegevens opnieuw ingevoerd wordt een nieuw ANR gebruikt in een nieuw account, tenzij de persoon in het bronsysteem herkend wordt op basis van bewaarde gegevens.

Tenslotte is er nog een **noodknop**. Bij een arbeidsconflict, ontslag op staande voet, ernstige misdraging, etc. kan op initiatief van de directeur van de betreffende school of divisie de toegang van de gebruiker met onmiddellijke ingang worden geblokkeerd.

2.4 Authenticatiemiddelen

2.4.1 Campus card

De campuscard (Tilburg University card) kan door PIL, PNIL en studenten worden aangevraagd. De kaart wordt niet automatisch verstrekt. Na verlies of (op eigen verzoek) als de naam is veranderd, kan een vervangende kaart worden aangevraagd, nadat de oude kaart is geblokkeerd. De kaart is voorzien van foto, naam en student- of administratienummer[3].

Voorafgaand aan uitgifte wordt het identiteitsbewijs van de persoon gecontroleerd. Er vindt geen vastlegging plaats van deze controle.

Elke gebruiker beschikt altijd over precies één geldige kaart, ook als hij/zij meerdere aanstellingen, rollen of studies heeft.

De kaart is na datum uitdienst / einde studie geblokkeerd, zodat deze niet meer gebruikt kan worden voor toegang.

2.4.2 Wachtwoorden (Eerste factor)

Een gebruiker krijgt na registratie een e-mail met daarin de TiU-accountgegevens en een link naar een pagina om het wachtwoord in te stellen. Het wachtwoord dient te voldoen aan het wachtwoordbeleid (zie onder bij regels voor het wachtwoord).

De regels het wachtwoord, herstel, lock-out en dergelijke zijn in het Toegangsbeleid vastgelegd.

2.4.3 Tweede factor

De TiU hanteert als beleid dat het account met een tweede factor wordt beschermd. Dit houdt in dat bij de inlog op applicaties naast een wachtwoord een tweede authenticatiemiddel (een app of token) vereist is. Hiervoor geldt: tweede factor, tenzij, waarbij de CISO adviseert over de uitzonderingen op basis van een risicoanalyse.

Indien een gebruiker niet de beschikking heeft over de tweede factor, dan is een procedure ingericht voor de verstrekking van een tijdelijk middel. De tweede factor wordt dus niet uitgezet.

2.4.4 TiU als identity provider

Bij toegang naar applicaties wordt bij voorkeur gebruik gemaakt van *single sign-on* via de door TiU beheerde voorzieningen of via SURFconext, de nationale federatie voor middelbaar en hoger onderwijs en onderzoek. Daarbij loggen gebruikers in met de TiU-identiteit en authenticatiemiddelen die aan hen zijn verstrekt. De applicatie leidt de gebruiker eerst langs de TiU identity provider waar de gebruiker inlogt – in de regel met wachtwoord én een tweede factor. Daarna wordt de gebruiker voorzien van de juiste attributen (ten behoeve van autorisatie) teruggestuurd naar de applicatie.

Voor eduroam wordt gebruik gemaakt van RADIUS als identity provider voor TiU.

[3] Zie https://www.tilburguniversity.edu/nl/studenten/administratie/university-card.

2.5 Andere account-types

Naast reguliere TiU-gebruikersaccounts worden ook beheer-, service-, leveranciers-, en functionele accounts gebruikt binnen TiU. De regels hiervoor zijn beschreven in een apart Toegangsbeleid.

2.6 Accounts in applicaties

Een applicatie dient gebruik te maken van de centrale TiU authenticatievoorziening of TiU identity provider (zie 2.4.4) volgens het “pas toe of leg uit” principe.

Als een applicatie niet is aangesloten op het IAM-platform, dan dient de verantwoordelijke voor de applicatie ervoor zorg te dragen dat aansluiting bij het proces in-, door en uitstroom is gewaarborgd, met name dat accounts na uitdienst c.q. na einde contract tijdig worden geblokkeerd en verwijderd.

Is het gebruik van lokale accounts onvermijdelijk, dan beschrijft het Toegangsbeleid de regels voor dit type accounts.

2.7 Accounts in apparatuur

De regels voor lokale accounts in apparatuur, zoals netwerk-, telefonie, AV- en laboratoriumapparatuur zijn eveneens uitgewerkt in een apart Toegangsbeleid

2.8 Archiveren en bewaren identiteitsgegevens

De identiteitsgegevens worden na twee jaar uit het IAM-platform verwijderd. Doel van het bewaren van gegevens is het opnieuw kunnen uitgeven van het administratienummer, de gebruikersnaam en het e-mailadres indien een gebruiker binnen deze periode weer opnieuw wordt geregistreerd in een van de bronsystemen. Deze periode is kort genoeg om geen overbodige gegevens in het systeem te houden en lang genoeg om in de praktijk terugkerende gebruikers van hun oude account en e-mailadres te kunnen voorzien.

Voor aanleverende bronsystemen kunnen afwijkende regels gelden.

3 Toegangsbeheer

3.1 Algemeen

Dit hoofdstuk is van toepassing op het logische bevoegdhedenbeheer (toegang naar informatiesystemen) en ook op fysieke toegang (toegang naar ruimtes binnen de universiteit).

Zie voor de definities van bevoegdheid, rol, autorisatie en permissie in paragraaf 1.4.

Een **rol** bevat een of meerdere autorisaties; een **autorisatie** wordt in een systeem vertaald naar een of meerdere **permissies**.

Toekennen (c.q. *intrekken*) heeft betrekking op de beslissing om de bevoegdheid al dan niet te verstrekken; het is een administratief proces. Als meerdere partijen goedkeuring moeten geven is dit een onderdeel van het toekenningsproces.

Het *verstrekken* (c.q. *afnemen*) is daarentegen een operationele taak zonder beslissingselement: de beheerhandelingen die nodig zijn om toegekende bevoegdheden voor de betrokken gebruiker in te richten; deze kunnen deels geautomatiseerd zijn.

Anders gezegd, toekennen en intrekken heeft betrekking op de norm (de '**Soll**'). Verstrekken en afnemen hebben als doel de actuele situatie (de '**Ist**') in overeenstemming te brengen met de norm.

3.2 Bevoegdheden toekennen en intrekken ('soll')

Tilburg University kiest voor pragmatisch rolgebaseerd toegangsbeheer met vastlegging in de IAM-voorziening. Dit houdt in:

i. Aan elke gebruiker worden automatisch, op basis van arbeidsrelatie, afdeling en functie, of opleiding, één of meer rollen toegekend. Deze rollen variëren van organisatiebreed ('student') via algemene afdelings- of opleidingsrollen ('Tilburg Law School') tot zeer fijnmazig ('Functioneel beheerder LIS'). Zodoende kunnen rollen worden toegekend of afgenomen bij mutatie van de relatie, ook bij meerdere relaties.

    a. In elke rol zijn de relevante autorisaties naar verschillende systemen en ruimtes opgenomen.

ii. Aanvullend hierop kunnen op individuele basis aan gebruikers losse rollen en autorisaties worden toegekend op basis van een bepaalde relatie met de universiteit.

iii. Onder 'pragmatisch' wordt verstaan dat we niet proberen alle bevoegdheden met rollen toe te kennen maar accepteren dat de automatisch toegekende rollen gemiddeld circa 60-80% van het totale toegangsprofiel omvatten – en dat de rest alsnog afzonderlijk moet worden toegekend.

Automatisch toegekende rollen zijn beleid. Voor automatisch toegekende rollen geldt dat zowel de roldefinitie (welke bevoegdheden) als de roltoekenningsregels organisatiebreed zijn vastgesteld en periodiek worden herzien. Toegang die wordt verleend op basis van deze automatische rollen is daarmee gebaseerd op beleid, niet op een individuele beslissing.

De TiU Autorisatiecommissie is verantwoordelijk voor het beheer van deze rollenlogica en zorgt dat deze periodiek wordt herzien, goedgekeurd en gepubliceerd (zie paragraaf 3.5).

De toekenning van **individuele autorisaties**, naast het rollenmodel maar binnen de kaders die daarvoor gelden, is een **managementbeslissing**. De direct leidinggevende is verantwoordelijk voor alle individueel toegekende bevoegdheden van de medewerkers. De leidinggevende beslist over het toekennen en intrekken hiervan, eventueel na goedkeuring door proces- en/of autorisatie-eigenaar.

Een leidinggevende kan individuele bevoegdheden toekennen of intrekken met directe invoer in de IAM-voorziening of via een melding in het servicemanagementsysteem naar IT Support.

Aanvullend, niet beperkend. Autorisaties die worden toegekend als onderdeel van een automatische rol kunnen niet worden ingetrokken voor individuele medewerkers.

Herleidbaarheid. Elke autorisatie die een gebruiker heeft, kan worden herleid naar een beleidsbeslissing of naar de beslissing van een verantwoordelijk leidinggevende of proces- of autorisatie-eigenaar.

Autorisatie-eigenaar. Sommige autorisaties hebben een zodanig risicoprofiel dat behalve de leidinggevende ook de ‘eigenaar’ van de ruimte of gegevens bij de toegangsbeslissing moet worden betrokken. Hiervoor gelden als spelregels:

i. De autorisatie-eigenaar meldt zich bij de IAM Poortwachter (zie paragraaf 3.5) van zijn/haar organisatieonderdeel en wordt door IAM beheer in de IAM-voorziening als zodanig bij de autorisatie vastgelegd.
ii. De leidinggevende die de betrokken autorisatie op individuele basis wil toekennen aan een medewerker stemt dit vooraf met de autorisatie-eigenaar af.
iii. De autorisatie-eigenaar ontvangt een automatische notificatie zodra de autorisatie op individuele basis wordt toegekend. Hij/zij kan de autorisatie per direct intrekken door melding te doen bij de IAM Poortwachter.
iv. Als een autorisatie-eigenaar bezwaar heeft tegen de opname van een toegangsrecht of autorisatie in een automatisch toegekende rol kan hij/zij de roldefinitie door de Autorisatiecommissie laten aanpassen. Dat geldt dan voor iedereen die de rol heeft of krijgt.

3.3 Bevoegdheden en de levenscyclus

Automatische roltoekenning voor aankomende gebruikers vindt plaats op het moment van registratie zodra deze is doorgegeven aan de IAM-voorziening, zie ook paragraaf 2.3.3.

Bij doorstroom, dat wil zeggen: mutaties in de afdeling, functie of opleiding wordt het automatisch toegekende rollenpakket voor de betreffende relatie aangepast per de datum waarop de mutatie van kracht wordt.

Er is geen 'overlap', geen periode waarin de gebruiker de oude rechten houdt en de nieuwe rechten 'alvast' verwerft. Als dit nodig is voor bijvoorbeeld overdracht of voorbereiding kunnen aanvullende autorisaties op individuele basis worden toegekend – bij voorkeur direct met een einddatum.

Op de uitdienstdatum of einde opleiding worden alle automatisch toegekende rollen ingetrokken met in achtneming van de in paragraaf 2.3.3 genoemde termijnen.

Individueel toegekende rollen en autorisaties blijven van kracht tot de einddatum van die autorisaties (indien aangegeven) en anders tot 90 dagen na uit-dienst of einde opleiding, dat wil zeggen: op dezelfde datum als het TiU-account wordt verwijderd. Het merendeel van de herintreders binnen deze periode bestaat uit gebruikers wier contractverlenging of registratie (en betaling) voor een opleiding niet tijdig is verwerkt en op deze manier houden we de impact hiervan zo klein mogelijk. Indien een herintreder binnen deze periode een andere functie of opleiding heeft, dan is er (alsnog) sprake van doorstroom.

3.4 Bevoegdhedenbeheer in applicaties ('soll naar ist')

Elke autorisatie die kan worden toegekend heeft een naam en omschrijving die voor leidinggevenden beschrijft wat het doel en bereik is van de autorisatie. Deze definities worden in de IAM-voorziening bijgehouden door functioneel beheer IAM.

Permissies onderbrengen in autorisaties. De functioneel beheerder van de applicatie is verantwoordelijk voor de juiste afbeelding van 'logische' autorisaties in de IAM-voorziening op de 'technische' permissies of profielen in de applicatie.

Verstrekking van permissies. De functioneel beheerder is er ook verantwoordelijk voor dat de toekenning van autorisaties (zoals geregistreerd in de IAM-voorziening) in de applicatie leidt tot de juiste verstrekking van permissies.

Voor applicaties met een geautomatiseerde koppeling aan de IAM-voorziening betekent dit vooral: bewaken dat de koppeling op functioneel niveau naar behoren werkt.

Voor applicaties die met een werkorder-proces zijn gekoppeld aan de IAM-voorziening betekent dit: bewaken dat de feitelijke permissies kloppen met de toegekende autorisaties, bijvoorbeeld ondersteund door Soll/Ist-vergelijkingen uit IAM.

Voor **permissies die niet in autorisaties in de IAM-voorziening zijn ondergebracht** geldt dat de functioneel beheerder zelf verantwoordelijk is voor de registratie van het gehele proces van

toekennen, verstrekken, intrekken tot afnemen. Elke verstrekte permissie moet door de functioneel beheerder kunnen worden herleid naar de concrete beslissing van een verantwoordelijke.

In sommige applicaties —bijvoorbeeld in Sharepoint, Teams, Canvas— kan het beheer van permissies voor bepaalde datagebieden (teams, sites, groepen) worden gedelegeerd naar de eigenaar daarvan.

3.5 Autorisatiecommissie en IAM Poortwachters

Samenstelling. In de Autorisatiecommissie komen ten minste tweemaal per jaar universiteitsbreed de verschillende belanghebbenden bij het beheer van toegangsrechten samen:

	beleid en procedures	rollenmodel en autorisatiematrix	casuïstiek
vaste leden			
Eigenaar domein IAM (CIO)	V	optioneel	optioneel
Hoofd Internal audit & Compliance	V	V	V
Internal audit / Privacy Officer	optioneel	V	optioneel
Chief Info Security Officer (CISO)	V	optioneel	optioneel
Centrale IAM Poortwachter(s)	optioneel	V	optioneel
LIS / Processpecialist IAM	optioneel	optioneel	optioneel

Daarnaast, voorzover zij een belang hebben bij de agenda:

- van het betrokken organisatieonderdeel: de Privacy Officer, IAM Poortwachter(s) en/of Informatiemanager;
- betrokken afdelingshoofden, proceseigenaren en projectleiders;
- functioneel beheerders van betrokken systemen.

De Autorisatiecommissie heeft als **taken en mandaat**:

- **Beleid en procedures** rond autorisatiebeheer beoordelen en inhoudelijk goedkeuren, eventueel in aanloop naar formele vaststelling door CvB. Hierbij geldt het huidige document als kader.
- Het **rollenmodel** beoordelen en vaststellen. Dit omvat:
  - roldefinities: welke groepen kennen we, hoe herkennen we die?
  - roltoekenning: wie krijgt (automatisch of handmatig) welke rollen toegekend?
  - autorisaties: welke profielen zijn er, zijn deze herkenbaar voor de business?
  - autorisatiematrix: welke autorisaties kunnen per rol automatisch of aanvullend worden verstrekt?
  - functiescheiding: welke autorisaties mogen niet gecombineerd worden?

  De autorisatiecommissie richt zich op het niveau van rollen en autorisaties, die elk een voor de business herkenbare naam en omschrijving hebben. Correcte afbeelding van autorisaties op de systeemspecifieke permissies is een verantwoordelijkheid van de betrokken functioneel beheerders (zie 3.4).
- **Casuïstiek**. In sommige gevallen kunnen betrokken partijen het niet eens worden over de inrichting of definitie van rollen en autorisaties, is er onduidelijkheid wie is gemachtigd te

beslissen of is er behoefte aan een uitzondering op de gestelde regels en kaders. Zulke gevallen worden dan ter beoordeling en besluitvorming voorgelegd aan de commissie.

De 'V' in de tabel met de samenstelling van de commissie geeft aan welke leden aanwezig moeten zijn om op de gegeven onderdelen beslissingen te kunnen nemen.

De **IAM Poortwachters** zijn gezamenlijk verantwoordelijk voor het onderhoud van het rollenmodel, waarbij geldt:

- **toekenningsregels** vereisen de goedkeuring van de betrokken leidinggevenden en/of proceseigenaren;
- **rolautorisaties** en **autorisatiematrix** vereisen de goedkeuring van betrokken leiding-gevenden en/of proceseigenaren én de functioneel beheerders van de betrokken systemen;
- de IAM Poortwachters zijn verantwoordelijk voor **afbakening, naamgeving en documentatie** van rollen en autorisaties, op zo'n manier dat leidinggevenden en de Autorisatiecommissie daar beslissingen op kunnen baseren;
- nieuwe of gewijzigde rollen en autorisaties worden ten minste tweemaal per jaar aan de Autorisatiecommissie **ter vaststelling** voorgelegd; tot die tijd zijn de IAM Poortwachters verantwoordelijk voor de juistheid van de rollen en autorisaties.

4 Bewaking en bescherming

4.1 Logging

Per applicatie / per systeem. De applicatie-eigenaar is er verantwoordelijk voor dat de logging naar behoren wordt ingericht:

- logbestanden moeten worden gemaakt, bewaard en regelmatig worden beoordeeld conform de Baseline Informatiebeveiliging TiU[4];
- beveiligings- en beschikbaarheidsincidenten moeten achteraf kunnen worden geanalyseerd en herleid naar gegevens/functie, plaats, tijdstip en persoon (wie/wat/waar/wanneer);
- de toegang naar en de omgang met logs voldoet de Baseline Informatiebeveiliging TiU.

Systemen sluiten bij voorkeur aan op de SIEM-voorziening van de TiU; applicaties niet.

Bewaartermijnen. Logging van applicaties moeten gedurende een vastgestelde periode worden bewaard.

In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.

[4] Zie Baseline TiU definitieve Versie 1.0 d.d. oktober 2021.

4.2 Attestatie door leidinggevenden

Eén keer per jaar wordt door functioneel beheer IAM aan alle leidinggevenden gevraagd of gefaciliteerd om te controleren of de gegevens zoals deze in IAM bekend zijn correct en volledig zijn.

Deze attestatie omvat:

- klopt de lijst met medewerkers (PIL en PNIL) die aan de leidinggevende rapporteert?
- kloppen voor deze medewerkers de toegekende individuele autorisaties?

Als onderdeel van het attestatieproces wordt aan de leidinggevende ook inzicht geboden in automatisch toegekende rollen, zodat eventuele fouten in de roltoekenning kunnen worden gesignaleerd. Voor dit deel is de leidinggevende echter niet primair verantwoordelijk.

Voor de attestatie van beheeraccounts, zie het aparte Toegangsbeleid.

4.3 Beheer en controle rollenboek en autorisatiematrix

Twee keer per jaar voert de (door de) Autorisatiecommissie (aangewezen medewerker) steekproefsgewijs een Ist/Soll controle uit op het rollenboek en de autorisatiematrix:

- zijn de feitelijke autorisaties van de geselecteerde medewerkers in lijn met de matrix?
- klopt voor de gekozen medewerkers de vertaling van IAM rollen naar autorisaties (toegang tot applicaties)?
- waar van de matrix is afgeweken, kunnen deze afwijkingen worden verklaard door eerdere beslissingen van de Autorisatiecommissie?

5 Gedocumenteerde uitzonderingen op dit beleid

Dit laatste hoofdstuk beschrijft kort de bekende uitzonderingen op dit beleid. Dit beleid beschrijft immers de gewenste spelregels in het IAM-domein en deze kunnen nog geen staande praktijk zijn.

- Ad paragraaf 2.3.1: Het account dat voor ieder persoon wordt aangemaakt betreft in beginsel een Microsoft Active Directory (AD) account. Tot nader order wordt geaccepteerd dat ook in OpenLDAP dit account wordt opgenomen.
- Ad paragraaf 2.2: Niet altijd vindt identiteitscontrole plaats bij registratie.
- Ad paragraaf 2.2.3.1: De aanmelder wordt niet als verantwoordelijke bij de registratie van gasten geregistreerd, maar degene van IT Support die de registratie verzorgt.
- Ad paragraaf 2.6: Niet alle applicaties maken gebruik van het TiU-account; er zijn er nog met een eigen account: o.a. Planon, SAP, Business Objects en xFlow.
- Diverse paragrafen: Nog op te stellen is het Toegangsbeleid voor niet-reguliere TiU-gebruikersaccounts.