



FB TOB KD

Kader Toegangsbeheer Amsterdam UMC

Dit document beschrijft op hoofdlijnen de uitgangspunten, doelstellingen en kaders voor Toegangsbeheer voor alle bedrijfsonderdelen en objecten van Amsterdam UMC.

Autorisatie	Naam	Paraaf
Auteur	Arjen Appelman Aissam el Khamsi Rob Jansen Elliz Slootweg	Goedkeuringsflow en wijzigingen worden beheerd in K2
Eigenaar	Hoofd SRM Aissam el Khamsi	
Vaststeller	Clustermanager Services & Veiligheid Stijn van Roosendaal Directeur Facilitaire Dienst Leo de Haan	
Datum revisie:	5 jaar na vaststelling	
Beheer	Versie	
K2: 080699	3.5 - 20-06-2026	

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Inhoudsopgave

Inhoudsopgave	2
1. Inleiding Toegangsbeheer Amsterdam UMC	3
1.1. Inleiding	3
1.2. Inrichting maatregelen Toegangsbeheer binnen SMS Amsterdam UMC	3
1.3. Verantwoordelijkheden	3
1.3.1 Eigenaarschap	4
1.3.2 Beheer	4
2. Uitgangspunten, doelstellingen en bewaartermijnen	5
2.1 Uitgangspunten	5
2.2 Doelstellingen	6
2.3 Bewaartermijnen	6
3. Architectuur en autorisatiemanagement	7
3.1 Architectuur autorisatiemanagement Toegangsbeheer	7
3.2 Architectuur meldkamer	7
3.2.1 Architectuur meldkamer AMC	8
3.2.2 Architectuur meldkamer VUmc	8
3.3 Autorisatieprincipes Toegangsbeheer	8
3.4 Positionering autorisatiemanagement	9
4. Toegangs niveaus, kleurenmethodiek en spelregels	10
4.1 Toegangs niveaus en kleurenmethodiek	10
4.2 Spelregels zonering	10
5. Toegang, toegangspassen, sleutels	12
5.1 Toegang tot en binnen gebouwen en niet publieke ruimten Amsterdam UMC	12
5.2 Pashouders en Amsterdam UMC-passen	12
5.3 Sleutels, sluitplannen en procedures	13
5.4 Processen en werkinstructies voor passen en sleutels	13
6. Inzet techniek en meldkamer	14
6.1 Inzet techniek	14
6.2 Sluittechnieken	14
6.3 Implementatie van techniek	15
6.4 Relatie naar meldkamer	15
6.5 Meldkamersystemen	15
7. Toezicht, handhaving, calamiteiten en borging	17
7.1 Toezicht en handhaving	17
7.2 Calamiteiten en crisissituatie	17
7.3 Borging Toegangsbeheer	17
Bijlage 1 Overzicht toegangsbeheer binnen SMS Amsterdam UMC	19
Bijlage 2 Overzicht systemen en beheer Toegangsbeheer Amsterdam UMC	20
Bijlage 5 Toezicht op radioactieve stoffen Amsterdam UMC	21
Bijlage 4 Overzicht wet- en regelgeving	23
Bijlage 5 Overzichten toe te passen sluittechnieken	24

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

1. Inleiding Toegangsbeheer Amsterdam UMC

1.1. Inleiding

De missie en ambitie van Amsterdam UMC is om samen de zorg van morgen te ontdekken. We zijn gericht op het verdiepen, verbreden en verspreiden van onze kennis. Kennis is de onverwoestbare basis van onze zorg en ons onderwijs. We leiden mensen op en met elkaar ontdekken we wat het menselijk lichaam verbergt. Om al onze taken op het hoogste niveau blijvend uit te voeren moeten we ze beschermen met respect voor ieders privacy. Daarvoor treffen we maatregelen waaronder die waarmee we het toegangsbeheer inrichten. Dit kader beschrijft de uitgangspunten, doelstellingen en spelregels voor toegangsbeheer binnen Amsterdam UMC (hierna Amsterdam UMC) voor de komende 5 jaar. Nog niet alle beschreven kaders zijn in 2025 geïmplementeerd, voor implementatie is de hele beleidsperiode nodig.

Definitie Toegangsbeheer Amsterdam UMC:

Het geheel van maatregelen (systemen, processen, beveiligingsplannen, beheer en onderhoud) dat er blijvend voor zorgt dat onbevoegden geen fysieke toegang hebben tot besloten Amsterdam UMC gebieden en ruimten en bevoegden/ geautoriseerden daar kunnen komen waar zij uit hoofde van de functie/ uit te voeren werkzaamheden/ gemaakte afspraken toegang moeten hebben.

Met toegangsbeheer beschermt Amsterdam UMC personen, bedrijfsprocessen, materialen en informatie tegen ontvreemding, sabotage, vernieling, verwonding of anderszins. Fysiek toegangsbeheer maakt geen onderscheid tussen divisies, afdelingen en locaties; door één manier van werken en op een gelijk niveau, afgezet tegen de daar aanwezige risico's, worden uniforme maatregelen getroffen waarbij verschillende systemen worden ingezet. Uniform toegangsbeheer voorkomt incidenten, beperkt de impact van incidenten en draagt zo bij aan betaalbare zorg.

Toegangsbeheer richt zich op het beheer van de fysieke toegang tot ruimten binnen Amsterdam UMC en is belegd binnen de Facilitaire Dienst.

De toewijzing van ruimten wordt gecentraliseerd uitgevoerd door dienst Huisvesting Vastgoed & Techniek (HV&T) op basis van het LTHP Bestemmingsplan Kantoren en het Masterplan Gebouwen. Ad hoc ruimten aanvragen worden beoordeeld door de [Commissie Huisvesting](#).

1.2. Inrichting maatregelen Toegangsbeheer binnen SMS Amsterdam UMC

Toegangsbeheer is één van de maatregelen binnen het Beveiligingsbeleid Amsterdam UMC. Voor fysieke beveiliging maakt Amsterdam UMC gebruik van een Security Management Systeem (SMS), zie [bijlage 1](#) die de structuur van documenten weergeeft. Dit systeem wordt aankomende jaren gevuld waarmee een geharmoniseerd framework voor fysieke beveiliging ontstaat.

Het Kader Toegangsbeheer is het kapstokdocument en beschrijft maatregelen op hoofdlijnen en geldt voor de toegang tot en binnen alle locaties van Amsterdam UMC. De toe te passen maatregelen zoals toegangssystemen, camera's, gebruik van sleutels en buitenbeveiliging (hekken, poorten, slagbomen) zijn nader uitgewerkt in verplichte standaarden/ specifieke technische bepalingen. Met de inhoud uit het kader en de standaarden is het mogelijk beveiligingsplannen per locatie, bouwdeel, etage, afdeling in te richten. Toegangsbeheer kent daarnaast uniforme werkprocessen en werkinstructies; deze beschrijven op 'één manier van samenwerken' hoe maatregelen te gebruiken en beheren. Alle documenten zijn eenduidig gecodeerd en beheerd en binnen K2 gepubliceerd.

1.3. Verantwoordelijkheden

De verantwoordelijkheden en het eigenaarschap voor Toegangsbeheer is bij meerdere diensten en afdelingen binnen Amsterdam UMC belegd. Alleen met heldere afspraken, een centrale focus

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

op het Amsterdam UMC belang en één manier van afstemming en samenwerken (ook met derden) is Toegangsbeheer succesvol te implementeren. Hieronder is het eigenaarschap en zijn de verantwoordelijkheden en taken beschreven:

1.3.1 EIGENAARSCHAP

Functioneel eigenaar: Facilitaire Dienst / Cluster Services & Veiligheid / SRM

- SRM is verantwoordelijk voor de mix van in te zetten systemen en de daarbij behorende functionaliteiten om zodoende fysieke beveiligingsrisico's beheersbaar te maken.
- FD financiert de taakuitvoering (fte) die nodig is om het functionele eigenaarschap efficiënt en effectief uit te voeren.

Technisch eigenaar: Dienst Huisvesting, Vastgoed & Techniek (HVT)

- HVT is verantwoordelijk voor de eerste installatie, uitbreidingen en het onderhoud van systemen (inclusief benodigde software). Binnen HVT bestaan de afdelingen Projecten (nieuwbouw en verbouwingen) en Onderhoud beheer en energie (OB&E).

1.3.2 BEHEER

Functioneel (Applicatie) Beheer (FB en FAB): Facilitaire Dienst / Cluster Services & Veiligheid en Staf & Projecten

- SRM (Cluster S&V) is verantwoordelijk voor het Functioneel Beheer: de inrichting van systemen op papier. Deze inrichting wordt afgestemd met belanghebbenden (bijvoorbeeld afdelingshoofden) en vastgelegd in brondocumenten per systeem.
- FAB (Cluster S&P) is verantwoordelijk voor het Functioneel Applicatie Beheer: de configuratie van de systemen op basis van de input uit de brondocumenten. FAB stemt af met Technisch Applicatie Beheer (DICT) en FB en heeft een rol bij te maken keuzes voor updates, upgrades en nieuwe systemen. FAB is tevens verantwoordelijk voor het oplossen van tweede lijns softwarematige storingen.

Technisch Applicatie Beheer (TAB): DICT / Applicatiediensten

- Applicatiediensten is verantwoordelijk voor het TAB: de ICT voorzieningen (servers, netwerken, clients) om systemen te kunnen laten draaien, de koppelingen tussen systemen en de uitvoering van updates en upgrades. Deze taken worden afgestemd met de FD en HVT.

Technisch Beheer (TB): Dienst Huisvesting, Vastgoed & Techniek

- HVT is verantwoordelijk voor de aanleg van de benodigde infra voorzieningen (spanning, data, koppelingen met brandsystemen, sturingen) daar waar componenten van systemen worden aangebracht. Naast de aanleg is HVT verantwoordelijk voor het ontvangen, registreren en oplossen van technische storingen.

Operationeel beheer (OB): Facilitaire Dienst / Cluster Services & Veiligheid

- Afdeling Beveiliging is verantwoordelijk voor het werken met de systemen: het monitoren en bedienen van systemen vanuit de meldkamer en op locatie (bijvoorbeeld bijvullen van de uitrijkaarten van het parkeerbeheersysteem).
- Services FD is verantwoordelijk voor het uitgeven van passen en het beantwoorden en oplossen van vragen en eerste lijn storingen.
- SRM is verantwoordelijk voor het uitgeven en registreren van sleutels.

Voor een overzicht van de verschillende beheertaken over de verschillende systemen die tot de scope van toegangsbeheer behoren zie [bijlage 2](#).

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

2. Uitgangspunten, doelstellingen en bewaartermijnen

2.1 Uitgangspunten

- Amsterdam UMC houdt zich aan de geldende wet- en regelgeving (zie [bijlage 3](#) voor overzicht);
- Het Amsterdam UMC heeft een openbaar karakter, echter, gebouwen zijn niet voor iedereen altijd toegankelijk;
- Alle internen en externen hebben een taak en verantwoordelijkheid voor wat betreft het beschermen van eigendommen van Amsterdam UMC;
- Op het gebruik van de gebouwen, ruimten en voorzieningen is voor medewerkers een gedragscode van toepassing voor bezoekers, patiënten, studenten en externen zijn huisregels van kracht;
- Gebouwen, afdelingen, ruimten en voorzieningen zijn toegankelijk op die dagen en tijdstippen dat de afdeling/ ruimte in bedrijf is en biedt slechts toegang aan die personen die voor een afspraak of de uit te voeren werkzaamheden toegang moeten hebben;
- Toegangsmogelijkheden worden alleen gebruikt voor het doel waarvoor ze aanwezig zijn. Denk aan nooduitgangen, MIVA en transport/expeditie toegangen en doorgangen;
- Ongeautoriseerde toegang wordt zoveel mogelijk voorkomen en geautoriseerde toegang wordt zo makkelijk mogelijk gemaakt, rekening houdend met de risico's en technische mogelijkheden;
- Van iedereen die over een Amsterdam UMC toegangsmiddel beschikt is de identiteit geverifieerd;
- Amsterdam UMC pashouders dragen de Amsterdam UMC-pas zichtbaar, de Amsterdam UMC-pas is het interne legitimatiemiddel;
- (Brand)veiligheid prevaleert boven de security-eisen die Amsterdam UMC stelt;
- Alle internen en externen zijn op de hoogte van de toepassing zijnde calamiteitenprotocollen;
- Bij calamiteiten kan de toegang voor specifieke groepen worden verruimd (calamiteitenteam) of juist beperkt (lock down scenario);
- Bij (het vermoeden van) strafbare feiten heeft Amsterdam UMC de mogelijkheid om logbestanden (waaronder camerabeelden en het pasgebruik indien beschikbaar) uit beveiligingssystemen te raadplegen;
- Van strafbare feiten kan aangifte worden gedaan;
- Amsterdam UMC is nimmer aansprakelijk voor verlies of diefstal van privé-eigendommen.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

2.2 Doelstellingen

De missie en ambitie van Amsterdam UMC is om samen de zorg van morgen te ontdekken. Dit doen we samen en in een veilige omgeving:

- We bieden medewerkers, studenten, patiënten, bezoekers, externen en huurders een veilige en aangename werk- en verblijfsomgeving;
- We voorkomen of beperken de impact van incidenten op terreinen en binnen gebouwen van Amsterdam UMC. Hierbij gaat om het vermijden van risico's als:
 - Agressie & Geweld;
 - Brandstichting;
 - Ongewenste/ onbedoelde binnendringing;
 - Ontvreemdingen (zoals diefstal met of zonder braak);
 - Overlast;
 - Vernielingen waaronder ook graffiti;
- We configureren en koppelen de beveiligingssystemen zo dat functionaliteiten maximaal benut worden;
- We richten het beheer van systemen zo eenvoudig mogelijk in en automatiseren zoveel als mogelijk door gebruik te maken van een doelmatige en flexibele systeemarchitectuur;
- We passen in beginsel zo min als mogelijk verschillende systemen toe waarbij grote afhankelijkheid (vendor locks) zoveel als mogelijk wordt voorkomen.

2.3 Bewaartermijnen

De systemen die onder toegangsbeheer vallen, zie hoofdstuk 3 en 6, kunnen persoonsgegevens bevatten. Deze persoonsgegevens kunnen bestaan uit de basisgegevens van de pashouders, de 'pashouder registratie' datgene wat de pashouder met haar/ zijn pas heeft gedaan binnen het systeem, de 'eventlog', en datgene wat systeemgebruikers (de users/ beheerders van de applicatie) hebben gedaan binnen het systeem, de 'userslog'. Voor deze drie gelden verschillende bewaartermijnen. Hieronder zijn de kaders hiervoor opgenomen:

- Pashouder registratie: 14 maanden;
- Eventlog: 24 maanden;
- Userslog: 24 maanden.

Voor specifieke systemen/ toepassingen kunnen afwijkende bewaartermijnen gelden:

- Beeldopslag: 28 dagen (zie ook kaderdocumenten Cameratoezicht).

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

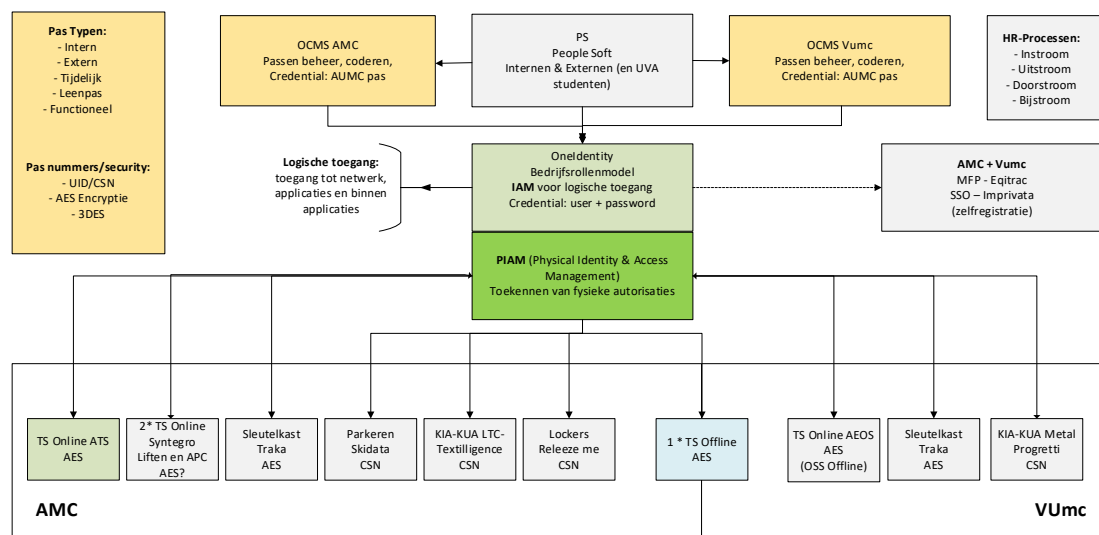
3. Architectuur en autorisatiemanagement

In dit hoofdstuk worden de architectuur en autorisatieprincipes voor toegangsbeheer beschreven. In dit kader is de gewenste doelarchitectuur beschreven. Er zijn 2 architecturen opgenomen:

1. De architectuur Toegangsbeheer: alle systemen die gegevens delen en de Amsterdam UMC-pas als toegangsmiddel/ credential gebruiken
2. De architectuur voor de meldkamers: alle systemen die gemonitord en bediend worden vanuit de 2 meldkamers voor beveiliging (locatie VUmc en AMC)

3.1 Architectuur autorisatiemanagement Toegangsbeheer

De architectuur voor toegangsbeheer bestaat uit alle systemen die de Amsterdam UMC-pas als credential gebruiken. Het gaat om die systemen die persoons- en of pasgegevens bevatten en waar autorisaties worden toegekend. Deze autorisaties vinden plaats op basis van gegevens uit de bovenliggende bronsystemen (PeopleSoft en Onelidentity). In deze architectuur gaat het om meer systemen dan de beveiligingssysteem alleen. Het eigenaarschap voor deze aanpalende systemen ligt bij andere diensten.



Toelichting architectuur:

Peoplesoft staat bovenin centraal als HR-systeem. Dit is de bron voor alle personen/identiteiten die binnen Amsterdam UMC-activiteiten verrichten. Voor locatie AMC en VUmc worden deze verrijkt met pasnummers (zie de twee OCMS applicaties in lichtoranje (oranje aangezien deze nog geharmoniseerd moeten worden)). Peoplesoft levert persoonsgegevens en overige gegevens aan One-Identity (OI), verrijkt met de pasgegevens vanuit OCMS aan de IAM-applicatie binnen Amsterdam UMC (OI in lichtgroen, wordt momenteel geharmoniseerd). One-Identity Manager (OIM) is de module binnen OI waarbinnen autorisaties worden beheerd en aanvraag- en goedkeuringsprocessen worden ingericht. Physical Identity & Access Management (PIAM) wordt binnen OIM ingericht (donkergroen, in 2025 op te starten). Middels PIAM worden alle daaronder gelegen applicaties gevoed met de strikt noodzakelijke (privacy by design) persoonsgegevens, pasgegevens en autorisaties. ATS in lichtgroen, upgrade systeemcomponenten is lopend project, TS offline in lichtblauw: wens, nog niet bestaand op locatie AMC.

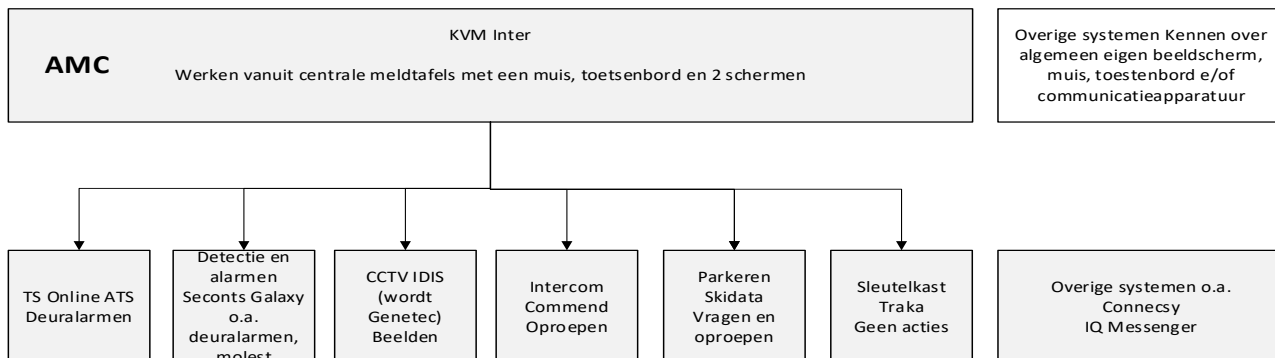
3.2 Architectuur meldkamer

De tweede architectuur bevat de systemen die uitkomen in de meldkamer en hier gemonitord en bediend worden door de afdeling Beveiliging. Niet alle systemen zijn in de architectuur opgenomen i.v.m. de overzichtelijkheid. In een separaat plan voor de meldkamers wordt hier meer uitgebreid op ingegaan. Alle systemen zijn functioneel en technisch eigendom van de FD

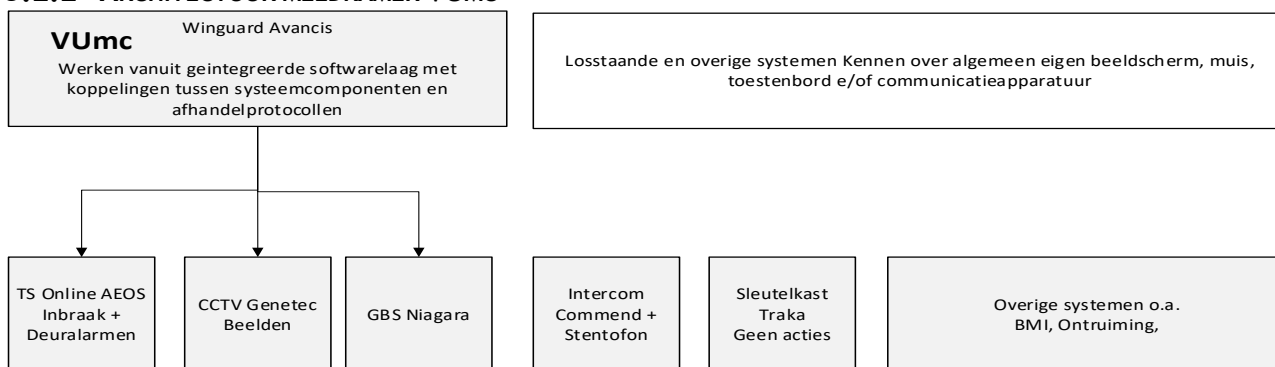
Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

en DHVT. Amsterdam UMC kent twee meldkamers die nog gescheiden opereren. Hierdoor zijn er twee architecturen. De komende jaren worden de meldkamers geharmoniseerd zodat er meer uniform gewerkt kan worden.

3.2.1 ARCHITECTUUR MELDKAMER AMC



3.2.2 ARCHITECTUUR MELDKAMER VUMC



3.3 Autorisatieprincipes Toegangsbeheer

Binnen toegangssystemen is ingesteld welke functiegroepen (niet op persoonsniveau) waar naar binnen mogen. Dit wordt binnen toegangssystemen geconfigureerd als toegangsprofielen. Toegangsprofielen worden samen met divisies, diensten en afdelingen vastgesteld. Binnen Amsterdam UMC worden verschillende typen toegangsprofielen onderscheiden die zijn afgestemd op het risico dat zij vertegenwoordigen:

1. Basisprofielen: bevatten laag risico deuren (veelal algemene buiten- en binnendeuren) en worden aan veel pashouders automatisch toegekend op basis van een rol (intern, extern, huurder, student);
2. Divisie & diensten profielen: bevatten algemene deuren die toebehoren aan divisies, diensten, logistieke gebieden. Deze worden automatisch toegekend aan pashouders op basis van een organisatie- of locatiecode;
3. Bedrijfsrollen profielen: bevatten specifieke deuren die toebehoren aan afdelingen en/of groepen van medewerkers, bedrijfsrollen, binnen afdelingen. Deze worden automatisch toegekend aan pashouders op basis van een afdelings- of functiecode of bedrijfsrol;
4. Vitale profielen bevatten de toegang tot een vitale ruimte die toebehoort aan een afdeling;
5. Generale profielen: bevatten heel veel toegangen op een of meerdere locaties bedoeld voor de calamiteitenbestrijding.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

De eerste drie typen profielen worden automatisch toegekend doordat systemen gekoppeld zijn (zie architectuur uit 3.1). Profieltypen 4 en 5 worden bewust handmatig toegekend vanwege het hogere risico. Profielen kunnen voorzien zijn van een dag/tijd zone waardoor toegekende autorisaties op deuren niet altijd werken. Naast de profieltypen 4 en 5 kan er bij de profieltypen 2 en 3 sprake zijn van tijdelijke toekenningen. Dit wanneer een persoon tijdelijk op een andere afdeling werkt of moet zijn. Voor alle handmatige toekenningen zijn aanvraag- en goedkeuringsprocessen beschikbaar en/of worden ontwikkeld.

Door veel autorisaties bij de HR-processen Instroom, Doorstroom, Bijstroom en Uitstroom te automatiseren is Amsterdam UMC in Control. Op deze wijze worden te ruime en onjuiste autorisaties zoveel als mogelijk voorkomen. Het opstellen, vaststellen en inrichten van toegangsprofielen komt tot stand door overleg tussen de functionele beheerders, de functionele applicatie beheerders en de gebiedsbeheerders (afdelingshoofden en gedelegeerden).

3.4 Positionering autorisatiemanagement

Het beheer van de toegangssystemen volgt de opbouw van de architectuur in 3.1. Het geautomatiseerd koppelen van toegangsrechten/ autorisaties aan pashouders waarvan de identiteit geverifieerd is, heet PIAM. Dit wordt zo hoog mogelijk binnen de architectuur belegd bij One-Identity Manager (OIM) omdat dit de meeste beheervoordelen kent:

- Een plek voor gecombineerd beheer van IAM en PIAM;
- Een beheer organisatie;
- Auditeerbaarheid vanuit 1 applicatie;
- Een loket voor aanvragers van tijdelijke en hoog-risico profielen;
- Meest eenvoudige migratiepad naar gewenste doelarchitectuur.

De opbouw van toegangsprofielen, die nodig zijn om pashouders te kunnen autoriseren, vindt plaats in de afzonderlijke applicaties aan de onderzijde van de architectuur. Hiervoor zijn de functionele applicatie-eigenaren verantwoordelijk. Het beheer van de PIAM-autorisatiematrix; wie heeft op basis van zijn rol en werkplek welke toegangsautorisaties nodig, vindt plaats binnen OIM en valt onder de verantwoordelijkheid van de FD (gedelegeerd beheer vanuit OIM).

Tot het PIAM beheer hoort het opstellen en bijhouden van de PIAM-autorisatiematrix en het opstellen en beheren van alle aanvraag- en goedkeuringsprocessen.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

4. Toegangs niveaus, kleurenmethodiek en spelregels

4.1 Toegangs niveaus en kleurenmethodiek

Op basis van aanwezige risico's, locatie en gebruik worden binnen de Amsterdam UMC verschillende toegangs niveaus met elk een eigen kleur onderscheiden. Middels de kleuren zijn plattegronden van locaties te zoneren en maatregelen toe te kennen op zone-overgangen. Binnen Amsterdam UMC worden de volgende toegangs niveau 's ofwel zones onderscheiden die kunnen voorkomen:

- Groen-** **Publiek gebied** - vrij toegankelijk voor iedereen. Geen toegangsmiddel nodig. Groen kan zowel binnen als buiten (publieke parkeerterreinen) voorkomen.
- Blauw-** **Beperkt publiek gebied** - toegankelijk voor iedereen met een doel, afspraak of toegangsmiddel. Hiertoe horen de klinieken en poliklinieken. Blauw kan zowel binnen als buiten voorkomen (denk aan parkeren voor dialyse patiënten).
- Rood-** **Medewerkers ruimten** - toegankelijk voor geautoriseerden die beschikken over een toegangsmiddel van Amsterdam UMC. Rood komt alleen binnen voor.
- Paars-** **Vitale ruimten** - hoog risico ruimten alleen toegankelijk voor internen en externen die uit hoofde van de functie in deze ruimten aanwezig moeten zijn. Deze ruimten kennen een beperkt toegangsregime en zijn zwaarder beveiligd dan andere ruimten. Paars komt alleen binnen voor.

Voor buitenruimten geldt aanvullend:

- Oranje-** **Beveiligd buitenterrein** - toegankelijk voor geautoriseerden die beschikken over een toegangsmiddel van Amsterdam UMC. Denk aan expeditieruimten, opslag goederen buiten, buitenterrein energiecentrale, opslag (brandbaar) vuil.
- Wit-** **Openbare ruimte** - Onbeveiligd gebied; toegankelijk voor iedereen, openbare weg/ruimte die grenst aan Amsterdam UMC gebouwen en terreinen.

Voor huurders geldt:

- Geel-** **Verhuurde ruimten** - huurder gebruikt eigen toegangsmiddel of toegangsmiddel van Amsterdam UMC. Huurders kunnen contractueel verplicht zijn aan te sluiten bij beveiligingsmaatregelen en calamiteitenprocedures van Amsterdam UMC.

4.2 Spelregels zonering

Per gebouw, bouwdeel en etage kunnen één of meer verschillende zones voorkomen. **De bij 4.1** genoemde toegangs niveaus/ zones worden geprojecteerd op plattegronden van locaties van Amsterdam UMC. Dit is de basis van beveiligingsplannen per bouwdeel, etage of afdeling, waarbij op zone overgangen maatregelen worden ingezet.

Binnen zones (bijvoorbeeld rode zone) kunnen meerdere afdelingen gehuisvest zijn. De verschillen in toegang worden dan gerealiseerd door verschillende autorisaties toe te kennen. Gebiedsbeheerders zijn samen met SRM verantwoordelijk voor het samenstellen van de juiste toegangsprofielen voor de afdelingen en voor het toekennen van de juiste autorisaties.

Voor de positionering van paarse ruimten binnen locaties geldt dat deze bij voorkeur alleen aan rode zones grenzen. Indien dit niet mogelijk is wordt de zone-overgang verzaamd uitgevoerd.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Zones (gebieden) worden gevisualiseerd bij de toegangen op een wijze dat de teksten zijn afgestemd op de publieksfunctie die Amsterdam UMC kent. Teksten zijn positief verwoord; zo wordt aangegeven wie toegang heeft en niet voor wie de toegang verboden is.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

5. Toegang, toegangspassen, sleutels

5.1 Toegang tot en binnen gebouwen en niet publieke ruimten Amsterdam UMC

Er worden verschillende vormen van toegang binnen Amsterdam UMC onderscheiden:

- Reguliere toegang voor publiek: iedereen zonder toegangsmiddel heeft toegang tot publieke ruimten (groene gebieden) tijdens reguliere openingstijden en tot zorggebieden (blauwe gebieden) als men een afspraak heeft, opgenomen is of op bezoek komt. Voor bezoekers in blauwe gebieden gelden vastgestelde bezoektijden;
- De meeste locaties beschikken over meerdere toegangsmogelijkheden, te weten de algemene publiektoegangen, toegankelijk voor iedereen. Voor specifieke afdelingen kunnen specifieke publiektoegangen voorzien zijn. Deze geven toegang tot blauwe zones en ruimten en zijn alleen toegankelijk voor personen die hier een doel of afspraak hebben. Afhankelijk van het tijdstip op de dag kunnen meer of minder algemene en specifieke publiektoegangen toegankelijk zijn.
- Reguliere toegang voor geautoriseerden: iedereen die in het bezit is van een geautoriseerd toegangsmiddel heeft toegang tot die ruimten die binnen de autorisatie passen. Er kunnen dag/tijdzones zijn ingesteld voor toegang waarbij geautoriseerden geen 24 uren toegang hebben.
- Toegang op afstand, bijvoorbeeld toegang voor leveranciers, patiënten en bezoekers (buiten reguliere openingstijden) en toegang voor geautoriseerden (buiten ingestelde dag/tijdzones). Toegang wordt verkregen via een intercom die in verbinding staat met de meldkamer en/of recepties op locaties.
- Toegang bij calamiteiten. In het geval van calamiteiten kunnen geautoriseerden die onderdeel zijn van de calamiteitenorganisatie via een aanvullend middel of aanvullende autorisaties toegang krijgen tot meer ruimten en toegangen dan in een reguliere situatie.
- De toegang tot ruimten kan beperkt worden voor geautoriseerden door het toegangsbeheer op de desbetreffende locatie of in het gebied op te schalen (lock down scenario bij verhoogde dreiging, zie ook bepalingen in het Continuïteitsplan 3.7);

Binnen locaties vindt compartimentering plaats zodat goed is in te regelen dat geautoriseerden van verschillende diensten, divisies en afdelingen niet bij elkaar naar binnen kunnen in het geval dit ongewenst is (denk aan ongewenste toegang in het kader van de aanwezigheid van vertrouwelijke en privacygevoelige informatie en/of kritische, potentieel gevaarlijke processen). Zo worden ruimten met meer kritische en/of waardevolle processen, informatie en goederen gescheiden van de meer algemene ruimten voor overleg, sanitaire en restauratieve doeleinden.

Op alle toegangen tot locaties (buitendeuren) wordt toezicht gehouden. Daar waar direct persoonlijk toezicht ontbreekt worden technische middelen ingezet. Bij toegangen met persoonlijk toezicht is dat toezicht aanwezig vanaf het moment dat de toegang wordt geopend tot het moment dat deze weer gesloten wordt.

5.2 Pashouders en Amsterdam UMC-passen

Het eerste en voorkeurs middel voor toegang is de Amsterdam UMC-pas. Deze maakt pashouders herkenbaar middels de verplichte draagplicht. Houders van de Amsterdam UMC-pas zijn te onderscheiden doordat passen van internen en externen een onderscheidende lay out¹ hebben. Passen zijn eigendom van Amsterdam UMC en worden in bruikleen gegeven, aan het eind van

¹ Naar verwachting gaat Amsterdam UMC een nieuwe pas implementeren. Nu is er nog een separate pas voor locatie AMC en VUmc.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

de dienstbetrekking, het contract of het bezoek worden passen ingeleverd. Passen op naam zijn voorzien van pasfoto en worden gebruikt als intern legitimatiemiddel. Een identificatieplicht geldt voor iedereen die een pas ontvangt. De volgende passen (en tags) worden onderscheiden (nog nader vast te stellen bij komst nieuwe Amsterdam UMC-pas):

- Interne Amsterdam UMC-pas - pas op naam voorzien van pasfoto
- Externe Amsterdam UMC-pas - pas op naam voorzien van pasfoto
- Tijdelijke pas - pas op naam zonder pasfoto voorzien van grote T (voor contracten < 1 maand)
- Leenpas - pas voor internen en externen die de pas zijn vergeten of kwijt zijn en die een pas kunnen lenen voor maximaal 7 dagen
- Functionele pas - pas op naam dienst, divisie of afdeling voorzien van grote F, denk hierbij aan:
 - Sleutelbadges
 - Liftenbadges
 - EKZ badges
 - Gastenbadges
- Calamiteitentag - tag voorzien van nummer en generale toegang. Beheerd vanuit bewaakte sleutelkasten en bedoeld voor de calamiteitenorganisatie

5.3 Sleutels, sluitplannen en procedures

Binnen alle locaties komen sleutels en sluitplannen voor. Het gebruik van sleutels en sluitplannen wordt naar de toekomst toe, mits technisch en financieel haalbaar, zoveel als mogelijk geminimaliseerd en uitgefaseerd. Binnen sluitplannen (verzamelnaam voor sloten/cilinders en sleutels) worden hoog- en laagrisico sleutels onderscheiden. Een sleutel voor maar 1 of enkele deuren is een laagrisico sleutel, sleutels die heel veel deuren openen (moedersleutels of generale hoofdsleutels) brengen een hoog risico met zich mee. Hoog risico sleutels worden beter beveiligd en middels sluitende registratie uitgegeven en blijven altijd op de locatie achter waar deze gebruikt wordt. Hoog risico sleutels worden bewaakt door geautomatiseerde sleutelkasten wanneer zij niet in gebruik zijn.

Laag risico sleutels kunnen op naam worden uitgegeven. Zij worden in bruikleen gegeven en de uitgifte wordt vastgelegd. Sleutels worden niet uitgeleend en verlies/ diefstal wordt direct gemeld bij de gebiedsbeheerder.

De gebruiker is ten alle tijden verantwoordelijk voor het juist gebruik en beheer van de sleutel in bruikleen. Bij verlies van sleutels kunnen kosten van vervanging (denk aan cilinders) verhaald worden op de betreffende medewerker/ afdeling.

5.4 Processen en werkinstructies voor passen en sleutels

Voor de aanvraag, uitgifte en inname van toegangsmiddelen en autorisaties zijn werkprocessen en werkinstructies van kracht waarbij deze zoveel als mogelijk geautomatiseerd zijn. Het aanvragen en toekennen van autorisaties worden via het PIAM ingeregeld [zie 3.4](#).

De uitgifte van interne en externe passen verloopt via het Service Centrum van FD. Passen op naam zijn voorzien van een pasfoto. Sleutels en cilinders worden beheerd door SRM en de uitgifte hiervan wordt ook door SRM verzorgd. Op beide locaties zijn verschillende sluitsystemen in gebruik.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

6. Inzet techniek en meldkamer

6.1 Inzet techniek

Op zoneovergangen worden beveiligingsmiddelen ingezet. Hierbij worden Organisatorische (O) bouwkundige (B) en elektronische (E) componenten onderscheiden. De volgende regels gelden voor de in te zetten B en E middelen:

- Er worden zo min als mogelijk verschillende systemen ingezet vanuit een financieel en beheer oogpunt (voorkeur voor 'Over de Amstel' systemen indien mogelijk);
- In te zetten elektronische systemen zijn koppel- en integreerbaar met de PSIM-applicatie² in de meldkamers om systemen efficiënt te kunnen monitoren en bedienen;
- Systemen worden eenduidig en uniform op centraal niveau ingericht en beheerd;
- Locatie systemen (bijvoorbeeld sluitplannen en sleutels) worden binnen de locatie ingericht en beheerd.

De volgende Bouwkundige componenten maken onderdeel uit van Toegangsbeheer:

- Sleutels en sluitplannen (mechanisch toegangsbeheer);
- Deuren, kozijnen en gevelelementen;
- Fysieke buitenmaatregelen zoals hekwerken en poorten voor zover aan beveiliging gerelateerd;
- Compartimenteringsmaatregelen zoals inbraak- en brandwerende kasten, kluizen en strong rooms (ruimten waarvan de wanden, kozijnen, vloeren en/of plafonds zwaarder dan standaard zijn uitgevoerd en overklim- en onderdoor kruipmogelijkheden zijn tegengegaan).

De volgende E beveiligingssystemen maken onderdeel uit van Toegangsbeheer:

- Meldkamersysteem/ PSIM en KVM³.
- Card Management Systeem (CMS)
- Online toegangssystemen;
- Offline toegangssystemen;
- Parkeermanagement systemen;
- Geautomatiseerde sleutelkastsystemen.
- Inbraak/ paniek/ molest detectie- en alarmeringssystemen;
- Intercominstallaties voor toegangsverlening op afstand;
- Camerasystemen voor zover ondersteunend aan toegangsbeheer

De beveiligingssystemen hebben een nauwe relatie met brandsystemen en kunnen gekoppeld zijn. De werking van de beveiligings- en brandsystemen is op elkaar afgestemd waarbij de functionaliteit van het brandsysteem altijd prevaleert boven die van het beveiligingssysteem. Voor meer details over de systemen zie [bijlage 2](#).

6.2 Sluittechnieken

Binnen Amsterdam UMC worden meerdere sluittechnieken ingezet te weten:

- Online paslezers (volledig bedraad en of op afstand te monitoren en te bedienen);
- Online paslezers (onbedraad), de wens bestaat deze op termijn uit te faseren;
- Offline paslezers (voorzien van een accu, pasmutaties op deze sloten komen vertraagd door);
- Cilindersloten bediend door sleutels.

² Physical Security Information Management

³ Keyboard, video en monitor/muis

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Beide locaties (AMC en VUmc) beschikken over een eigen online toegangssysteem (AMC heeft 2 online systemen). Gewenst is een Over de Amstel breed offline toegangssysteem in te zetten. Momenteel maakt alleen VUmc beperkt gebruik van offline paslezers.

Offline paslezers zijn veel aantrekkelijker qua aanschaf dan online paslezers. Echter niet alle deuren kunnen worden voorzien van offline paslezers gezien de beperkingen die deze sluittechniek kent. Om deze reden is een overzicht gemaakt wanneer online, offline of een sleutel toe te passen. Dit overzicht is leidend bij bouw- en verbouwprojecten en is te vinden in **bijlage 4**. Het gaat om de volgende 2 overzichten

1. Het eerste betreft een functioneel overzicht: op welk type toegang wordt welke sluittechniek toegepast.
2. Het tweede overzicht is een meer technisch overzicht; het geeft op basis van dezelfde typen toegangen aanvullende technische informatie

6.3 Implementatie van techniek

Het kan zijn dat bouwdelen, etages en/of ruimten qua inzet van beveiligingssystemen nog niet voldoen aan de in dit document gestelde kaders. In deze gevallen worden de kaders uit dit document gevolgd op het moment dat hiervoor een verbouwings-/ renovatieproject start.

In geval Amsterdam UMC besluit tot aanschaf van een geheel nieuw systeem dan worden de functionele en technische eisen opgesteld door SRM respectievelijk **HVT** (de twee eigenaren van de beveiligingssystemen). Minimale vereisten zijn dat systemen naadloos passen in de in hoofdstuk 3 opgenomen architecturen en dat de systemen zo flexibel als mogelijk zijn en vendor locks zoveel als mogelijk uitgesloten worden.

6.4 Relatie naar meldkamer

In de twee meldkamers van Amsterdam UMC komen de **bij 6.1 genoemde** systemen samen volgens de architecturen genoemd **bij 3.2**. In de meldkamers komen meldingen en alarmen van systemen binnen waarop beveiligers van Amsterdam UMC acties uitzetten. Naast de beveiligingssystemen komen hier ook communicatiesystemen binnen. De Meldkamer is het centrale knooppunt voor toegangsbeheer. Momenteel beschikt Amsterdam UMC over 2 meldkamers die nog niet geharmoniseerd zijn. Het werken op de twee hoofdlocaties vraagt specifieke kennis en vaardigheden van beveiligers per locatie. De komende tijd wordt gewerkt aan een harmonisatie van systemen en werkprocessen opdat de beveiliging verder geoptimaliseerd kan worden.

Meldingen en alarmen v.w.b. toegangsbeheer worden vastgelegd en gebruikt als input voor het bijsturen (plan-do-check-act) van maatregelen.

6.5 Meldkamersystemen

Momenteel zijn de meldkamers voorzien van verschillende oplossingen. Locatie AMC gebruikt een KVM oplossing als schil over de verschillende systemen om met slechts een muis, toetsenbord en 2 schermen alle systemen te kunnen bedienen. Locatie VUmc werkt met een softwarematige integratie laag over een aantal beveiligingssystemen. Beide systemen hebben voordelen en de uiteindelijke oplossing ligt in het gebruik van beide meldkamersystemen op beide locaties.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Op beide locaties worden alle systemen onder de KVM oplossing gebracht. Deze oplossing is eenvoudig schaalbaar en flexibel inzetbaar. Hiermee zijn systemen van locatie AMC vanuit locatie VUmc te bedienen en vice versa. Daarnaast worden die systemen, die het meest profiteren van een diepgaande integratie, geïntegreerd binnen de PSIM oplossing die reeds aanwezig is op locatie VUmc.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

7. Toezicht, handhaving, calamiteiten en borging

7.1 Toezicht en handhaving

Maatregelen zijn pas effectief wanneer zij door de Amsterdam UMC-organisatie gedragen en goed gebruikt worden. Hier komt de noodzakelijke focus en een Amsterdam UMC manier van samenwerken om de hoek kijken. Om deze reden is er veel aandacht voor de nut en noodzaak van maatregelen door middel van gerichte communicatie en bewustwordingsprogramma's in de vorm van ontwikkelprogramma's die voor alle Amsterdam UMC'ers gelden. Toezicht, handhaving en beloning zorgen ervoor dat een juist gebruik van voorzieningen ingebed raakt binnen de organisatie.

Iedereen die bij of voor Amsterdam UMC werkt heeft een taak en is verantwoordelijk voor toegangsbeheer. Hierbij gaat het onder andere om het op de juiste manier gebruiken van de toegangsmiddelen en -rechten, het zichtbaar dragen van de Amsterdam UMC-pas en het tegengaan dat 'onbekenden' meelopen naar gebieden/zones waar ze niet toe geautoriseerd zijn. Het lijn- en stafmanagement is verantwoordelijk voor toezicht en handhaving binnen locaties en is hiermee belegd binnen de divisies en diensten en daartoe behorende afdelingen.

Bij overtreding van regels en afspraken op het gebied van toegangsbeheer kan de toegang ontzegd, passen geblokkeerd en sleutels ingenomen worden. Het lijn- en stafmanagement heeft een voorbeeldfunctie en kan de eigen medewerkers disciplinaire maatregelen opleggen bij frequente overtredingen. Aangezien belonen beter werkt dan straffen worden er ook acties ingezet om medewerkers op positieve wijze te stimuleren de maatregelen goed te gebruiken.

Bij vermoedens van misbruik/ incidenten kan Amsterdam UMC de log van beveiligingssystemen raadplegen om vermoedens te staven. Hierbij worden onder andere de regels van de AVG gerespecteerd en gevolgd en de afdeling Juridische Zaken betrokken.

In contracten met derden zijn afspraken vastgelegd hoe om te gaan met toegang tot locaties (terreinen en gebouwen). Bij overtreding van afspraken kunnen sancties worden opgelegd en kan de toegang ontzegd worden. Inkoop legt de afspraken binnen contracten met derden vast.

7.2 Calamiteiten en crisissituatie

Bij een externe ramp of een grote interne calamiteit is binnen Amsterdam UMC sprake van een crisissituatie (zie ook Integraal Crisisplan: ZIROP en Bedrijfsnoodplan). Hiervan is sprake bij bijvoorbeeld een pandemie (besmettingsgevaar), een brand of een potentiële terreuractie in de omgeving van Amsterdam UMC. In dit geval schakelt Amsterdam UMC over van de reguliere situatie naar een crisissituatie en wordt het toegangsbeheer aangepast. Dit kan ertoe leiden dat toegangen worden afgesloten, aanvullend menselijk toezicht of screening plaatsvindt, hulpdiensten prominent aanwezig zijn en dat pashouders met een calamiteitenfunctie ruimere autorisaties krijgen. In deze situatie bevindt Amsterdam UMC zich in 'Lock Down'.

7.3 Borging Toegangsbeheer

Door SRM worden tests, controles en inspecties uitgevoerd om de werking en het juiste gebruik van systemen te toetsen. Afhankelijk van het risico dat aanwezig is op locaties/ in ruimten kan dit meer of minder frequent worden uitgevoerd. Met leveranciers van beveiligingssystemen worden contracten voor software assurance en preventief & correctief onderhoud afgesloten om systemen naar de toekomst up to date en functioneel te houden.

Meldingen, incidenten en alarmen voor wat betreft toegangsbeheer en resultaten uit bovengenoemde tests, controles en inspecties worden zorgvuldig vastgelegd opdat verbeteracties kunnen worden ingezet en gevolgd. Dit hele proces om toegangsbeheer te borgen en hiermee te optimaliseren wordt



Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

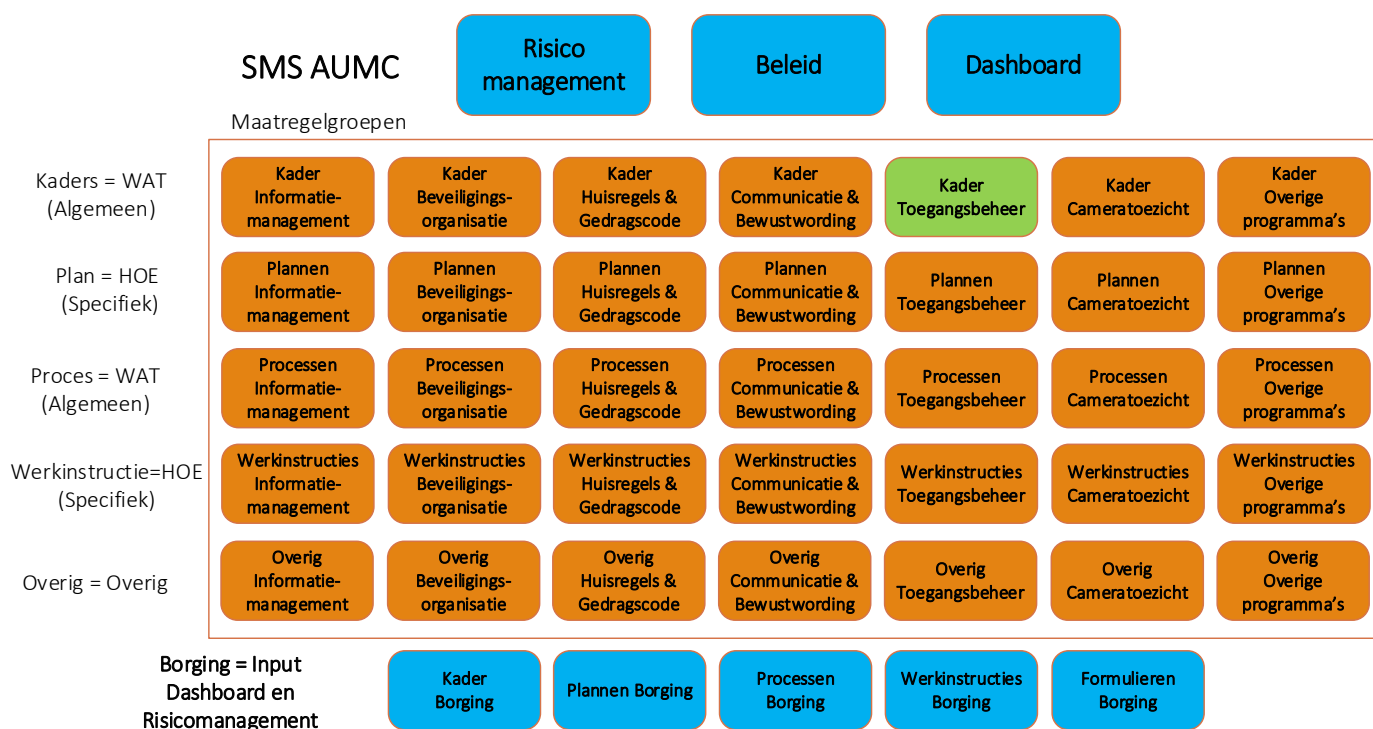
beheerd door SRM en in samenwerking met Beveiliging en **HVT (afdeling Onderhoud beheer en energie)** uitgevoerd.

Met behulp van de hier beschreven borging is Amsterdam UMC in staat om Toegangsbeheer conform een continu kwaliteitsproces van 'plan - do - check - act' over de tijd te optimaliseren.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Bijlage 1 Overzicht toegangsbeheer binnen SMS Amsterdam UMC

Onderstaand is een overzicht van het Security Management Systeem voor Fysieke Beveiliging van Amsterdam UMC opgenomen. Toegangsbeheer is een van de maatregelkolommen voor fysieke beveiliging. Dit kaderdocument is het bovenste veld van deze maatregelkolom (zie groene veld).



Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Bijlage 2 Overzicht systemen en beheer Toegangsbeheer Amsterdam UMC

In deze bijlage zijn een aantal overzichten opgenomen:

1. Overzicht met alle systemen die tot Toegangsbeheer behoren
2. Overzicht van de beheertaken per systeem

Overzicht systemen

Systemen Toegangsbeheer	Locatie	Fabricaat	Software	Geharmoniseerd	Software domein	OnPrem/SAAS	Hardware aanwezig	Firmware aanwezig
Toegang online	AMC	EAL ATS	Ja	Niet nodig	AMC	OnPrem	Ja, veel	Ja, paslezers/ controllers
Toegang online	AMC (Liften)	SynGuard	Ja	Niet nodig	AMC	OnPrem	Ja, veel	Ja, paslezers/ controllers
Toegang online	AMC (HIC - APC)	SynGuard	Ja	Niet nodig	AMC (HIC)	OnPrem	Ja, veel	Ja, paslezers/ controllers
Toegang online/ offline	Vumc	Nedap AEOS	Ja	Niet nodig	Vumc	OnPrem	Ja, veel	Ja, paslezers/ controllers
Toegang offline (Gewenst)	AMC + Vumc	NTB		Gewenst				
CMS en AUMC-pas	AMC + Vumc	OCMS (2 systemen)	Ja, 2 maal	Gewenst	AMC en Vumc	OnPrem	Ja, beperkt (printers)	Ja, printers
Sleutelkasten	AMC + Vumc	Traka (2 systemen)	Ja, 2 maal	Gewenst	AMC en Vumc	OnPrem	Ja	Ja, de kasten
Lockers	AMC (Vumc geen)	Vecos Release me	Ja	Gewenst	AMC	SAAS?	Ja, lockers	Ja, lockers
Parkeren	AMC (Vumc bij VU)	SkiData	Ja	Niet nodig	AMC	OnPrem	Ja	Ja, automaten
KiaKua	AMC	LTC	Ja	Gewenst?	AMC	OnPrem	Ja	Ja
KiaKua	VUmc	Metal Progetti	Ja	Gewenst?	VUmc	OnPrem	Ja	Ja
MFP	AMC + Vumc	Ricoh / Equitrac	Ja	Ja	AUMC	OnPrem?	Ja (alleen paslezer)	Ja, paslezers
SSO/2FA	AMC + Vumc	Imprivata	Ja		AUMC	OnPrem?	Ja (alleen paslezer)	Ja, paslezers
Systemen Meldkamer	Locatie	Fabricaat	Software	Geharmoniseerd	Software domein	On Prem / SAA	Hardware aanwezig	Firmware aanwezig
Toegang online	Zie boven							
Camerasysteem (security)	AMC + Vumc	Genetec (IDIS AMC)	Ja	Ja (eind 2025)	AUMC	OnPrem	Ja	Ja, camera's
Intercomsysteem	AMC	Commend	Ja	Gewenst	AMC	OnPrem	Ja	Ja, posten
Intercomsysteem	VUmc	Commend + Stentofon		Gewenst	VUmc	OnPrem	Ja	Ja, posten
Inbraakdetectiesysteem	AMC	Aritech, Unii, Galaxy	Ja	Niet nodig	AMC	OnPrem	Ja	Ja, op componenten
Inbraakdetectiesysteem (schil)	AMC	Seconts	Ja	Niet nodig	AMC	OnPrem	Nee	Nee
Inbraakdetectiesysteem	VUmc	Nedap AEOS	Ja	Niet nodig	Vumc	OnPrem	Ja	Ja, op componenten
GBS Niagara (alarmen)	VUmc	Niagara	Ja	Niet nodig	VUmc	OnPrem	Ja	Ja?
KVM	AMC	Inter OppSpace	Ja	Gewenst	AMC	OnPrem	Ja	Ja?
PSIM	VUmc	Advancis Winguard	Ja	Gewenst	VUmc	OnPrem	Nee	Nee

Overzicht beheer systemen

Systemen Toegangsbeheer	Functioneel Beheer	Technisch Beheer	FAB	TAB	Operationeel	Opmerkingen
Toegang online EAL/ATS	SRM	DHVT/Beheer	SRM/DICT	DICT	Beveiliging	Op termijn naar FD/WIM
Toegang online Synguard (liften)	DHVT	DHVT	DHVT	DICT	Beveiliging	Buiten scope SRM
Toegang online Synguard (HIC)	HIC	HIC	HIC	HIC	HIC	Systemen derden (HIC)
Toegang online/ offline AEOS	SRM	DHVT/Beheer/SRM	SRM	DICT	Beveiliging	Op termijn naar FD/WIM
Toegang offline NTB	SRM	DHVT/Beheer	SRM	DICT	Beveiliging	
CMS en AUMC-pas	FD/MedServices	FD/MedServices	DICT	DICT	FD Service Centrum	Buiten scope SRM
Sleutelkasten	SRM	DHVT/Beheer	SRM	DICT	SRM / Beveiliging	Op termijn naar FD/WIM
Lockers	FD/MedServices	FD/MedServices	FD/Wim	DICT (SAAS)	Gebruiker	Buiten scope SRM
Parkeren (alleen AMC)	FD/Mobiliteit	FD/Mobiliteit	FD/Wim	DICT	Beveiliging	Buiten scope SRM
KiaKua	FD/Textiel	FD/Textiel	FD/Textiel	DICT	Linnenkamer	Buiten scope SRM
KiaKua	FD/Textiel	FD/Textiel	FD/Textiel	DICT	Linnenkamer	Buiten scope SRM
MFP	DICT	DICT	DICT	DICT	AUMC	Buiten scope SRM
SSO/2FA	DICT	DICT	DICT	DICT	AUMC	Buiten scope SRM
Systemen Meldkamer	Functioneel Beheer	Technisch Beheer	FAB	TAB	Operationeel	Opmerkingen
Toegang online	Zie boven					
Camerasysteem (security)	DHVT	DHVT/Beheer	SRM/DHVT	DICT/DHVT	Beveiliging	Na uitrol Genetec op AMC
Intercomsysteem AMC	DHVT	DHVT/Beheer	DICT	DICT?	Beveiliging	
Intercomsysteem VUmc	DHVT	DHVT/Beheer	DHVT	DHVT	Beveiliging	
Inbraakdetectiesysteem AMC	SRM	DHVT/Beheer	SRM	DICT	Beveiliging	Galaxy niet beheerd
Inbraakdetectiesysteem AMC (schil)	SRM	NVT	SRM	DICT	Beveiliging	Mogelijk via Winguard
Inbraakdetectiesysteem VUmc	SRM	DHVT/Beheer	SRM	DICT	Beveiliging	
GBS Niagara (alarmen)	DHVT	DHVT/Beheer	DHVT	DICT	Beveiliging	Buiten scope SRM
Inter KVM	DHVT	DHVT/Beheer	DHVT	DICT	Beveiliging	
Winguard Advancis	SRM/ Beveiliging	NVT	SRM	DICT	Beveiliging	

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Bijlage 5 Toezicht op radioactieve stoffen Amsterdam UMC

1. Rol, benoeming en delegatie gedelegeerd beveiligingsverantwoordelijke BRAS

1.1 Benoeming

Om te voldoen aan de wet- en regelgeving met betrekking tot de Beveiliging Radioactieve Stoffen (BRAS) wordt binnen Amsterdam UMC een beveiligingsverantwoordelijke voor de beveiliging van radioactieve stoffen aangewezen.

1.2 Delegatie

De clustermanager Services en Veiligheid draagt deze verantwoordelijkheid op het gebied van BRAS, in nauw overleg en afstemming, over aan het Hoofd Security Risk Management (SRM). Het Hoofd SRM vervult daarmee de rol van gedelegeerd beveiligingsverantwoordelijke voor de beveiliging van radioactieve stoffen binnen Amsterdam UMC.

1.3 Doel en verantwoordelijkheid

De gedelegeerd beveiligingsverantwoordelijke (Hoofd SRM) zorgt ervoor dat binnen Amsterdam UMC de maatregelen tegen diefstal en misbruik van radioactieve bronnen voldoen aan de geldende wet- en regelgeving en interne beleidskaders.

2. Taken van de gedelegeerd beveiligingsverantwoordelijke

2.1 Beveiligingsplannen

Het opstellen van beveiligingsplannen voor radioactieve stoffen.

2.2 Evaluatie

De jaarlijkse evaluatie van deze beveiligingsplannen.

2.3 Oefeningen en scenario's

Het organiseren van een jaarlijkse oefening (scenario), mede ten behoeve van:
De toetsing en evaluatie van het beveiligingsplan.
Het oefenen van de respons bij (dreigende) incidenten.

3. Jaarlijkse controles en informatie-uitvraag

3.1 Bouwkundige en elektronische beveiliging

Jaarlijks worden fysieke controlerondes uitgevoerd gericht op:
Bouwkundige beveiligingsmaatregelen.
Elektronische beveiligingsmaatregelen.

3.2 Organisatorische informatie-uitvraag binnen Amsterdam UMC

Jaarlijks wordt informatie opgevraagd bij:
Security Risk Management (SRM).
Beveiliging.
Huisvesting, Vastgoed & Techniek (HV&T).
ICT.
Doel: toetsing en borging van de organisatorische maatregelen rondom de beveiliging van radioactieve stoffen.

3.3 Lokale stralingsverantwoordelijken

Jaarlijks wordt aanvullende organisatorische informatie opgevraagd bij de lokale stralingsverantwoordelijken.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

4. Juridische grondslag en beleidskaders

4.1 Wet- en regelgeving

De taken, bevoegdheden en verantwoordelijkheden op beveiligingsgebied vloeien voort uit:

Besluit Basisveiligheidsnormen stralingsbescherming.
 Regeling Basisveiligheidsnormen stralingsbescherming.
 ANVS-verordening Basisveiligheidsnormen stralingsbescherming.

5. Toezicht op bronnen en toegangverlening

5.1 Aanwijzen van toezichthouders

De gedelegeerd beveiligingsverantwoordelijke ziet erop toe dat er personen worden aangewezen die persoonlijk toezicht houden op de radioactieve bron. Dit gebeurt in overleg en samenwerking met de Stralingsbeschermingseenheid (SBE), vertegenwoordigd door de algemeen coördinerend stralingsdeskundigen. De SBE wijst deze personen formeel aan.

5.2 Toegangverlening

De gedelegeerd beveiligingsverantwoordelijke:
 Verleent daadwerkelijke toegang tot beveiligde gebieden via Security Risk Management. Zorgt dat toegangverlening plaatsvindt in overeenstemming met de lokale stralingsverantwoordelijken, zoals door SBE aangewezen. De medewerkers belast met het persoonlijk toezicht zijn dus indirect aangewezen door de beveiligingsverantwoordelijke conform Art. 4.14, lid 2. Hierbij zijn zij dus verantwoordelijk voor juiste omgang met radioactieve stoffen en dat deze niet worden onttreemd.

6. Rapportage, informatievoorziening en opvolging

6.1 Rapportage en informatievoorziening

Rapportages worden gedeeld via een beveiligde omgeving met:

6. De Stralingsbeschermingseenheid (SBE).
7. De gedelegeerd beveiligingsverantwoordelijke.
8. De lokale stralingsverantwoordelijke.

6.2 Monitoring en opvolging van acties

Ieder kwartaal worden acties, voortvloeiend uit controles, incidenten en evaluaties: Samen met SBE gemonitord.
 Uitgezet bij de verantwoordelijke afdelingen/personen.

6.3 Aanpassing van beleid

Zo nodig wordt het beleid aangepast naar aanleiding van:

1. Evaluatie-uitkomsten.
2. Bevindingen uit incidenten.
3. Gewijzigde wet- en regelgeving.

6.4 Periodieke terugkoppeling en escalatie

Bevindingen uit evaluatieprogramma's en incidenten worden periodiek gedeeld met: Directeuren bedrijfsvoering.
 Bij incidenten wordt teruggekoppeld aan:
 De Raad van Bestuur, conform interne escalatie- en meldingsprocedures.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Bijlage 4 Overzicht wet- en regelgeving

Op fysiek toegangsbeheer voor Amsterdam UMC zijn de volgende wetten, normen en regelingen van kracht:

Wetten en regelingen:

- Arbeidsomstandighedenwet;
- AVG;
- Bouwbesluit;
- Burgerlijk Wetboek, Boek 5 (zakelijke rechten);
- CER (Critical Entities Resilience Directive); Wet weerbaarheid kritieke entiteiten (Wwke)
- NIS2 (Network and Information Security); Cyberbeveiligingswet (Cbw)
- Milieuwetgeving;
- Omgevingswet;
- Politiewet;
- Wet particuliere beveiligingsorganisaties en recherchebureaus (voor zover Amsterdam UMC externen inhuurt voor taken op gebied van toegangsbeheer);
- Wetboek van Strafrecht; artikel 461- verboden toegang;
- Wet vervoer gevaarlijke stoffen;
- Opiatenwet;
- Wet MLIII labs;
- Verordening van de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Wet op de dierproeven
- Arbeidsomstandighedenbesluit
 - Artikel 4.84. Biologische agentia, celculturen en micro-organismen
- Regeling genetisch gemodificeerde organismen (Regeling GGO)
- Wet Geneeskundige Behandeloovereenkomst (WGBO);
- NEN7510.

Normeringen

- Alle normen die van toepassing zijn op het installeren, onderhouden en beheren van mechanische en elektronische beveiligingssystemen en meldkamers.

Wetten, regelingen en normeringen zijn aan verandering onderhevig. Van toepassing is telkens de laatste versie of meest recente definitieve uitvoering.

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

Bijlage 5 Overzichten toe te passen sluittechnieken

Overzicht sluittypen Amsterdam UMC (functioneel overzicht)

#	Type toegang Binnen/ Buiten	Type sluiting (on-, offline of sleutel)	Toegangszone (AMC kleuren)	Voorbeelden binnen Amsterdam UMC	Bijzonderheden
1	Buiten: Poorten, speedgate, slagbomen	Online	ORANJE	Expeditie, goederenontvangst, bouwterreinen en overige beveiligde buitenterreinen (geen parkeerterreinen, deze hebben een lager beveiligingsniveau)	Gebied, terrein is omheind en niet vrij toegankelijk. Uitzondering parkeerterreinen medewerkers.
2	Buiten: Slagbomen	Online	GROEN en ORANJE	Parkeerterreinen en -garages	Parkeren: kan ook onderdeel Parkeer Management Systeem.
3	Buitendeuren: Personeelstoegangen	Online	GROEN, BLAUW, ROOD	Buitendeuren permanent gesloten en alleen toegankelijk voor personeel	Publiekstoegang kan na sluitingstijd een personeelstoegang worden)
4	Buitendeuren: Publieksingangen via tourniquet	Sleutel	GROEN en BLAUW	Buitendeuren die toegang geven aan alle publieksfuncties	In geval Blauw betreft dit een specifieke publiekstoegang (bijv. toegang polikliniek)
5	Buitendeuren: Nooduitgangen zonder toegangsfunctie en bewaakt	Geen of calamiteiten-cilinder	GROEN, BLAUW, ROOD	Alle nooduitgangen op alle etages bedoeld om te vluchten bij calamiteiten	
6	Binnendeuren: Toegang gebied, etage,	Online	GROEN, BLAUW, ROOD	Toegangen alle bouwdelen, afdelingen, (poli)klinieken	Veel van deze toegangen in blauwe gebieden zijn overdag open en zijn na sluitingstijd afgesloten
7	Binnendeuren: Toegang vitale ruimte	Online	PAARS	MER, bepaalde SER, hoofd installatieruimten, MLIII labs, centrale opslag opiaten, opslag HR CBRN materiaal, meldkamer beveiliging / techniek, ...	Gecontroleerde deur uitvoering. NB: indien toegang is buitendeur: extra maatregelen treffen.
8	Binnendeuren: Toegang ruimten	Offline	GROEN, BLAUW	Alle werkruimten binnen groen en blauwe zones waar 5 - 30 personen werken	
9	Binnendeuren: Toegang ruimten	Sleutel	GROEN, BLAUW	Alle werkruimten binnen groene en blauwe zones waar 1 - 5 personen werken	Op termijn worden hier ook offline sloten geplaatst
10	Binnendeuren: Toegang werkruimte	Geen	ROOD	Alle werkruimten binnen rode gebieden waarvan de voordeur op slot zit	Dit zijn werkgebieden/ kantoren met een 24u gesloten voordeur. Mits juiste voorzieningen op entredeuren en lockers en past binnen de risico's.
11	Binnendeuren: Toegang laboratoria en technische ruimten	Offline	ROOD	Alle labs MLI, MLII, DMI en DMII en techniekruimten (E en W) waar minder dan 50 personen werken	In kader van regelgeving en/of specifieke wensen kan van voorgeschreven sluittype worden afgeweken
12	Binnendeuren:	Offline	GROEN, BLAUW, ROOD	Alle voorraadkasten en -ruimten grenzend aan gangen en binnen afdelingen, gebieden. Schoonmaakkasten.	

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

	Toegang voorraadruimten en -kasten				
13	Binnendeuren: Toegang kasten	Sleutel	GROEN, BLAUW, ROOD	Alle kasten grenzend aan gangen, denk aan E- en W-kasten en schachten.	Op termijn worden hier ook offline sloten geplaatst
14	Binnendeuren: Doorgang en toegang toiletten en badkamers	Geen	GROEN, BLAUW, ROOD	Brandscheidingsdeuren, sanitaire ruimten voor bezoekers en patiënten en medewerkers binnen RODE zones	Indien personeelstoilet binnen groen en blauwe gebieden: offline
15	Binnendeuren specials - Medicijnkamers - Couveuseruimte, neonatologie	Online	ROOD	Medicijnkamers waar veelal ook andere voorzieningen dan medicatie wordt beheerd	Ruimten kunnen voorzien zijn van automatische deuren en beschikken mogelijk over separaat afgesloten opbergmedium (voor opiaten)

Overzicht sluittypen Amsterdam UMC (technisch overzicht)

#	Type toegang	Type gebruik	# gebruik	Online/ Offline Sleutel	Aanvullingen gewenst	Realtime monitoren en bedienen vanuit MK	Signalering bij deur	Bijzonderheden
1	Poorten, speedgate, slagbomen	Geautoriseerden	Klein	Online, 2 paslezers	Ja Camera+ Intercom	Ja Openen via intercom	Nee	Kan voorzien zijn van stoplicht
2	Slagbomen	Publiek en geautoriseerden	Groot	Online, 2 paslezers	Ja Camera+ Intercom	Ja Openen via intercom	Ja, via PMS	Parkeren AMC: Paslezers zijn onderdeel PMS
3	Personeelstoegangen	Geautoriseerden	Groot	Online, 2 paslezers	Ja Camera+ intercom	Ja Openen via intercom	Piep bij deur te lang open	Bij voorkeur zetten we tourniquets in. Voor karren etc. kunnen dit sluizen zijn
4	Publieksingangen via tourniquet	Publiek	Groot	Sleutel	Ja, optioneel Camera+ intercom	Ja, optioneel via camera en automatische deur		
5	Nooduitgangen zonder toegang en bewaakt	Iedereen	Klein	Optioneel sleutel of (voorkeur) zelfsluitend	Ja, camera op meerdere nooduitgangen	Ja, via deurcontact en signalering nooddrukker	Piep bij deur te lang open	Kan via insteekslot, espagnolet of kleeftmagneet vergrendeld zijn
6	Toegang gebied, etage, afdeling	Publiek en geautoriseerden	Groot >50 personen	Online (als gebied afgesloten moet kunnen worden)	Optioneel camera en intercom (afh. van gebruik)	Ja, alleen bedienen		Dit kunnen 24 uur en gedeeltelijk gesloten toegangen zijn
7	Toegang vitale ruimte	Geautoriseerden	Klein	Online	Optioneel camera en intercom (afh. van gebruik)	Ja, monitoren op oneigenlijk gebruik	Ja, piep bij deur te lang open	Gecontroleerde deur uitvoering, optioneel sterke authenticatie toepassen i.o.m. eigenaar
8	Toegang ruimten binnen publieke zone	Geautoriseerden	Klein 5-30 pers.	Offline	Nee	Nee	Nee	
9	Toegang ruimten binnen publieke zone	Geautoriseerden	Klein < 5 pers.	Sleutel	Nee	Nee	Nee	Deze worden op termijn uitgefaseerd, naar offline

Domein: Fysieke Beveiliging (FB)	Code: FB TOB KD	Titel: Kader Toegangsbeheer Amsterdam UMC
Versie: 3.5 Definitief	Datum: 20-06-2026	Classificatie: Intern gebruik

10	Toegang ruimten binnen gesloten gebieden (rood)	Geautoriseerden	Klein	Geen	Nee	Nee	Nee	Dit zijn werkgebieden/ kantoren met een 24u gesloten voordeur
11	Toegang laboratoria en technische ruimten	Geautoriseerden	Klein 1 - 30 personen	Offline	Nee	Nee	Nee	
12	Toegang voorraadruimten en -kasten	Geautoriseerden	Klein	Offline		Nee		
13	Toegang kasten, bijv. schachten	Geautoriseerden	Klein	Sleutel		Nee		Via hoofdsleutel
14	Doorgang en toegang toiletten en badkamers	Publiek en geautoriseerden	Van klein tot groot	Geen Vrij/bezet		Nee		Indien personeelstoilet: offline
15	Specials zoals: -Medicijnkamers - Couveuse, neonatologie	Geautoriseerden	Groot	Online	Nee	Ja, monitoren openstand deur. Per special te bepalen.	Ja, medicijnkamers	Opiaten zijn apart afgesloten

NB1: Vitale (paarse) ruimten kunnen optioneel aangevuld zijn met een code of biometrisch kenmerk (sterke authenticatie). Hier wordt echter zeer terughoudend mee omgegaan i.v.m. de extra beheerlast die dit met zich meebrengt. Dit geldt ook voor publiektoegankelijke ruimten, het kan op gewenst zijn de toegang tot bijvoorbeeld de kraamafdeling of dialyse te voorzien van een lezer die QR-codes kan uitlezen van mobiele telefoons van patiënten en bezoekers.

NB2: In bovenstaand overzicht zijn de toegangszones/ kleuren zoals gehanteerd in AMC opgenomen. Deze worden in VUmc gewijzigd zodat deze geharmoniseerd zijn met de locatie AMC.