HANDLEIDING · V1.0

AccessGuard

Zeker weten wie waar toegang heeft.

Volledige referentie voor het gebruik van AccessGuard, van je eerste matrix tot periodieke reviews, van het onboarden van nieuwe medewerkers tot het waterdicht afsluiten bij uitdiensttreding.

Inhoud

01 Introductie

AccessGuard is toegangsbeheer voor MKB zonder IT-afdeling. Deze handleiding behandelt alles, van de eerste opzet tot dagelijks gebruik.

Welk probleem lost dit op?

In de meeste MKB-bedrijven is toegangsbeheer verspreid over Excel-sheets, e-mails en geheugens van mensen. Niemand heeft een betrouwbaar antwoord op "wie heeft toegang tot Salesforce?" of "hebben we alles ingetrokken toen Lisa vertrok?". Deze chaos zie je niet, tot er een audit is, een incident, of een ex-medewerker die nog steeds bij gevoelige data kan.

Voor wie is dit?

- Organisaties van 10-200 medewerkers
- Geen dedicated IT-afdeling of IAM-team
- Gebruik van 5-30 SaaS-systemen (M365, Slack, Salesforce, Exact, etc.)
- Compliance-eisen (ISO 27001, NEN 7510, GDPR-audits)
- Externe leveranciers en tijdelijke krachten die ook toegang krijgen

Kernbegrippen

BEGRIP	BETEKENIS
Persoon	Een medewerker, inhuur-kracht of externe partij wiens toegang je bijhoudt. Heeft een status: active, scheduled_in, scheduled_out of inactive.
Systeem	Een app of service waar iemand toegang tot kan hebben. Gecategoriseerd als SaaS, on-prem, infrastructuur, financieel, security, communicatie of overig.
Cell	Het kruispunt van een persoon en een systeem in de Access Matrix. Bevat één van vier statussen.

Access item	Een fijnmazige permissie binnen een systeem (rol, licentie, account). Optioneel; alleen gebruikt als het systeem ze heeft.
Review-cyclus	Een periodieke exercitie waarbij elke cel (of item) een keep/revoke/change beslissing krijgt van een reviewer.
Proces	Een onboarding- of offboarding-workflow voor één persoon, met checklist, bewijs-uploads en automatische toegang-effecten.

02 Aan de slag

In ongeveer 15 minuten heb je je eerste matrix ingevuld en kun je beginnen met beslissen wat je gaat opruimen.

VEREISTEN

AccessGuard is beschikbaar vanaf het Pro-plan (€12/maand). Registreer je, kies Pro, en je bent binnen.

01. Voeg je personen toe

Ga naar AccessGuard → Personen. Voeg elke medewerker, inhuur-kracht en externe partij toe wiens toegang je wilt bijhouden. Je hoeft niet vanuit HR te importeren, een handvol rijen is prima om mee te starten.

02. Voeg je systemen toe

AccessGuard → Systemen. Alles waar je mensen toegang toe kunnen hebben: M365, Slack, Salesforce, Exact, 1Password, AWS, domeinbeheer, de fysieke alarmcode. Denk breed.

03. Vul de matrix in

AccessGuard → Access Matrix. Klik op een cel om door de statussen te rouleren: onbekend → heeft toegang → geen toegang → heroverwegen. Streef niet naar perfectie; vul in wat je al weet.

04. Start je eerste review-cyclus

AccessGuard → Reviews → Nieuwe cyclus. De huidige matrix wordt gesnapshot; jij beslist per rij behouden/intrekken/wijzigen. Bij afronding krijgt IT een acties-lijst.

03 De Access Matrix

De matrix is het hart van AccessGuard. Een 2D-rooster waarin de rijen personen zijn en de kolommen systemen. Elke cel toont één van vier statussen.

De vier cel-statussen

STATUS	BETEKENIS
✓ has_access	De persoon heeft momenteel toegang tot het systeem. Status is bevestigd.
× no_access	De persoon heeft geen toegang, en dat is bewust. Bevestigd negatief.
? needs_review	Niet zeker, markeer voor volgende review. Gebruikt als de status onduidelijk of verdacht is.
, unknown	Nooit beslist. De standaardstatus voor nieuwe cellen. Streef ernaar dit naar nul te brengen.

Hoe klik je door de matrix

Klik op elke cel zonder items om door de vier statussen te rouleren in volgorde. Klik nog eens om door te gaan. Elke klik wordt geregistreerd in last_verified_at, nuttig voor de review-cyclus om te zien "wanneer hebben we dit voor het laatst bevestigd?".

> **TIP**
>
> Vul eerst alleen has_access cellen in, de mensen die zeker toegang hebben. Dat alleen al laat zien waar toegang te ruim is. De rest mag "unknown" blijven tot de eerste review-cyclus.

04 Fijnmazige access items

Soms is "toegang tot Salesforce" te grof. Is deze persoon global admin, standaard gebruiker of read-only? Access items laten je per rol/licentie/account binnen een systeem bijhouden.

Wanneer gebruik je items

- Systemen met meerdere licentie-niveaus (M365: Basic / E3 / E5)
- Systemen met rol-hiërarchieën (Salesforce: Admin / Standard / Read-only)
- Systemen waar verschillende accounts uitmaken (Google Workspace: persoonlijk / service-account)
- Waar compliance-rapportages rol-niveau detail vereisen

Hoe de matrix zich gedraagt met items

Zodra een systeem één of meer actieve items heeft, wordt de cel op de matrix een drill-down link i.p.v. een klik-knop. De cel-status wordt automatisch afgeleid:

ITEM-COMBINATIE	CEL-STATUS
≥1 item has_access, alle gelijk	has_access
Enige needs_review of mix van statussen	needs_review
Alle items no_access	no_access
Nog geen items gezet	unknown

Items beheren

AccessGuard → Systemen → klik "Items" naast het systeem. Voeg toe / bewerk / deactiveer items. Elk item heeft een type (rol, licentie, account, sleutel, pas, groep, overig) en een

sorteervolgorde. Gedeactiveerde items verdwijnen uit de drill-down maar hun historie blijft in de audit-log.

05 Review-cycli

Een review-cyclus is een periodieke exercitie, per kwartaal of jaarlijks, waarin iemand elke matrix-cel doorloopt en beslist: deze toegang behouden, intrekken of wijzigen.

Cyclus-levensloop

`planned ? active ? completed` (of cancelled)

Een cyclus starten

AccessGuard → Reviews → Nieuwe cyclus. Kies een titel ("Q1 2026 access review"), een scope (actieve personen, of iedereen inclusief inactief), een optionele deadline, en notities voor de reviewer. Bij opslaan wordt de huidige matrix gesnapshot in review_items, één rij per cel (of per item als het systeem items heeft).

> **BELANGRIJK**
>
> Nadat de snapshot is genomen, beïnvloeden latere matrix-wijzigingen de cyclus NIET. De snapshot bevriest wat er werd besloten. Dit houdt het audit-spoor schoon.

Beslissingen nemen

BESLISSING	WAT GEBEURT ER BIJ AFRONDING
keep	De cel last_verified_at wordt bijgewerkt. Geen verdere actie nodig.
revoke	Een open revoke_access actie wordt aangemaakt. IT moet erop handelen.
change	Een open review_level actie wordt aangemaakt (bv. admin naar read-only degraderen).
(leeg)	Niet-besliste items worden standaard "keep" bij cyclus-afronding.

Bulk-beslissingen

Gebruik de checkboxes om meerdere review-items te selecteren en dezelfde beslissing in één klik toe te passen. Handig bij grote cycli waar de meeste beslissingen "keep" zijn.

06 Acties-queue

Als een review-cyclus afrondt (of een offboarding), materialiseren revoke- en change-beslissingen als open acties. De acties-queue is wat IT afwerkt.

Twee actie-soorten

- **revoke_access**, Verwijder deze toegang. Bij "afronden" flipt de matrix-cel naar no_access (of het individuele item als item-scoped).
- **review_level**, Wijzig het niveau (bv. admin → read-only). Bij "afronden" wordt alleen de verified timestamp bijgewerkt; je handelt de daadwerkelijke niveau-wijziging extern af en noteert het hier.

Typische flow

1. Reviewer sluit een cyclus met 6 revoke-beslissingen
2. 6 revoke_access acties verschijnen in de queue met status=open
3. IT deactiveert de accounts in de daadwerkelijke systemen (M365 admin centre, Slack, etc.)
4. IT klikt "Afronden" op elke actie, de bijbehorende matrix-cel flipt naar no_access
5. De audit-log registreert wie afgerond heeft + wanneer + wat is toegepast

07 Onboarding- en offboarding-processen

Een proces is een per-persoon workflow: een checklist van dingen die moeten gebeuren, met optionele bewijs-uploads per item. Twee soorten: onboarding (nieuwe medewerker) en offboarding (vertrekker).

Checklist-item statussen

`todo ? in_progress ? done / blocked / na`

- **todo**: standaard, niet gestart
- **in_progress**: wordt aan gewerkt
- **done**: succesvol afgerond
- **blocked**: wacht op iets externs, reden verplicht
- **na**: niet van toepassing voor dit geval, reden verplicht

Offboarding → automatische revokes

Het afronden van een offboarding heeft een krachtig neveneffect: elke has_access cel of item van de betreffende persoon wordt automatisch een revoke_access actie. Hierdoor kun je fysiek niet "vergeten" om toegang in te trekken, het systeem toont elke open deur.

> **BEWIJS-UPLOADS**
>
> Per checklist-item kun je PDF / JPG / PNG bestanden uploaden tot 15 MB. Handig voor: getekend hardware-retour formulier, screenshot van gedeactiveerd M365 account, foto van teruggegeven toegangspas. Elk bestand wordt opgeslagen met een UUID, SHA-256 gehasht voor integriteit, en alleen toegankelijk binnen de tenant.

08 Risico-detectie

Een geplande scan draait elke nacht om 03:00 en brengt risicovolle patronen naar boven als open risk-flags. Zeven detectie-regels dekken de meest voorkomende MKB access-control-problemen.

De zeven detectie-regels

REGEL	ERNST	TRIGGER
stale_admin	4	Admin-achtig item met has_access maar geen verificatie voor 90+ dagen
orphan_access	5	Inactieve persoon heeft nog actieve has_access cellen of items
excessive_access	3	Persoon heeft has_access op ≥10 verschillende systemen
overdue_review	4-5	Open cyclus voorbij due_at (5 bij >30 dagen over)
overdue_action	3-4	Open actie ouder dan 14 dagen (4 bij >30 dagen)
pending_onboarding	3	Persoon scheduled_in maar geen actief onboarding-proces
stale_credential	4-5	Vault credential voorbij expires_at (5) of rotatie overdue (4)

Risico's afhandelen

Voor elke open risk-flag heb je drie acties:

- **Bevestig**, Ik heb dit gezien, ga erop handelen. Gaat naar "acknowledged" status.
- **Opgelost**, Het onderliggende probleem is opgelost (account ingetrokken, review afgerond, etc.). Gaat naar "resolved".
- **Heropen**, Als iets te vroeg opgelost is, kun je het heropenen.

09 Reminders

Een tweede geplande job (dagelijks 03:15) scant op aankomende deadlines en maakt reminders aan. Reminders zijn in-app notificaties, lichter dan risk-flags.

REMINDER-SOORT	TRIGGERT WANNEER
cycle_due	Open review-cyclus due_at binnen 7 dagen of overdue
process_due	Actieve onboarding/offboarding due_at binnen 7 dagen of overdue
action_overdue	Open actie ouder dan 14 dagen
person_starting	Persoon scheduled_in met start_date binnen 7 dagen
person_leaving	Persoon scheduled_out met end_date binnen 7 dagen

Een reminder wegklikken markeert hem permanent dismissed, de volgende geplande run zal hem niet terugbrengen. "Klaar" sluit hem schoon af.

10 Vault (versleutelde credentials)

Bewaar wachtwoorden, tokens, API keys, SSH keys en certificaten, gekoppeld aan systemen of access items. Secrets worden versleuteld met AES-256 + HMAC; elke view of decrypt wordt gelogd.

Access-model

- De maker is impliciet admin (view + decrypt + rotate + delete). Geen ACL-row nodig.
- Iedereen anders heeft een expliciete ACL-grant nodig met de juiste flags.
- Vier rechten-niveaus: can_view, can_decrypt, can_rotate, can_admin.

Reveal-on-click workflow

Op de detail-pagina is de secret gemaskeerd als bolletjes. Klik "Toon" → het JSON endpoint decrypt en geeft de plaintext terug. De UI toont het 30 seconden met een aflopende teller, verbergt dan automatisch. Je kunt op de kopieer-knop klikken om het op het klembord te zetten.

> **AUDIT-TRAIL**
>
> Elke actie op een credential wordt gelogd: aangemaakt, bijgewerkt, bekeken (metadata), gedecrypteerd, geroteerd, verwijderd, en ACL-grants/revokes. Elke log-rij bevat de gebruiker en een gehashed IP-adres. Houd dit in gedachten, secret-toegang is NIET stil.

Offboarding → automatische ACL-revoke

Als een offboarding-proces afrondt voor een Persoon wiens e-mailadres matcht met een Gebruiker in de tenant, wordt elke ACL-row die die Gebruiker heeft automatisch ingetrokken. Eén email-match, nul credentials blijven toegankelijk.

11 AI-aangedreven uitleg

Niet iedereen in je team is een security-persoon. De AI-explain widget vertaalt een risk-flag naar begrijpelijke taal, wat het is, waarom het belangrijk is, en drie of vier concrete vervolgstappen.

Hoe het werkt

Klik op de □□ Uitleg knop bij een risk-flag. Een modal opent met:

- **Samenvatting**, twee-drie zinnen die het risico beschrijven
- **Waarom dit ertoe doet**, business + security context
- **Aanbevolen stappen**, drie of vier concrete acties in AccessGuard
- **Waarschuwingen**, waar je op moet letten

> **PRIVACY**
>
> Alleen de risk-flag metadata wordt naar OpenAI gestuurd, nooit secrets, nooit volledige e-mailadressen, nooit vault-inhoud. De payload is whitelist-gebaseerd op veilige keys (ids, counts, datums). Elke AI-call wordt gelogd met het aantal tokens. Rate-limited op 10 calls per tenant per uur; identieke prompts worden 24 uur gecached.

12 Plannen & limieten

AccessGuard is inbegrepen vanaf het Pro-plan. Business voegt multi-user-toegang toe en verwijdert de AI rate-limit.

FUNCTIE	FREE	PRO €12/MO	BUSINESS €39/MO
Access Matrix + items	,	✓	✓
Review-cycli	,	✓	✓
Onboarding / offboarding	,	✓	✓
Risk flags + reminders	,	✓	✓
Vault	,	✓	✓
AI-uitleg	,	10/u	unlimited
Multi-user toegang	,	,	✓

13 Begrippenlijst

Snelle referentie voor de termen en afkortingen in AccessGuard.

BEGRIP	BETEKENIS
ACL	Access Control List, de per-gebruiker permissie-rijen op een vault credential.
Access cel	Het kruispunt van persoon en systeem in de matrix.
Access item	Een fijnmazige permissie binnen een systeem (rol, licentie, account).
Cyclus	Een review-cyclus: een tijdgebonden exercitie waarbij elke cel in een snapshot wordt beoordeeld.
has_access	Cel-status: persoon heeft momenteel bevestigde toegang.
IAM	Identity and Access Management, de bredere discipline waar AccessGuard onder valt.
last_verified_at	Tijdstip waarop een cel/item voor het laatst is bevestigd. Drijft stale-admin detectie.
needs_review	Cel-status: status onduidelijk, markeer voor volgende cyclus.
no_access	Cel-status: persoon heeft bewust geen toegang.
Offboarding	Het proces voor iemand die de organisatie verlaat. Afronding triggert automatische revoke-acties.
Onboarding	Het proces voor iemand die bij de organisatie komt. Checklist-gebaseerd met bewijs-uploads.
Persoon	Iemand wiens toegang je bijhoudt, medewerker, inhuur of extern.

Risk flag	Een gedetecteerd risico-patroon. Heeft severity 1-5 en statussen open / acknowledged / resolved.
Scope	Een cyclus scope: "actieve personen" (default) of "iedereen incl. inactief" (voor jaarlijkse audit).
Snapshot	Een bevroren kopie van de matrix bij cyclus-start. Latere wijzigingen beïnvloeden de cyclus niet.
Systeem	Een app of service waar mensen toegang kunnen hebben. Kan items hebben (voor fijnmazige tracking).
Tenant	De geïsoleerde ruimte van jouw organisatie. Alle AccessGuard-data is gescoped per tenant.
unknown	Cel-status: nooit beslist. Standaard voor nieuwe cellen.
Vault	Versleutelde credential-opslag. Per-gebruiker ACL; elke toegang wordt gelogd.

AccessGuard is een product van Beter Geregeld ICT. Deze handleiding wordt automatisch gegenereerd, de digitale versie op de website is altijd leidend.
Contact: info@betergeregeld.com · Handleiding gegenereerd: 04-07-2026