Informatiebeveiligingsbeleid

Versie 31-10-2026

Control iso27001:A.5.1 in het nalevingsregister; ondersteunt ook clausule 5 (leiderschap), iso27001:A.6.7 (werken op afstand) en iso27001:A.8.24 (cryptografie).

Vastgesteld door de eigenaar op 2-10-2026. Tegelijk aanvaardde de eigenaar de restrisico's die het risicoregister als "aanvaard" behandelt, waaronder één persoon als eigenaar en beheerder en het ontbreken van een externe penetratietest.

Dit is het beleid dat ISO 27001 A.5.1 vraagt: één document waarin staat wat Stilops met informatiebeveiliging wil bereiken, wie waarover beslist, en welke regels gelden. Het is bewust kort en het beschrijft wat er werkelijk gebeurt. Een beleid dat mooier is dan de praktijk is geen beleid maar een wens.

1. Doel en reikwijdte

Stilops levert AI-agents die namens een organisatie werk uitvoeren. Klanten vertrouwen ons daarbij hun bedrijfsgegevens toe, en soms persoonsgegevens van hún relaties. De kern van het product is niet alleen dat het werk gedaan wordt, maar dat achteraf te herleiden is wát er is gebeurd en wie het heeft goedgekeurd.

Dit beleid geldt voor het volledige platform: het klantenportaal, de beheeromgeving, de publieke site, de uitvoering van agent-taken, en de infrastructuur waarop dat draait. Het geldt voor iedereen die eraan werkt — op dit moment de eigenaar — en voor de agents die zelf in de codebase werken.

2. Doelstellingen

1. **Vertrouwelijkheid.** Gegevens van een organisatie zijn niet toegankelijk voor een andere organisatie, en geheimen van gekoppelde systemen staan versleuteld opgeslagen en worden niet aan een agent getoond. Waar een agent een geheim technisch nodig heeft, krijgt hij het alleen voor de duur van die taak; de uitzonderingen staan onder "Cryptografie en sleutelbeheer" en in §5.
2. **Integriteit en herleidbaarheid.** Wat een agent voorstelde, wie het goedkeurde en wat het resultaat was, ligt vast en wordt niet achteraf gewijzigd.
3. **Beschikbaarheid.** De dienst draait, en een storing is herstelbaar zonder verlies van het auditspoor.
4. **Menselijk gezag.** Geen enkel effect zonder een mens die het heeft goedgekeurd.

De vierde is bij Stilops geen beveiligingsmaatregel maar het uitgangspunt van het product. De andere drie zijn er om die vierde geloofwaardig te maken.

3. Wie beslist wat

Onderwerp	Wie
Beleid vaststellen en wijzigen	De eigenaar
Beveiligingsbeoordeling, dreigingsinformatie, incidentanalyse	De CISO-rol
Alles wat een wettelijke verplichting raakt of een publieke uitspraak wordt	De eigenaar, altijd — dit is niet te delegeren en niet per mandaat uit te schakelen
Technische uitvoering, wijzigingen aan de software	De ontwikkelrollen, langs de vaste kwaliteitspoort
Toekennen van bevoegdheden aan een agent	De eigenaar

Dat de eigenaar de enige mens in deze tabel is, is een feit en geen tekortkoming om te verbergen — maar het is wél het grootste enkele risico in het risicoregister, en daar staat het ook als zodanig.

4. Regels die gelden

Toegang. Toegang is op naam en op rol. Wachtwoorden worden opgeslagen als sterke, gezouten hash. Tweestapsverificatie is voor elke gebruiker beschikbaar, en verplicht als extra stap bij handelingen met gevolgen — waaronder het publiek bevestigen van een nalevingsclaim. Er zit een snelheidslimiet op inloggen en op formulieren.

Werkplek en werken op afstand. Stilops heeft geen kantoor; al het beheer gebeurt op afstand, vanaf de werkplek van de eigenaar. Daarvoor gelden deze regels: de schijf van het apparaat is versleuteld en het scherm vergrendelt automatisch na korte inactiviteit; besturingssysteem en browser krijgen beveiligingsupdates zodra ze uitkomen; de accounts bij de code-, hosting-, DNS- en betaalleveranciers zijn beveiligd met tweestapsverificatie; toegang tot servers gaat alleen via SSH-sleutels, niet via wachtwoorden; productiegegevens worden niet naar de werkplek gekopieerd, behalve een tijdelijke kopie voor een herstel of een onderzoek die daarna wordt verwijderd. Bij verlies of diefstal van het apparaat worden binnen 24 uur de sessies beëindigd en de sleutels die erop stonden vernieuwd, en wordt beoordeeld of het een datalek is volgens de Incident- en datalekprocedure.

Geheimen. Geheimen van gekoppelde systemen en van de infrastructuur worden versleuteld opgeslagen (AES-256-GCM) met een sleutel per omgeving, en pas ontsleuteld op het moment dat een taak ze nodig heeft. Ze komen nooit in de opdracht aan het taalmodel. Het per ongeluk meecommitten van een geheim wordt maar deels tegengehouden: een toets in de kwaliteitspoort zoekt in de code naar geheimen met een vast voorvoegsel (zoals GitHub-, Anthropic- en Stripe-sleutels en privésleutels), en dezelfde patronen worden toegepast op wat agents als wijziging indienen. Een geheim zonder herkenbaar voorvoegsel, zoals een Hetzner-token of een wachtwoord, vangt die controle niet. Een gebruiker die een geheim in een chatbericht zet, krijgt dat bericht onderschept vóórdat het model het ziet.

Uitvoering van agent-taken. Een agent-taak draait ingesloten onder een eigen, beperkt account uit een

vaste pool. Zijn er meer gelijktijdige taken dan de pool groot is, dan draait een taak voorlopig onder het gedeelde agent-account, waar een andere gelijktijdige taak zijn ontsleutelde configuratie kan lezen. Dat wordt gedicht. Een agent van een klant krijgt nooit toegang tot gegevens van een andere organisatie, heeft geen mailbox en verstuurt geen e-mail.

Wijzigingen aan de software. Elke wijziging gaat langs een vaste geautomatiseerde poort: stijl, typecontrole, de volledige toetsenset, een controle op meegecommitte geheimen en een controle op bekende kwetsbaarheden in afhankelijkheden. Een wijziging aan een poort of een bevoegdheid moet bovendien met opzet worden gebroken om te bewijzen dat de bijbehorende toets rood wordt — een poort die niet is gebroken, bewaakt niets tot het tegendeel is aangetoond.

Wijzigingen en de naleving. Elke wijziging wordt vóór de samenvoeging ook getoetst op wat zij betekent voor de naleving: raakt zij iets wat een nalevingsdocument, de controls of de voorwaarden beloven? Software bepaalt welke onderwerpen een wijziging raakt; een aparte, alleen-lezende toetsagent beoordeelt dan of de wijziging zo door mag, of een nalevingsdocument mee moet veranderen (dat werkt Stilops zelf bij in dezelfde wijziging, waarna de eigenaar de nieuwe tekst vaststelt), of de eigenaar moet beslissen, of de wijziging wordt tegengehouden. Een wijziging aan de voorwaarden, de privacyverklaring, de verwerkersovereenkomst of de lijst van subverwerkers, een risico dat aanvaard moet worden en een maatregel die zwakker wordt, liggen altijd bij de eigenaar; een toets die niet tot een oordeel komt ook. Daarnaast legt Stilops elk kwartaal alle nalevingsdocumenten naast de code en maakt van elke afwijking een bevinding.

Vastlegging. Handelingen van beheerders en van organisatiegebruikers worden append-only vastgelegd. Een vastgelegde handeling wordt niet gewijzigd en niet verwijderd.

Cryptografie en sleutelbeheer. Verkeer loopt over TLS. Gegevens in rust die een geheim vormen, zijn versleuteld met AES-256-GCM, met twee bekende uitzonderingen: het kortlevende leestoken van de Search Console-koppeling (hoogstens een uur geldig) staat bewust onversleuteld, en de Anthropic-API-sleutel voor klantruns staat tijdens zo'n run, tot twee minuten, als bestand op schijf. De sleutel staat per omgeving buiten de broncode en de database en is alleen leesbaar voor de dienst zelf, op machines waar de agents onder een apart account draaien (een aparte instelling voor dat account). Waar die scheiding niet is ingesteld, zoals op de lokale ontwikkel- en productieomgeving, draaien agents als dezelfde gebruiker als de dienst en kunnen ze de sleutel en de versleutelde waarden allebei lezen.

Wat een agent kan lezen, ook waar de scheiding wél is ingesteld: de Anthropic-API-sleutel tijdens een klantrun; het gewone Cloudflare-token; zolang de lokale tunnel voor geheimen van koppelingen niet aan staat, het ontsleutelde configuratiebestand van een taak; en bij een volle pool ook het configuratiebestand van een andere gelijktijdige taak, met de koppelingsgeheimen van een klant. Waar die tunnel aan staat, komen die geheimen niet in een leesbaar bestand terecht. Ook de database met de gegevens van alle organisaties is leesbaar voor het agent-account, omdat de servers die agents gebruiken hem nodig hebben. Een agent van een klant komt er niet bij: hij heeft dan geen shell, een vaste controle vóór elke handeling beperkt zijn lezen tot zijn eigen werkmap en bijlagen, en de gereedschappen die hij krijgt filteren op zijn organisatie. Die scheiding zit in de applicatie, niet in het besturingssysteem: valt die controle weg, dan houdt het account niets tegen. Dit zijn restrisico's, en het eerste staat in het risicoregister (R13).

Externe toegangssleutels worden vernieuwd voor zover de leverancier dat toelaat. Het Cloudflare-token vernieuwt Stilops zelf. Voor Hetzner, GitHub, Anthropic, Stripe en MXroute maakt Stilops een herinnering als bevinding en vernieuwt de eigenaar de sleutel zelf. Voor de overige koppelingen (S3, OneDrive, VirusTotal, LinkedIn, PageSpeed, Bing, het Google-servicekonto en de SMTP- en IMAP- wachtwoorden) staat geen herinnering klaar; daar geldt alleen de handmatige sleutelrotatie in de operationele planning. Voor Hetzner komt daar een bewaking bij die elke handeling in het actielogboek van Hetzner meldt die niet uit Stilops zelf komt; voor de andere leveranciers bestaat die bewaking niet.

Een sleutelwissel na een (vermoed) lek maakt bestaande publieke nalevingsbevestigingen ongeldig: die moeten dan opnieuw worden gegeven, want wie de oude sleutel had kan ze vervalst hebben. Bij een gewone wissel tekent Stilops elke bevestiging die met de oude sleutel klopte opnieuw met de nieuwe sleutel. Sessies en uitnodigings- en resetlinks vervallen bij elke wissel.

Incidenten. Wat een incident is, hoe het binnenkomt en binnen welke termijn wat aan wie wordt gemeld, staat in de Incident- en datalekprocedure. De beslissing om te melden is menselijk.

Leveranciers. Elke partij die persoonsgegevens verwerkt, staat met naam, doel, land en de stand van de verwerkersafspraak in de Subverwerkerslijst — ook waar die afspraak ontbreekt.

5. Wat dit beleid eerlijk moet toegeven

- **Er is geen functiescheiding.** Eén persoon stelt beleid vast, keurt goed en beheert. De compensatie is dat het auditspoor volledig en append-only is, en dat de zwaarste handelingen een extra verificatiestap vragen. Dat is een compensatie, geen oplossing.
- **Herstel wordt beproefd, maar nog niet volledig.** Het ontsleutelen en controleren van de back-ups is getest; een volledige hersteloefening per kwartaal is ingericht en de eerste uitvoering staat nog open. Details staan in het continuïteitsplan, dat klanten in het portaal kunnen inzien.
- **Geheimen zijn niet voor elke agent onleesbaar.** Zie "Cryptografie en sleutelbeheer": de Anthropic-API-sleutel tijdens een klantrun, het gewone Cloudflare-token, en op machines zonder gescheiden agentaccount ook de sleutel zelf. Het afdichten daarvan is een openstaande afweging.
- **De scheiding tussen organisaties in de database is een scheiding in de applicatie.** De database met de gegevens van alle organisaties is leesbaar voor het agent-account, omdat de servers die agents gebruiken hem nodig hebben. Dat een agent van een klant er niet bij komt, regelt een vaste controle in de applicatie, niet het besturingssysteem: valt die controle weg, dan houdt het account niets tegen.
- **Er is geen externe penetratietest.**

Deze punten staan als open punt in het nalevingsregister. Ze staan hier omdat een beveiligingsbeleid dat alleen de sterke kanten noemt, de lezer misleidt over waar hij op kan rekenen.

6. Naleving en herziening

Het nalevingsregister op stilops.com/nalevingsregister is de doorlopende meting van dit beleid: per norm en per control wat de stand is, met bewijs. Afwijkingen komen binnen als bevinding en worden gerouteerd naar wie erover gaat.

Dit beleid wordt herzien wanneer de organisatie groeit tot meer dan één persoon, wanneer er een nieuwe categorie gegevens of een nieuwe leverancier bijkomt, na een incident met impact, en uiterlijk jaarlijks.

VASTGESTELD

Fabian Dutrieux

CEO · 1 november 2026 · versie 4

Controlecode 195E-6862-65C6. Vastgelegd met tweestapsverificatie in het ondertekeningsregister van Stilops.