Klant-vragenlijst Compliant

Acht business-besluiten voor het inrichten van jullie beveiligings-baseline

DOCUMENT
Klant-vragenlijst Compliant

DATUM
Mei 2026

CLASSIFICATIE
Openbaar

VERSIE
V1.0 · Definitief

Werkwijze

Acht clusters van technische maatregelen, samengevat in één business-besluit per cluster. Per cluster ons advies plus wat dit voor medewerkers en organisatie betekent. Klant kiest: advies volgen of afwijken met reden. Resultaat ligt vast voor MT-archief en audit. Doorlooptijd 2 tot 3 uur, verdeeld over 1 of 2 sessies binnen stap 2 van de onboarding.

Inhoudsopgave

Cluster 1 — Werken met externen

Business-vraag: Hoe vrij of strikt mogen externen (klanten, leveranciers, freelancers) in jullie omgeving werken?

Onze advies-keuze	**Strikt — externen krijgen tijdelijke en gerichte toegang**
Wat dit voor medewerkers betekent	Externen krijgen alleen toegang tot specifieke mappen of Teams-kanalen, niet tot de hele omgeving. Externen kunnen geen documenten of mappen doorzetten naar hun eigen contacten. Toegang vervalt automatisch na 90 dagen of bij afsluiting van de samenwerking. Externe gasten zien niet wie er allemaal in jullie organisatie werkt.
Praktische gevolgen	Per externe partner een aanvraag voor toegang via vaste flow. Bij langdurige samenwerking: toegang verlengen, geen permanente status.
Waarom dit advies	Bij Compliant moet aantoonbaar zijn waar bedrijfsdata terechtkomt. Wijd-open externe deling laat data buiten zicht raken.
Wat we technisch regelen	■ Beperken extern delen tot vooraf goedgekeurde domeinen. **Resultaat:** Externe partner krijgt alleen toegang, andere domeinen vallen buiten. ■ Voorkomen dat externen documenten doorzetten naar derden. **Resultaat:** Wat bij de externe ligt blijft daar, gaat niet weer een schakel verder. ■ Maken gast-toegang automatisch vervallen na 90 dagen. **Resultaat:** Vergeten externe gasten verzamelen zich niet op met nog actieve toegang.

	■ Voorkomen dat gasten andere medewerkers of gasten zien. **Resultaat:** Externe partij kan jullie organisatiestructuur niet uitlezen voor phishing. ■ Sluiten doorsturen van mail naar externe adressen af. **Resultaat:** Een gehackt account kan niet ongezien jullie mailbox naar buiten kopiëren. ■ Geven externe afzenders een zichtbare 'extern'-melding in Outlook. **Resultaat:** Medewerker herkent direct of mail van een collega is of niet.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 2 — Inloggen en wachtwoorden

Business-vraag: Hoe streng moet inloggen voor medewerkers en admins zijn?

Onze advies-keuze	**Strikt — Microsoft Authenticator-app voor iedereen, hardware-key voor admins**
Wat dit voor medewerkers betekent	Iedere medewerker logt in met wachtwoord plus Authenticator-app op telefoon. SMS, voice of e-mail als tweede stap is niet meer mogelijk. Admins en directie gebruiken bovenop dat een hardware-key (FIDO2) of Windows Hello. Inloggen vanuit niet-toegestane landen of locaties wordt geblokkeerd.
Praktische gevolgen	Iedere medewerker installeert Authenticator-app tijdens onboarding. Voor admin-rol: hardware-key aanschaf (50-100 euro per persoon). Medewerker zonder smartphone krijgt FIDO2-key als alternatief.
Waarom dit advies	Wachtwoord-alleen is geen bescherming meer. Zwakke tweede-stap-methodes (SMS, voice) worden actief aangevallen. Voor admin-accounts is de schade bij compromittering te groot voor reguliere MFA.
Wat we technisch regelen	■ Eisen Authenticator-app als tweede stap voor alle medewerkers. **Resultaat:** Gestolen wachtwoord alleen is niet meer genoeg om binnen te komen. ■ Blokkeren SMS, voice en e-mail als tweede-stap-methode. **Resultaat:** Aanvaller met sim-swap of doorgestuurde mail komt geen stap verder. ■ Verplichten hardware-key (FIDO2) voor admin-accounts. **Resultaat:** Phishing van admin-wachtwoorden levert geen toegang op. ■ Tonen locatie en app-naam bij elke inlog-prompt. **Resultaat:** Medewerker ziet een vreemde locatie en weigert direct. ■ Blokkeren oude inlogmethoden zonder tweede-stap-support. **Resultaat:** Aanvalsroutes uit pre-MFA-tijdperk zijn dicht. ■ Houden specifieke wachtwoorden (bedrijfsnaam, sector-jargon) verboden. **Resultaat:** Voorspelbare wachtwoorden worden bij wijziging geweigerd.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 3 — Apparaten en thuiswerken

Business-vraag: Waar mogen medewerkers werken met bedrijfsdata?

Onze advies-keuze	**Strikt — alleen beheerde bedrijfsapparaten**
Wat dit voor medewerkers betekent	Privé-iPhone of -laptop heeft geen toegang tot bedrijfsmail, Teams, SharePoint of OneDrive. Alleen bedrijfslaptops en bedrijfs-telefoons werken voor bedrijfsapps. Bij verlies of diefstal van een bedrijfsapparaat wissen wij het op afstand zodra wij de melding krijgen. Nieuwe medewerker krijgt eerst apparaat voor toegang.
Praktische gevolgen	Hardware-budget per medewerker (1 laptop + 1 telefoon). Bij thuiswerk-rol: bedrijfslaptop mee naar huis. Vakantie-bereikbaarheid alleen via bedrijfsapparaat. Voor seizoens-stagiairs of bezoekers met data-toegang: tijdelijke werkplek of bewust geen toegang.
Waarom dit advies	Bij Compliant is aantoonbaar nodig waar bedrijfsdata staat. Privé-apparaten vallen buiten ons beheer, dus daar is geen garantie op te geven.
Wat we technisch regelen	■ Sluiten apparaten af die niet onder beheer staan. **Resultaat:** Privé-laptop op terras komt er niet in. ■ Versleutelen elke bedrijfslaptop en -Mac. **Resultaat:** Gestolen apparaat is een baksteen. ■ Eisen pincode plus actuele beveiliging op elk bedrijfsapparaat. **Resultaat:** Gevonden telefoon zonder pincode bestaat niet. ■ Wissen apparaten op afstand bij verlies of vertrek. **Resultaat:** Bedrijfsdata is weg voor iemand het kan openen. ■ Blokkeren automatisch een apparaat met virus. **Resultaat:** Eén besmette laptop verspreidt het niet. ■ Ruimen inactieve apparaten op na 6 maanden. **Resultaat:** Oude rommel-apparaten zijn geen achterdeur.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 4 — E-mail beveiliging

Business-vraag: Welk beschermingsniveau willen jullie op e-mail tegen phishing en datalek?

Onze advies-keuze	**Strikt — volledige Defender-suite plus zichtbare extern-melding**
Wat dit voor medewerkers betekent	Iedere binnenkomende link en bijlage wordt vooraf gescand. Verdachte mail belandt in quarantaine. Externe afzenders krijgen een zichtbare 'extern'-banner. Mail van vermeende bekenden (CEO-fraude) wordt herkend en gewaarschuwd. Add-ins voor Outlook installeren door medewerkers zelf is niet meer mogelijk. Automatische doorsturing naar externe ontvangers is uit.
Praktische gevolgen	Bijlagen komen 1-3 minuten later binnen door scan-vertraging. Sommige nieuwsbrieven landen in quarantaine en moeten naar whitelist. Bestaande Outlook-add-ins centraal bij IT in beheer.
Waarom dit advies	E-mail is nog steeds de belangrijkste route voor aanvallen en datalekken. Zonder deze laag is een gehackt account ongezien een data-uitstroom.
Wat we technisch regelen	■ Scannen bijlagen vóór aflevering in een veilige testomgeving. **Resultaat:** Onbekende bijlage doet eerst niks bij de medewerker zelf. ■ Scannen links op het moment dat erop geklikt wordt. **Resultaat:** Aanvallers die link na verzending wijzigen, vangen wij alsnog op. ■ Tonen 'extern'-banner bij elke mail van buiten. **Resultaat:** Medewerker ziet direct of een mail van een collega is. ■ Voorkomen automatische doorsturing naar externe adressen. **Resultaat:** Gehackt account kan niet ongezien mailbox naar buiten kopiëren. ■ Blokkeren eigen installatie van Outlook-add-ins. **Resultaat:** Schadelijke add-in krijgt geen toegang tot mailbox-inhoud. ■ Vangen mail die zich voordoet als directie of leverancier (CEO-fraude). **Resultaat:** Vermeende mail van de baas met betaal-verzoek wordt herkend.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 5 — Data binnen houden

Business-vraag: Waar mag bedrijfsdata opgeslagen worden?

Onze advies-keuze	**Strikt — alleen in jullie Microsoft 365-omgeving, niet in privé-clouds**
Wat dit voor medewerkers betekent	Dropbox, Google Drive, Box en persoonlijke OneDrive zijn niet meer bereikbaar vanuit Office of Outlook Web. Nieuwe SharePoint-sites kunnen alleen door IT of een aangewezen sitemanager aangemaakt worden. Spontane Teams-aanmaak door medewerkers is uit, gaat via aanvraag.
Praktische gevolgen	Medewerkers met privé-cloud-flow moeten overschakelen naar SharePoint of OneDrive. Aanvraag-flow nodig voor nieuwe sites of Teams. Per branche-software apart bekijken of cloud-integratie noodzakelijk is.
Waarom dit advies	Voor Compliant moet duidelijk zijn waar bedrijfsdata leeft. Versnipperde opslag in privé-clouds is niet beheersbaar en niet auditbaar.
Wat we technisch regelen	■ Sluiten privé-clouds (Dropbox, Google Drive, persoonlijke OneDrive) af binnen Office. **Resultaat:** Bedrijfsdata kan niet ongezien naar privé-account verschuiven. ■ Voorkomen dat medewerkers nieuwe SharePoint-sites aanmaken. **Resultaat:** Wildgroei aan ongoverneerde sites blijft uit. ■ Voorkomen dat medewerkers spontaan Teams aanmaken. **Resultaat:** Voor elk nieuw Team een bewuste keuze, geen rommel-Teams. ■ Beperken delen via Teams tot goedgekeurde cloud-storage. **Resultaat:** Bestanden delen in Teams loopt via SharePoint, niet via Dropbox-link. ■ Blokkeren downloaden van besmette bestanden uit SharePoint. **Resultaat:** Geïnfecteerd bestand verspreidt zich niet via download-en-mail-keten.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 6 — Hoe vrij is de gebruiker

Business-vraag: Hoeveel mag een medewerker zelf doen zonder tussenkomst van IT?

Onze advies-keuze	**Strikt — IT bepaalt wat mag, gebruiker werkt binnen kaders**
Wat dit voor medewerkers betekent	Medewerkers kunnen geen apps installeren die jullie data willen lezen zonder admin-goedkeuring. Geen self-service voor Microsoft-licenties via bedrijfsrekening. Sessie in een webapp sluit na 1 uur inactiviteit automatisch af. Geen mogelijkheid om een nieuwe Microsoft-tenant aan te maken.
Praktische gevolgen	App-installaties lopen via aanvraag-flow (uren tot dagen). Licentie-aanvraag via IT. Vaker opnieuw inloggen bij lange documenten. Voor ontwikkelaar- of consultant-rollen die wel apps moeten registreren: uitzondering instellen.
Waarom dit advies	OAuth-phishing en self-service-misbruik zijn aanvalsroutes die zonder restrictie open staan. Bij Compliant is afgesproken kader nodig om controle te bewaren.
Wat we technisch regelen	■ Eisen admin-goedkeuring voor apps die bij mailbox of bestanden willen. **Resultaat:** Phishing-app krijgt geen toegang ook al klikt medewerker akkoord. ■ Voorkomen self-service licentie-aanvraag op bedrijfsrekening. **Resultaat:** Geen onverwachte facturen voor ongebruikte licenties. ■ Voorkomen aanmaak van een nieuwe tenant door medewerkers. **Resultaat:** Geen schaduw-omgeving naast jullie hoofd-omgeving. ■ Sluiten webapp automatisch na 1 uur zonder activiteit. **Resultaat:** Onbewaakte laptop in publieke ruimte vergeet niets meer. ■ Tonen melding 'verdachte activiteit' in Authenticator-app. **Resultaat:** Medewerker kan ongeziene inlog-pogingen direct melden.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 7 — Logging, opruimen en bewijslast

Business-vraag: Wat leggen we vast en hoe streng ruimen we op?

Onze advies-keuze	**Strikt — alles loggen, inactieve accounts en apparaten automatisch opruimen**
Wat dit voor medewerkers betekent	Alle activiteit in Microsoft 365 wordt gelogd (vereist voor audit). Gast-accounts die 90 dagen niet inloggen worden geblokkeerd. Apparaten die 6 maanden niet zien zijn worden uit de registratie verwijderd. Bij elke beveiligings-melding kan precies achterhaald worden wie wat gedaan heeft.
Praktische gevolgen	Vergeten gast-account moet opnieuw uitgenodigd worden bij hervatting. Bij elk incident: audit-rapport beschikbaar. Per kwartaal of half jaar: rapport voor auditor of MT.
Waarom dit advies	Zonder logging is forensisch onderzoek bij een incident onmogelijk. Zonder opruimen verzamelen zich oude toegangsmomenten die een achterdeur worden.
Wat we technisch regelen	■ Loggen alle activiteit in Microsoft 365 standaard. **Resultaat:** Bij incident is precies na te gaan wie wat gedaan heeft. ■ Blokkeren gast-accounts na 90 dagen zonder activiteit. **Resultaat:** Vergeten gasten zijn geen openstaande deur meer. ■ Verwijderen inactieve apparaten na 6 maanden. **Resultaat:** Verloren laptop met nog werkende inlog-tokens bestaat niet. ■ Verzamelen Defender-signalen van elk apparaat centraal. **Resultaat:** Bij verdacht gedrag op één laptop is meteen heel het netwerk-beeld zichtbaar. ■ Beschermen Defender zelf tegen uitschakelen door malware. **Resultaat:** Aanvaller die anti-virus probeert uit te zetten krijgt geen kans. ■ Houden gebruikersnamen leesbaar in rapportages (niet pseudo-anoniem). **Resultaat:** Compliance-rapport is direct bruikbaar, geen vertaalslag nodig.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Cluster 8 — Anti-phishing herkenning en uitstraling

Business-vraag: Hoe maken we zichtbaar dat een inlog-pagina echt van jullie is?

Onze advies-keuze	**Strikt — eigen branding op Microsoft-inlogpagina, plus volledige DMARC en DKIM**
Wat dit voor medewerkers betekent	Bij elke inlog op Microsoft 365 zien medewerkers jullie eigen logo en achtergrond. Mail die zogenaamd van jullie domein komt maar niet legitiem is, wordt door ontvangende mailservers afgewezen. Eén centraal IT-contactadres ontvangt updates en waarschuwingen van Microsoft.
Praktische gevolgen	Logo, achtergrond en huisstijlkleur aanleveren (eenmalig). Centraal IT-mailadres instellen (bijvoorbeeld ict@jouwbedrijf.nl). Indien geen huisstijl-elementen beschikbaar: los te bestellen als aparte opdracht.
Waarom dit advies	Inlog-pagina van Microsoft ziet er overal hetzelfde uit. Met eigen branding herkent medewerker direct of een inlog-pagina echt van jullie is. DKIM en DMARC voorkomen dat aanvallers mails versturen alsof het van jullie komt.
Wat we technisch regelen	■ Tonen jullie logo en achtergrond op Microsoft-inlogpagina. **Resultaat:** Medewerker ziet direct of het echte jullie-pagina is of een nep. ■ Voorkomen verzending van mail die zich voordoet als jullie domein. **Resultaat:** Klanten en partners krijgen geen vervalste mail uit jullie naam. ■ Versleutelen uitgaande mail met digitale handtekening (DKIM). **Resultaat:** Ontvangende mailserver kan checken of mail echt van jullie komt. ■ Vernieuwen versleutel-sleutels naar moderne standaard. **Resultaat:** Oudere sleutels zonder voldoende sterkte zijn vervangen. ■ Sturen één centraal IT-adres alle Microsoft-meldingen. **Resultaat:** Updates en waarschuwingen landen op één plek, niet bij één persoon.
Volgen jullie ons advies	☐ Ja ☐ Nee
Reden bij nee	_____
Akkoord namens jullie organisatie	Naam: _____ Datum: _____

Vaste keuzes (geen klant-besluit)

Deze maatregelen liggen altijd vast in Compliant, daar is geen keuze in:

- Lokaal admin-wachtwoord-beheer op alle Windows-apparaten (LAPS).
- Authenticator-app als tweede stap voor inloggen.
- Gasten vanuit andere organisaties mogen hun eigen MFA gebruiken voor toegang.
- Standaard-tijdzone Europe/Amsterdam.

Niet meer in gebruik bij Compliant:

Security Defaults en per-user-MFA. Beide vervangen door fijnmazige Conditional Access uit cluster 2.