Wat moet ik doen met de ICT-toegang van een vertrekkende medewerker?

https://aucuba.nl/kennisbank/uncategorized/wat-moet-ik-doen-met-de-ict-toegang-van-een-vertrekkende-medewerker/

Bij een vertrekkende medewerker moet je direct alle ICT-toegangen intrekken op de laatste werkdag, of bij voorkeur al op het moment dat het dienstverband officieel eindigt. Denk aan e-mailaccounts, cloudopslag, bedrijfssystemen en externe toegang via VPN. Hoe sneller je handelt, hoe kleiner het risico op datalekken of misbruik van bedrijfsinformatie. In dit artikel beantwoorden we de meest gestelde vragen rondom ICT-offboarding, zodat je precies weet wat er moet gebeuren en wanneer.

Welke accounts en toegangen moet je direct afsluiten?

Bij een vertrekkende medewerker sluit je op de laatste werkdag minimaal de volgende toegangen af: het e-mailaccount, inloggegevens voor bedrijfssystemen en software, cloudopslagdiensten zoals Microsoft 365 of Google Workspace, VPN-toegang, en eventuele fysieke toegangspassen of codes. Dit zijn de meest kritieke toegangspunten die directe risico's vormen als ze open blijven staan.

Naast deze basisaccounts zijn er vaak ook minder zichtbare toegangen die over het hoofd worden gezien. Denk aan accounts voor projectmanagementsoftware, CRM-systemen, boekhoudpakketten, externe portalen van klanten of leveranciers, en gedeelde wachtwoorden die de medewerker kende. Ook toegang tot socialmedia-accounts van het bedrijf of gedeelde mailboxen valt hieronder.

Een gestructureerde aanpak is essentieel. Maak bij het offboardingproces gebruik van een volledige inventarisatie van alle systemen waartoe de medewerker toegang had. Zonder zo'n overzicht is de kans groot dat er ergens een toegangsdeur openblijft die later problemen veroorzaakt.

Wat gebeurt er als je ICT-toegang niet tijdig intrekt?

Als je de ICT-toegang van een vertrekkende medewerker niet tijdig intrekt, loop je als bedrijf aanzienlijke risico's op het gebied van gegevensveiligheid, privacywetgeving en

bedrijfscontinuïteit. Een voormalige medewerker kan bewust of onbewust toegang houden tot gevoelige klantdata, bedrijfsgeheimen of financiële informatie.

Vanuit de Algemene Verordening Gegevensbescherming (AVG) ben je als organisatie verplicht om toegang tot persoonsgegevens te beperken tot uitsluitend degenen die daar een actieve reden voor hebben. Blijft een vertrokken medewerker toegang houden, dan kan dit bij een datalek leiden tot een meldplicht bij de Autoriteit Persoonsgegevens en mogelijke boetes.

Daarnaast is er het praktische risico van misbruik. In de meeste gevallen is dit niet kwaadwillig bedoeld, maar de mogelijkheid bestaat. Een medewerker die vertrekt naar een concurrent met toegang tot klantlijsten of offertehistorie vormt een reëel bedrijfsrisico. Tijdig handelen is dan ook geen formaliteit, maar een noodzakelijke beveiligingsmaatregel.

Hoe lang mag een vertrekkende medewerker nog toegang hebben?

Een vertrekkende medewerker mag in principe alleen toegang hebben zolang het dienstverband actief is. Op de laatste officiële werkdag, of op het moment van het einde van het contract, moeten de toegangsrechten worden ingetrokken. In sommige gevallen kan een korte overgangsperiode worden afgesproken, maar dit vereist expliciete toestemming en een duidelijk omschreven doel.

Er zijn situaties waarbij een tijdelijke uitzondering logisch lijkt, bijvoorbeeld als een medewerker nog lopende projecten afrondt of kennisoverdracht verzorgt. In dat geval is het verstandig om de toegang te beperken tot alleen de systemen die strikt noodzakelijk zijn voor die overdracht, en een harde einddatum vast te leggen.

Vanuit de **ICT-beveiliging bij uitdiensttreding** geldt als vuistregel: hoe korter de toegangsperiode na de laatste werkdag, hoe beter. Onbeperkte of ongedefinieerde toegang na vertrek is in alle gevallen onwenselijk en brengt onnodige risico's met zich mee.

Wat doe je met de e-mail en bestanden van een vertrokken medewerker?

De e-mail en bestanden van een vertrokken medewerker bewaar je tijdelijk in een gearchiveerde vorm, zodat lopende communicatie en documenten toegankelijk blijven voor de organisatie. Het account zelf wordt geblokkeerd voor de gebruiker, maar de inhoud wordt niet direct verwijderd.

Hoe lang je dit bewaart, hangt af van wettelijke bewaarplichten en interne afspraken.

E-mailafhandeling na vertrek

Stel op de laatste werkdag een automatische afwezigheidsmelding in die inkomende berichten doorstuurt naar een collega of een algemeen bedrijfsadres. Zo mis je geen belangrijke klantcommunicatie. Afhankelijk van de functie is het ook verstandig om inkomende e-mails gedurende een afgesproken periode door te sturen naar een leidinggevende of opvolger.

Beheer van bestanden en documenten

Bestanden die de medewerker heeft aangemaakt of beheerd, vallen onder het eigendom van de organisatie. Zorg dat deze tijdig worden overgedragen aan een verantwoordelijke collega of worden opgeslagen in een centrale, gedeelde omgeving. Persoonlijke bestanden die niets met het werk te maken hebben, kunnen in overleg worden teruggegeven of verwijderd. Documenteer altijd wat er is gedaan met de data, zodat je dit kunt aantonen als dat ooit nodig is.

Wie is verantwoordelijk voor de ICT-offboarding binnen een bedrijf?

De verantwoordelijkheid voor ICT-offboarding ligt gezamenlijk bij HR, de directe leidinggevende en de ICT-beheerder of externe ICT-partner. HR signaleert het vertrek en initieert het proces, de leidinggevende geeft aan welke systemen relevant zijn, en de ICT-beheerder voert de technische acties uit. Zonder duidelijke taakverdeling vallen er snel dingen tussen wal en schip.

In veel MKB-bedrijven zonder interne IT-afdeling is de externe ICT-partner de aangewezen partij om de technische offboarding te coördineren. Zij hebben het overzicht over alle systemen, accounts en toegangsrechten en kunnen snel en gestructureerd handelen. Wij nemen deze rol bij onze klanten actief op ons, zodat niets over het hoofd wordt gezien.

Belangrijk is dat de verantwoordelijke persoon of partij tijdig wordt geïnformeerd over het vertrek van een medewerker, bij voorkeur ruim voor de laatste werkdag. Zo is er voldoende tijd om alles zorgvuldig voor te bereiden en af te ronden.

Hoe stel je een vaste ICT-offboarding checklist op?

Een vaste ICT-offboarding checklist stel je op door alle systemen, toegangen en apparaten in kaart te brengen die een medewerker binnen jouw organisatie kan gebruiken, en deze te vertalen naar

concrete actiepunten die bij elk vertrek worden doorlopen. Een goede checklist is volledig, herhaalbaar en afgestemd op jouw specifieke ICT-omgeving.

Een effectieve checklist bevat minimaal de volgende onderdelen:

- Blokkeren van het e-mailaccount en instellen van een automatische doorstuurmelding
- Intrekken van toegang tot bedrijfssoftware, cloudplatforms en interne systemen
- Deactiveren van VPN-toegang en andere externe verbindingen
- Innemen van bedrijfsapparatuur zoals laptop, telefoon en toegangspas
- Overdragen van bestanden, projecten en klantcontacten aan een collega
- Wijzigen van gedeelde wachtwoorden die de medewerker kende
- Verwijderen of archiveren van het account conform het bewaarbeleid
- Documenteren van alle uitgevoerde stappen

Koppel de checklist aan het HR-proces, zodat de ICT-offboarding automatisch in gang wordt gezet zodra een vertrek bekend is. Evalueer de lijst minimaal jaarlijks en pas hem aan als er nieuwe systemen worden toegevoegd aan de ICT-omgeving. Een goede checklist is nooit af, maar groeit mee met je organisatie.

Wil je zeker weten dat de ICT-offboarding in jouw bedrijf goed is geregeld en niets over het hoofd wordt gezien? Neem dan contact met ons op. We helpen je graag bij het opstellen van een waterdicht offboardingproces dat past bij jouw organisatie.