# Zakelijk gebruik van iPhones en iPads

Elke organisatie die haar medewerkers faciliteert met een iPad of iPhone, staat voor de beslissing hoe om te gaan met het Apple ID. Het Apple ID is de grootste uitdaging bij het inzetten van Apple in een zakelijke omgeving. In dit whitepaper leggen we eerst uit wat het Apple ID precies is en waarom de opzet van het Apple ID diepgaande gevolgen heeft voor het zakelijk inzetten van Apple. Vervolgens geven we aan welke beslissingen genomen moeten worden om o.a. eigenaarschap, privacy, aansprakelijkheid en beveiliging goed te regelen in een beleid.

**“Het Apple ID is de grootste uitdaging bij het inzetten van Apple in een zakelijke omgeving.”**

## Het Apple ID

Voor een optimale gebruikerservaring van ‘iApparaten’ is een persoonlijk Apple ID nodig. Een Apple ID geeft toegang tot talloze diensten, zoals de Appstore, de iCloud en iMessage. Het is echt een persoonlijke identiteit zoals deze bij Apple bekend is. Volgens Apple moet iedereen een eigen Apple ID hebben.

Een Apple ID is niet statisch: een gebruiker is vrij om op elk moment bijvoorbeeld het primaire emailadres te wijzigen evenals andere gegevens. Apple moedigt gebruikers ook aan om het emailadres te wijzigen op het moment dat zij een bedrijf, organisatie of opleidingsinstituut verlaten of van provider wisselen.

### Het Apple ID is ontworpen voor individuen

Het Apple ID, en daarmee ook de apparaten zelf, zijn in de basis ontworpen voor individuen. Apple stimuleert gebruikers om slechts één Apple ID te gebruiken voor alle activiteiten met Apple-producten. Desondanks laten de meeste, maar niet alle, diensten, apparaten en apps het toe om verschillende Apple ID’s te gebruiken.

Apple staat niet toe dat Apple ID’s worden samengevoegd of gesplitst. Het is bedacht voor individuen en niet voor een compleet gezin, klaslokaal of bedrijf. Vanuit de consument gezien kan dit soms verwarrend en restrictief overkomen.

# Aandachtspunten in relatie tot het Apple ID

## Het eigendomsvraagstuk

Bij het zakelijk inzetten van Apple wordt een zakelijk toestel verbonden aan een privé-Apple ID. Dit komt feitelijk neer op het overdragen van het eigenaarschap omdat het gebruikers in staat stelt om eigen apps en andere inhoud op het apparaat te plaatsen, ook apps die een potentiële bedreiging voor de integriteit van het apparaat vormen. Deze inbreuk op de integriteit kan in potentie ook worden overgedragen op de integriteit van het bedrijfsnetwerk als geheel.

**“Door het Apple ID worden apps eigendom van de gebruiker, en niet van de organisatie.”**

Tot op de dag van vandaag betekent het beschikbaar stellen van apps aan gebruikers op hun iApparaten dat deze apps hun eigendom worden omdat ze verbonden zijn aan het Apple ID van de gebruiker. In de praktijk betekent dit dat zij bij het verlaten van de organisatie, deze apps meenemen.

De introductie van Apple van het Volume Purchase Programma brengt hier verandering in. Dit programma wordt eerst echter uitgerold in de VS dus voorlopig is dit in Nederland nog niet beschikbaar. Met dit programma is een organisatie in staat om apps te kopen, te installeren en weer te verwijderen van het toestel van de eindgebruiker, zonder dat het Apple ID van de gebruiker bekend hoeft te zijn. Op deze manier hoeven gebruikers hun Apple ID niet te delen met de IT afdeling. Een hele slimme zet van Apple om de privacy en veiligheid rondom de persoonlijke informatie van de eindgebruikers te waarborgen.

## Privacy

Deze bescherming is hard nodig, want Apple ID is geassocieerd met een enorme lijst van Apple diensten waar gebruikers gebruik van moeten en willen maken: iTunes, iBooks, iCloud, App Store, apparaat activeringen, het Activeringsslot in iOS 7 maar ook communicatietoepassingen zoals iMessage, FaceTime en Zoek-mijn-vrienden. Sommige van deze diensten zijn bovendien gekoppeld aan meer vertrouwelijke informatie zoals creditcardgegevens en in de iCloud-sleutelhanger staan alle gebruikersnamen, pincodes en wachtwoorden opgeslagen en krijg je toegang tot allerlei online diensten. Voeg daaraan toe dat gebruikers met een Apple ID ook toegang krijgen tot hun Mac en van daaruit gebruikmaken van de netwerk-resources en het is wel duidelijk dat het Apple ID echt een onmisbaar en zeer persoonlijk onderdeel is van het gebruik van zo’n apparaat.

Deze diepe integratie van een Apple ID in het Apple ecosysteem stelt een IT afdeling voor een aardige uitdaging bij het activeren van bedrijfsapparaten, het ondersteunen van BYOD-apparaten en het management van de soft- en hardware-voorraad van ongeacht welke Apple-oplossing.

**“Deze diepe integratie van een Apple ID in het Apple ecosysteem stelt een IT afdeling voor een aardige uitdaging.”**

### Mobile Device Management

Met het Volume Purchase Programma wordt de privacy van de gebruiker beschermd. Met Mobile Device Management worden de bedrijfsgegevens beschermd.

IOS 7 maakt onderscheid tussen apps die centraal beheerd en verspreid worden via Mobile Device Management tools, en apps die van de gebruiker zijn. Verschillende Entreprise Device Management oplossingen stellen IT in staat om apps te installeren buiten de gebruiker om.

Via verschillende policies is een mate van bescherming mogelijk. IT afdelingen kunnen wachtwoordregels instellen, vertrouwde certificaten instellen en bepalen of zij Clouddiensten toestaan.

### Verantwoordelijkheid

Het Apple ID maakt iApparaten ook fraudegevoelig, omdat aan het Apple ID veel gegevens gekoppeld zijn. Bij verlies of diefstal van het iApparaat en de mogelijke fraude die dat als gevolg heeft, ontstaat dan ook de vraag van verantwoordelijkheid. Is het bedrijf aansprakelijk te houden omdat het gevoerde beveiligingsbeleid onvoldoende is gebleken om het apparaat of de inhoud ervan te beveiligen, of is de gebruiker zelf aansprakelijk, omdat deze onvoldoende maatregelen heeft genomen om het hem of haar toevertrouwde apparaat te beschermen?

## Het Activeringsslot

Met iOS 7, Zoek-mijn-iPhone en het Activeringsslot wordt er nog een belangrijk aspect toegevoegd aan het vraagstuk van verantwoordelijkheid en eigenaarschap. Bij het activeren van Zoek-mijn-iPhone wordt het Activeringsslot ingeschakeld. Wanneer dit slot eenmaal is ingeschakeld, kan het apparaat niet meer opnieuw geactiveerd worden zonder de invoer van het oorspronkelijk gebruikt Apple ID en het bijbehorend wachtwoord. Dit is een effectief anti-diefstalslot gebleken.

Er zijn ook MDM-systemen waarmee een iApparaat op afstand geblokkeerd en gewist kan worden, maar deze systemen kunnen niet verhinderen dat het apparaat opnieuw geactiveerd kan worden en daarmee blijven het gewilde objecten om gestolen te worden. Het Activeringsslot maakt hier een eind aan. Het is in dat oogpunt een goede keuze, maar het impliceert ook dat een werknemer die het bedrijf verlaat, zijn wachtwoord moet achterlaten zodat het apparaat opnieuw geactiveerd kan worden voor een volgende gebruiker. Maar hiermee geeft de oud-werknemer ook toegang tot het Apple ID en de daaraan gekoppelde gegevens. Is het wachtwoord om welke reden dan ook niet meer te achterhalen, dan is het apparaat alleen nog geschikt voor de prullenbak. Ook Apple kan het apparaat dan niet meer herstellen.

**“Het Apple ID maakt iApparaten ook fraudegevoelig, omdat aan het Apple ID veel gegevens gekoppeld zijn.”**

Apple geeft aan dat het gebruik van Zoek-mijn-iPhone/iPad/Mac uitsluitend bedoeld is voor persoonlijk gebruik. Bij apparaten die zijn geconfigureerd met Apple’s Configurator is de functie niet te activeren, hetgeen Apple’s bedoelingen op dit vlak nog eens onderstreept. Deze en andere aspecten maken een beleid met een set van spelregels omtrent het bezit van en de omgang met een iApparaat noodzakelijk.

## Het delen van een iApparaat

Er zijn situaties denkbaar waarin een persoonlijk Apple ID niet voldoet of gewenst is. Dat geldt voor omgevingen waar iApparaten gedeeld worden, bijvoorbeeld op scholen, in de horeca en in ziekenhuizen. In deze omgevingen zijn de apparaten niet bedoeld om privé-apps of eigen content te bevatten. Deze apparaten worden gebruikt in een gecontroleerde omgeving waar IT verantwoordelijk is voor de uitrol en bepaalt wat ermee gedaan mag worden.

### Combinaties

Bij het ontwikkelen van het Apple ID is rekening gouden met verschillende scenario's. Zo is het mogelijk om een combinatie te maken van twee Apple ID's. Een iPhone (of iPad) gebruikt een Apple ID op verschillende manieren: voor activatie, voor iCloud en voor de App Store. Met twee Apple ID's kun je variëren: een zakelijk ID voor de activatie en een privé ID voor iCloud en App Store.

**"Technisch kan veel opgelost worden, maar een aantal aspecten zul je van tevoren moeten vastleggen."**

## Beleid

Er zijn verschillende scenario's denkbaar en er kan altijd wel een oplossing worden gevonden. Maar er zijn afspraken nodig tussen werknemer en werkgever. Technisch kan veel opgelost worden, maar een aantal aspecten zul je van tevoren moeten vastleggen in een gebruikersovereenkomst. Vaste onderdelen daarin kunnen zijn:

- Aansprakelijkheid bij verlies of diefstal ten aanzien van gegevens, creditcardgegevens en content
- Het waarborgen van de privacy in relatie tot het gebruik van een persoonlijk Apple ID
- Verantwoordelijkheden gebruikers in de omgang met gegevens en wachtwoorden als er geen beperkingen worden opgelegd
- Afspraken rondom het Activeringsslot als gebruikers een privé Apple ID gebruiken en dit slot dus zelf kunnen bedienen

Kortom, het is meer een kwestie van intern afstemmen en het opstellen van een beleid en bijpassende gebruikersovereenkomst dan van een technische oplossing. Daarom ligt een dergelijk beleid zeker niet primair bij de afdeling IT, maar zijn er meerdere interne partijen bij betrokken, zoals de afdeling HR, juridische zaken en het management.

## Conclusie

Apple biedt apparaten van goede kwaliteit en het heeft ook een zekere cultstatus. Het Apple ID is echter een uitdaging bij het zakelijk inzetten van Apple. Aan het Apple ID zijn veel (privé) gegevens gekoppeld en het zit diep geïntegreerd in het Apple ecosysteem, wat extern beheer bemoeilijkt. Er zijn oplossingen mogelijk, daarvoor moeten er eerst een aantal beslissingen worden genomen omtrent eigenaarschap, privacy, beveiliging en verantwoordelijkheid. Deze afspraken tussen werkgever en werknemer worden vastgelegd in een beleid.

## Waarom WCS TeleAdvies

**“Heldere communicatie, duidelijke werkafspraken en goede bereikbaarheid zijn essentieel voor het succes van elke organisatie.”**

WCS TeleAdvies geeft samenwerking vorm. Dit doen wij door samen met onze klanten een communicatie-omgeving in te richten die perfect is afgestemd op de strategie, kernactiviteiten en werkprocessen binnen de organisatie. Ook bieden wij praktische gereedschappen om de visie over klantcontact en bereikbaarheid te vertalen naar de juiste houding en kennis van medewerkers. Heldere communicatie, duidelijke werkafspraken en goede bereikbaarheid zijn essentieel voor het succes van elke organisatie. Neem gerust contact op voor meer informatie of een vrijblijvende kennismaking. Wij zijn u graag van dienst!

**Wilco Smit, Business Consultant**
**WCS TeleAdvies B.V. | Stemerdingweg 5 | Soesterberg**
**0346 - 350808 | www.wcsteleadvies.nl | info@wcsteleadvies.nl**