



Ontwikkeling BYOD beleid



Niet alleen de generaties Y en Z zijn als het ware vergroeid met de smartphone en tablet als onverbreekelijk onderdeel van het dagelijkse functioneren. Ook steeds meer dertigers, veertigers en vijftigers gebruiken deze devices voor andere, meer innovatieve, functies dan alleen maar telefonie of communicatie via SMS berichten.

De 30 plussers zijn nog opgegroeid in de periode van de desktop PC en laptop als belangrijkste IT device en kunnen er daarom mee leven dat werkgevers verlangen dat deze (door de werkgever beschikbaar gestelde) devices moeten worden gebruikt voor de zakelijke doeleinden. Naast de smartphone of tablet voor privé doeleinden.

digitaal persoonlijk verlengstuk

De generaties Y en Z daarentegen zijn opgegroeid met de eigen smartphone of tablet als verlengstuk van de eigen ogen, oren, mond en vingers, waarmee je via internet sociaal en maatschappelijk functioneert. Voor hen is het onbegrijpelijk dat je daarmee niet zakelijk kunt functioneren omdat de werkgever geen toegang verschaft tot het bedrijfsnetwerk en de bedrijfsapplicaties via de smartphone of tablet, of via de van thuis meegebrachte netbook. Zelfs als de werkgever toestaat dat de beschikbaar gestelde desktop PC of notebook ook wordt gebruikt voor persoonlijk internet doeleinden, bijvoorbeeld voor social media, is het voor hen nog steeds niet te verteren dat ze worden verplicht tot het gebruik van twee verschillende devices; de persoonlijke en die van de werkgever.

Dat is ook moeilijk verteerbaar als je bedenkt dat de nieuwe devices technisch ook prima bruikbaar zijn voor zakelijke doeleinden. Een netbook verschilt immers nauwelijks van een "laptop van de baas", een tablet verschilt weinig van die netbook en de smartphone verschilt weinig van de tablet.



Toch wordt het gebruik van deze nieuwe devices voor zakelijke doeleinden door veel werkgevers niet toegestaan omdat de IT afdeling zich daartegen verzet. Terecht voeren deze professionals tal van argumenten aan op het gebied van security. Maar die argumenten zijn weerlegbaar, omdat er technische maatregelen bestaan die deze risico's terugdringen tot een niveau dat vergelijkbaar is met het risiconiveau van een laptop PC "van de baas". Het achterliggende echte argument van de IT afdeling betreft de beheersbaarheid. Desktop PC's en laptops "van de baas" worden door de IT afdeling beheerd en dus gecontroleerd op alle security aspecten die de IT afdeling niet kan controleren als persoonlijke devices worden ingezet voor toegang tot het bedrijfsnetwerk en de bedrijfssoftware.

Het "gelijk" van de IT afdeling laten prevaleren boven het "gelijk" van de nieuwe generatie medewerkers is vanuit het ICT beleid te verantwoorden, maar vanuit het HRM beleid niet verstandig omdat het de aanwas van jongeren sterk beperkt.



BYOD beleid



Steeds meer organisaties beseffen dan ook dat deze tegenstelling niet houdbaar is en kiezen via een BYOD beleid voor een symbiose benadering. Een BYOD beleid dat het gebruik van persoonlijke devices voor zakelijke doeleinden mogelijk maakt omdat daarin de basis wordt gelegd voor maatregelen waarmee zowel de nieuwe medewerkers als de bestaande IT afdeling uit de voeten kunnen. Deze ontwikkeling wordt meestal versterkt omdat de werkgever ook invulling geeft of wil geven aan het HNW concept (Het Nieuwe Werken; waarmee we doelen op het fysieke plaats- en werkplekonafhankelijk uitvoeren van zakelijke taken/werkzaamheden.) Het invullen van het HNW concept vereist immers een antwoord op de vraag welke devices daarbij kunnen worden ingezet.

ITEM-C is gespecialiseerd in de management aspecten van bedrijfssoftware en daar hoort ook de toegang via verschillende devices bij. Daarom hebben wij, op basis van onze eigen ervaring en gesprekken met onze doelgroep, een concept ontwikkeld voor de succesvolle invoering van een BYOD beleid. Een concept dat aandacht besteedt aan:



1. De omgevingsontwikkeling (het waarom).
2. De formulering van het BYOD beleid (beleidskeuzen) in relatie tot de verschillende stakeholders als bestuur, business management, informatiemanagement, ICT management en ondernemingsraad.
3. De operationele uitwerking van het BYOD beleid in termen van toegestane devices, toegang tot het bedrijfsnetwerk en bedrijfsapplicaties, gegevensbestanden, internet, portal en de bijbehorende beveiligingsmaatregelen.
4. De beleidsbewaking op zowel het strategische, tactische en operationele niveau (informatiemanagement, ICT management), alsmede medewerker zeggenschap via de OR. Beleidsbewaking inclusief afspraken over rapportage en monitoring.
5. De financiële aspecten.
6. De risico beheersing.
7. De communicatie aspecten (intern / extern).
8. Appendices op het gebied van:
 - a. Organisatie.
 - b. Devices.
 - c. Toegang tot bedrijfstoepassingen.
 - d. Overeenkomst met medewerker.

kosten



Wij leggen dat “concept BYOD beleid” voor aan uw organisatie waarna we in een aantal iteraties van de verschillende stakeholders verlangen dat zij hun commentaar (bijdrage) leveren, zodat het bestuur uiteindelijk uw eigen BYOD beleid op maat van uw organisatie kan vaststellen. Als u zich in deze aanpak kunt vinden doen we dat voor een vaste prijs van € 2.900,- exclusief BTW.

ITEM-C

ITEM-C advies en interim management is gespecialiseerd in bedrijfssoftware. Wij combineren ruim dertig jaar management ervaring met bedrijfssoftware aan zowel de klant- als de leverancierskant.

Wij weten derhalve wat belangrijk, mogelijk en haalbaar is en projecteren die kennis vakkundig op de situatie bij onze klanten in de Lokale overheid en het middelgrote bedrijfsleven.

