Qteco
UP & RUNNING DOOR SLIMME ICT

SMART CONNECTIVITY

VIJF ADVIEZEN

BYOD veiliger dan veilig

Het aantal eigen smartphones, tablets of laptops op het werk groeit. Op zich niks mis mee, maar er zijn ook een aantal risicofactoren. Wat te denken van bijvoorbeeld illegale software? De werkgever kan aansprakelijk worden gesteld. Bovendien neemt het gebruik van dergelijke software een groot aantal risico's met zich mee. Denk aan schadelijke bestanden, identiteitsdiefstal en dataverlies. Daarom hebben we een vijftal adviezen voor u, om BYOD veilig te maken en te houden.

1. Maak een duidelijk, helder BYOD-beleid

Stel duidelijke regels op over BYOD/ CYOD. Op die manier weten alle medewerkers meteen waar ze aan toe zijn. Wijs iedereen op de consequenties van het werken met software zonder geldige licentie.

2. Controleer

Vaak weet niet iedereen precies hoe het BYOD-beleid in elkaar zit. Soms moeten medewerkers daarom geholpen worden. Met een software audit kunnen nare consequenties worden voorkomen.

3. Verzamel persoonlijke softwarelicenties

Sommige bedrijven stellen het verplicht dat iedereen de licentie van hun software meeneemt naar het werk. Een kopie hiervan wordt bewaard in de kluis. Zodra iemand het programma niet meer nodig heeft, kan de IT-afdeling de installatie ongedaan maken.

4. Scheid zakelijk en privé, ook technisch

Met virtuele desktops kan er een hoop ellende voorkomen worden. Wanneer men gebruik maakt van een virtuele desktop, kunnen er op één apparaat afzonderlijke partities (delen) gemaakt worden. Een voor zakelijk, een voor privé.

5. Blijf beveiligen

Firewall, virusscanners en controle op de netwerktoegang up-to-date?
Op die manier wordt voorkomen dat medewerkers toegang tot het bedrijfsnetwerk krijgen als ze (illegale) software op hun eigen laptop of smartphone.

Qteco B.V.
Boschdijk 131
5612 HB Eindhoven

Telefoon +31 40 303 15 00
E-mail info@qteco.nl
Twitter @byQteco

www.qteco.nl
KvK 58100466
IBAN NL44 INGB 0006 0848 14