Samen zorgen we ervoor dat de ICT veilig is!

Neem security serieus
De continuïteit van uw bedrijf is afhankelijk van de ICT. Daarnaast is de kans groot dat u persoonsgegevens verwerkt. Om deze redenen heeft u de plicht om serieus met ICT-veiligheid om te gaan.

Vertrouw geen onbekende bronnen
Kent u de bron van nieuwe informatie niet? Krijgt u een mail om een betaling te doen of een link te openen? Verifieer dit dan eerst. Eventueel belt u de afzender om zeker te zijn van uw zaak. Wees ook voorzichtig met het versturen van vertrouwelijke informatie.

Gebruik zakelijke computers alleen zakelijk
Gebruik uw zakelijke computer alleen voor de functie waar deze voor bedoeld is. Zo voorkomt u het oplopen van infecties en houdt u het zakelijke systeem gesloten.

Gebruik de privé computer alleen privé
Gebruik uw privé computer niet om toegang te krijgen tot zakelijke toepassingen of het zakelijke netwerk. Hiermee voorkomt u dat onveilige privé computers zakelijke systemen infecteren.

Gebruik het computernetwerk alleen voor zakelijke systemen
Gebruik de zakelijke WiFi (met uitzondering van een gesegmenteerd gasten WiFi) alleen voor zakelijke computers en niet voor privé laptops/ telefoons en als internet toegangspunt voor gasten. Zo voorkomt u dat zakelijke systemen geïnfecteerd worden. Geef ook geen toegang tot fysieke netwerkaansluitingen om dezelfde redenen.

Sluit geen informatiedragers aan op de computer
Sluit geen telefoons of tablets aan op uw zakelijke computer. Gebruik alleen USB-sticks of USB-schrijven wanneer u ervan overtuigd bent dat deze schoon zijn en gebruik ze alleen als het echt nodig is. Hiermee voorkomt u dat uw zakelijke systeem geïnfecteerd wordt door onveilige informatiedragers.

Installeer niet zelfstandig software
Het is verboden om zelfstandig software te installeren op uw zakelijke computer om infecties met ongewenste software te voorkomen.

Gebruik een sterk wachtwoord met MFA en verander dit met regelmaat
Voorkom dat uw account gehackt wordt doordat er een te simpel wachtwoord gebruikt wordt. Een sterk wachtwoord bestaat uit minimaal 8 tekens en bestaat uit hoofd- en kleine letters, cijfers en een speciaal teken. Gebruik bij bedrijf kritische systemen 2-factor authenticatie als dit beschikbaar is. Gooi regelmatig de opgeslagen wachtwoorden van uw browser weg zodat derden geen toegang hebben tot uw websites wanneer uw systeem gehackt wordt.

Gebruik een VPN op publieke internetpunten
Probeer het gebruik van publieke internetpunten te voorkomen. Maakt u hier met uw zakelijke computer toch gebruik van, maak dan altijd een VPN met het bedrijfsnetwerk.

Sluit uw systeem af
Laat computersystemen niet onbeheerd achter. Zodra u de werkplek verlaat, blokkeer deze en zet aan het eind van de werkdag de computer uit. Geef geen toegang tot uw werkplek aan derden, ook niet als deze uitstaat.

Verwijder lokale bestanden
Verwijder bestanden op uw lokale computer wanneer u deze niet meer gebruikt. Wanneer u oude bestanden niet opschoont blijven deze staan op de plaats waar ze niet thuishoren. Archiveer bestanden die niet meer gebruikt worden in de juiste netwerkmappen of gooi ze weg.

Bijsterhuizen 2414 | Wijchen
085 877 09 90
info@smartiq.nl
www.smartiq.nl

SMARTIQ
IT SUPPORT