10 gouden regels voor informatiebeveiliging

1. Wachtwoorden zijn strikt persoonlijk. Geef je wachtwoord nooit aan collega's, leerlingen of anderen en bewaar ze op een veilige plek, dus niet in je agenda of op een geel briefje.

2. Het melden van beveiligingsincidenten. Melden via datalek@rockopnh.nl is verplicht. Voorbeelden zijn een virusmelding, inbraak of poging daartoe of als jezelf of iemand anders gegevens kan inzien als dat niet de bedoeling is er juist gegevens kwijt zijn. Eventueel kun je dit ook bellen met de helpdesk als er direct actie nodig is.

3. Geheimhoudingsplicht. Binnen ROC Kop van Noord-Holland wordt met vertrouwelijke gegevens van onder meer collega's en leerlingen gewerkt. Hou je aan de richtlijnen hoe hiermee om te gaan.

4. Gedragscode Internet- en e-mail gebruik. Ga zorgvuldig om met internet en email, mijdt onveilige situaties en open geen e-mail van onbekenden.

5. Kennisnemen van het informatiebeveiligingsbeleid. Dit beleid met bijbehorende richtlijnen is van kracht. Neem daar kennis van via je leidinggevende.

6. Gegevensverstrekking aan derden via de telefoon. Het uitgangspunt is dat er nooit aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dit betekent ook dat er geen telefonische informatie over collega's, leerlingen en partners wordt verstrekt aan personen of instanties die beweren namens betrokkene te bellen.

7. Clear desk/clear screen policy. De vertrouwelijke omgang met gegevens houdt in dat elke werkplek zo is ingericht dat onbevoegden niet in jouw afwezigheid aan deze gegevens kunnen komen. Dit betekent dat jij je werkstation bewust dient te vergrendelen m.b.v. de screen-lock functie (Windowstoets + L) wanneer je je werkplek of werkstation verlaat. Ook mogen geen vertrouwelijke stukken zoals dossiers of verslagen onbeheerd op je bureau of in een niet afsluitbare kast blijven liggen. Ook de printer is een werkplek, haal vertrouwelijke gegevens direct na het afdrukken bij de printer weg.

8. Geen vertrouwelijke gegevens in de prullenbak. Zie ook punt 7. Het vernietigen van deze gegevens moet ook op een veilige manier plaatsvinden. Gebruik de papierversnipperaars en/of papiercontainers. Stop vertrouwelijke zaken in ieder geval nooit in de prullenbak of de normale oud-papier bak op je kantoor of werkplek.

9. Aanspreken van onbekende personen. Ben je al een keer in de situatie geweest dat je onbekenden tegenkwam in de met sleutels beveiligde ruimten? Spreek deze persoon of personen aan, stel jezelf voor en vraag wat hij/zij hier komt doen. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Begeleid deze personen naar de persoon die ze willen bezoeken of begeleid ze naar het publieke gedeelte van het pand.

10. Informatiebeveiliging krijg je niet gratis. Het vraagt aandacht, neem het serieus want het is belangrijk en het hoort bij de professionele en bekwame uitvoering van het werk.