Gebruikersreglement computer- en netwerkgebruik, melden datalek

U heeft zich te houden aan de regels die gelden bij de werkplek waar u bent gedetacheerd. Mocht u daar niet voldoende informatie vinden dan gelden onderstaande regels.

Dit reglement is van toepassing op alle ter beschikking gestelde faciliteiten en voorzieningen. Het geldt voor alle personen die op de werkplek werkzaam zijn of die gebruik maken van de faciliteiten en voorzieningen ongeacht of ze op de werkplek aanwezig zijn.

Zorgvuldigheid
Ga netjes om met de computer, deze is in bruikleen.
Installeer zelf geen software zonder overleg met de ICT beheerder.
Sla geen grote hoeveelheden privé materiaal op op de werkcomputer (foto's, films, muziek).
Maak geen gebruik van illegale software.
Log uit, of blokkeer uw scherm als u de werkplek verlaat.
Sla documenten op een logische plaats op zodat ook voor anderen de naam herkenbaar is en de locatie duidelijk (bijv. in geval van vervanging bij ziekte).
Verander regelmatig (minimaal 2 keer per jaar) het wachtwoord en gebruik verschillende wachtwoorden voor privé en werk.

Wijze van gebruik
Ga zorgvuldig om met de data waar u mee werkt.
Let goed op bij het versturen van een mail dat de juiste geadresseerde in het "aan" veld staat.
Wees u bewust van privacygevoelige data en de behandeling ervan.
Stuur geen vertrouwelijke (privacygevoelige) gegevens onversleuteld naar anderen.
Geef niet zomaar vertrouwelijke gegevens of informatie door aan derden.
Bij mail op telefoon of tablet, zorg voor een pincode of wachtwoord en stel deze zodanig in dat het apparaat na enkele minuten wordt geblokkeerd en bij gebruik weer om de code vraagt.

Do's en don't-s
Maak buiten de deur gebruik van de telewerkomgeving (daardoor hoeft data in principe nooit 'de deur' uit).
Neem nooit gevoelige data mee op een onbeveiligde memory-stick of andere drager.
Vraag eventueel aan de ICT beheerder om advies over veilige manieren van datatransport.
Zet geen privacy-gevoelige informatie in cloud-boxen als dropbox en one-drive als onduidelijk is wie er allemaal toegang hebben.
Ga niet in/open geen mails/links van mensen/bedrijven die u niet persoonlijk kent.
Let goed op dat mails van leveranciers (bijv. KPN) ook echt van KPN zijn (controleer linkjes, open geen bijlagen en check of de mail gepersonaliseerd is – en of alles klopt). Bij twijfel – vraag ondersteuning aan de ICT beheerder.
Ga zorgvuldig om met telewerk-faciliteiten. Volg de telewerk instructies van de ICT beheerder.

Bij het versturen van vertrouwelijke data aan derden is het verplicht om deze data te voorzien van een wachtwoord of in te pakken in een beveiligde zip-file. Verstuur het wachtwoord apart en bij voorkeur via een andere weg dan de bijhorende data (bijv. via sms / whatsapp / telefoon).

Persoonlijk verantwoordelijk en aansprakelijk

U bent persoonlijk verantwoordelijk voor uw datagebruik

Uw gebruikersnaam, password en emailadres zijn strikt persoonlijk. U bent verantwoordelijk voor ieder gebruik van uw gebruikersnaam, password en emailadres.

U bent aansprakelijk voor schade die voortvloeit uit het misbruik van de faciliteiten en voorzieningen: dat geldt voor schade die voortvloeit uit onjuist, onzorgvuldig of onrechtmatig gebruik van uw gebruikersnaam, password en emailadres.

Voor misbruik van computerfaciliteiten dan wel het (opzettelijk) bekend maken van vertrouwelijke informatie kan door uw directie een sanctie worden opgelegd. Het opzettelijk lekken van vertrouwelijke informatie kan in bepaalde omstandigheden ook strafrechtelijk vervolgd worden.

Melden Datalek

Bij het ontdekken van een datalek of het vermoeden ervan - waaronder ongeautoriseerde toegang tot en of ongeautoriseerd gebruik van vertrouwelijke informatie – moet u direct uw leidinggevende informeren.

Informeer bij diefstal of vermissing van een data-drager (telefoon, laptop, e.a.) uw leidinggevende en overleg met de ICT beheerder over eventuele vervolgstappen. Wijzig daarna in ieder geval uw wachtwoord(en).

UvA Ventures Holding
1 maart 2017