



Werkplek- en wachtwoordbeleid

Rijnbrink

Auteur: Huub Overbeek
Datum: Januari 2023
Status: v1.0 definitief

Inhoudsopgave

1	Inleiding	3
2	Aanleiding	3
3	Werkplekbeleid	3
4	Wachtwoordbeleid	4
5	Geldigheid	5

1 Inleiding

In september 2020 is in het MT voor het laatst gesproken over een werkplekbeleid. Destijds is besloten om delen van het voorgestelde beleid alvast over te nemen in afwachting van het verwerken van de opmerkingen en aanvullingen. Een definitief werkplekbeleid is daarna niet meer vastgesteld. Inmiddels zijn we ruim 2 jaar verder en is er op werkplekgebied het nodige gebeurd. Tijd om opnieuw met elkaar af te spreken hoe wij willen samenwerken op digitaal gebied.

2 Aanleiding

Het jaar 2022 is gebruikt om de overgang van een Citrix- naar een volledige Microsoft-werkplek te realiseren. Het besluit om dit te gaan doen stamt uit 2020 naar aanleiding van een adviesrapport van M&I-partners. In coronatijd is in korte tijd MS-Teams ter beschikking gesteld aan iedereen en zijn laptops aangeschaft t.b.v. het thuiswerken. Vorig jaar - na de corona-beperkingen - is er serieus aandacht besteed aan het opleiden van alle medewerkers.

Ook technisch is in 2022 het nodige veranderd. Zonder in details te treden: het beheerproduct van Microsoft voor werkstations is in gebruik genomen (MS-Intune) t.b.v. onze werkplekken (dus niet smartphones, deze zijn in beheer bij Facilitair). Hiermee is het mogelijk om elke werkplek op afstand te beheren, van het overnemen van een sessie tot het inspoelen van software of zelfs het wissen van gegevens bij diefstal of vermissing van een laptop.

3 Werkplekbeleid

Als uitgangspunt voor onze digitale werkomgeving geldt het concept “anytime, anyplace, anywhere”. Het betekent dat iedereen, die een werkrelatie heeft met Rijnbrink (vast of gedetacheerd), gebruik kan maken van de digitale diensten van Rijnbrink. Enkele voorbeelden van deze diensten: toegang tot Wifi/internet, printen, gebruiken van alle ter beschikking staande applicaties (mits daarvoor geautoriseerd), opslaan van persoonlijke en met collega's gedeelde data.

Een ander uitgangspunt is dat wij zoveel mogelijk gebruik maken van cloud-diensten: zo min mogelijk techniek in huis, maar geleverd door gespecialiseerde bedrijven. Of het nu om software, data-opslag, autorisatie functionaliteit, printdiensten of anderszins gaat.

Rijnbrink medewerkers voeren allen zeer diverse werkzaamheden uit, zijn vaak bezig met innovatieve oplossingen en hebben behoefte aan vrijheid om hun eigen werkplek zo gepersonaliseerd mogelijk in te richten. Daar hoort ook bij dat men bijv. de mogelijkheid moet hebben om bepaalde software uit te proberen, data lokaal op te slaan etc.

Randvoorwaarde om dit te kunnen toestaan is dat er voldoende maatregelen zijn genomen om veilig te werken met zo min mogelijk risico's op datalekken, cybercriminaliteit (phishing, ransomware etc.) of onbedoeld verlies van data.

Dit betekent dat elke werkplek:

- up-to-date moet zijn v.w.b. security patches
- een actueel antivirus product bevat
- geen illegale/ongelicenseerde software bevat
- voorzien is van een geëncrypte harde schijf

- op afstand beheerd kan worden, niet alleen voor het inspoelen van software, oplossen van problemen, maar ook t.b.v. het wissen van Rijnbrink data, mocht er sprake zijn van vermissing, verlies of diefstal van de werkplek

Bovenstaande geldt zowel voor door Rijnbrink uitgeleverde (standaard-) werkplekken als voor eigen werkplekken. Mochten er door zelf geïnstalleerde software op een Rijnbrink laptop onverhoopt toch problemen ontstaan, dan is de beherende afdeling gerechtigd om - in overleg met de gebruiker - de laptop terug zetten naar fabrieksinstellingen en vervolgens een herinstallatie uitvoeren.

De huidige standaard werkplek is een HP Probook 440 of 450 met Windows 10.

Voor mensen met een eigen laptop kan het mogelijk bezwaarlijk zijn om hun werkplek te laten beheren door Rijnbrink, althans, voor zover het de Rijnbrink diensten en -data betreft. Zij hebben de mogelijkheid om volledig webbased te werken en kunnen ook in dat geval van alle diensten van Rijnbrink gebruik maken (MS365 incl. Teams, Onedrive, printing, etc.).

4 Wachtwoordbeleid

Om veilig te werken is vanzelfsprekend ook een goed wachtwoordbeleid noodzakelijk. Het hieronder beschreven wachtwoordbeleid beperkt zich tot de toegang tot de werkplek an sich, dus niet tot het inloggen op applicaties, zoals bijv. Wise, AFAS etc. Dat wordt natuurlijk anders als we Single Sign On gaan invoeren, maar zover is het nog niet. Single Sign-On, kortweg SSO, is dat eindgebruikers eenmalig hoeven in te loggen. De SSO-software zorgt er daarna voor dat authenticatie tot andere applicaties automatisch verloopt.

Uitgangspunt is dat iedere medewerker zorgt voor een sterk wachtwoord. Sterk betekent: minimaal 8 karakters, bestaande uit minimaal 1 hoofdletter, 1 cijfer en 1 speciaal teken. Het gebruik van eigennamen, geboortedata etc. wordt ten sterkste afgeraden. Elk geheugensteuntje wordt in feite afgeraden, omdat dat de kans tot kraken van het wachtwoord vergroot.

Het wachtwoord is permanent, dus hoeft niet om de zoveel tijd gewijzigd te worden. Reden is dat bij frequent wijzigen medewerkers juist gaan kiezen voor eenvoudige wachtwoorden. Aangezien gebruik wordt gemaakt van z.g. Multi Factor Authentication (MFA), is het ook niet nodig om het wachtwoord periodiek te wijzigen. MFA houdt in dat men, als men wil inloggen, een code ontvangt op de smartphone, die men bij het inloggen dient in te voeren. 1x per week moet men m.b.v. MFA inloggen.

Indien men de werkplek verlaat, al is het maar voor even, dan dient deze altijd vergrendeld te worden.¹²

¹ Tip1: moderne apparaten bieden de mogelijkheid om je smartphone via Bluetooth te koppelen; loop je met je smartphone dan buiten het bereik van je werkplek, dan vergrendelt deze automatisch. Vraag de Servicedesk hoe dit werkt.

² Tip2: Je kunt je werkplek instellen op gezichtsherkenning; dan hoeft je niet elke keer je wachtwoord in te tikken om te ontgrendelen.

5 Geldigheid

Dit wachtwoordbeleid gaat in per 1 februari 2023 en zal elk jaar worden herzien. Indien geen herzieningen nodig zijn, dan wordt het beleid automatisch met een jaar verlengd.