Gedragsregeling voor de digitale werkomgeving_20v03

Gedragsregeling voor de digitale werkomgeving

Medewerkers en leveranciers van Bekwaam krijgen de beschikking over een fysieke werkplek en/of een laptop en een 'digitale werkomgeving'. Een mobiele telefoon behoort ook tot de middelen waarop een digitale werkomgeving kan staan (e-mail/agenda). Tevens krijgen de medewerkers toegang tot een online Cloud. De functie en het soort informatie waarmee gewerkt wordt bepaalt welke ICT-functionaliteiten nodig zijn voor de uitoefening van de functie.
De digitale werkomgeving biedt jou mogelijkheden die een zeker risicobesef vragen. Deze Gedragsregeling voor de digitale werkomgeving bevat daarom afspraken over de gebruiksmogelijkheden van de digitale werkomgeving, jouw online gedrag en bewuste omgang met de risico's. Het is van belang dat je je bewust bent van bestaande wettelijke rechten en plichten. Vanuit Bekwaam zal nauwlettend worden toegezien op veranderingen op het gebied van het informatieveiligheidsbeleid. Belangrijke veranderingen zullen wij door middel van een toolbox communiceren met medewerkers en professionals.

Beveiligingsmaatregelen Bekwaam

Bekwaam zorgt met technische beveiligingsmaatregelen (antivirussoftware, beveiligde harde schijf, back-ups, beveiligde USB poorten) voor de beschikbaarheid, duurzame toegankelijkheid, integriteit en vertrouwelijkheid van de informatie op de laptop. Indien een leverancier gebruikt maakt van zijn eigen digitale middelen, verwacht Bekwaam dat daarop up-to-date antivirussoftware geïnstalleerd is en dat er gebruik gemaakt wordt van de meest recente versies van besturingssoftware. Informatie die opgeslagen wordt op het medium moet niet toegankelijk zijn voor onbevoegden, enerzijds door gebruik van unieke wachtwoorden of door het toepassen van een versleutelde harde schijf. Doordat niet alle risico's uit te sluiten zijn, wordt er verwacht dat er op een veilige manier gebruik gemaakt wordt van de digitale werkomgeving en online gedrag.

Gedragsregels

- Zorgvuldig gebruik van de voorzieningen. Bij vermissing of het vermoeden van diefstal van digitale apparatuur moet direct melding gemaakt worden bij de Informatie Veiligheid Coördinator (hierna te noemen IVC). De IVC bepaalt vervolgens welke vervolgstappen er genomen moeten worden. Bij het lekken van persoonsgegevens moet, indien dit een groot risico vormt, ook melding worden gedaan bij de Autoriteit Persoonsgegevens (hierna te noemen AP). Tevens wordt elk incident opgenomen in het register voor datalekken.
- Laat mobiele apparaten en gegevensdragers nooit onbeheerd achter, indien je tijdelijk de werkplek moet verlaten zorg er dan voor dat je afgemeld bent. Bij het vervoeren van de mobiele apparaten buiten de werkomgeving dient deze altijd uitgeschakeld te zijn.
- Voor het uitoefenen van je werkzaamheden op locatie zijn zogenaamde flexwerkplekken ingericht. Hier geldt een *Clean Desk Policy,* laat je werkplek achter zodat een collega hier ook kan werken. Dit betekent dat er geen persoonlijke spullen achter mogen blijven en uiteraard ook geen documenten.
- De ter beschikking gestelde laptop/mobiele telefoon mag niet door derden worden gebruikt.
- Indien het voor de continuering van de werkzaamheden noodzakelijk is om je laptop tijdelijk uit te lenen aan een collega, dan is het belangrijk dat je er zorg voor draagt dat je afgemeld bent uit de systemen van de klant. Tevens blijf je verantwoordelijkheid voor schade door onbehoorlijk gebruik.

Wilhelminasingel 1b _ 4818 AA Breda
info@bekwaam.com _ +31 (0)76 205 08 88
www.bekwaam.com

IBAN _ NL47RABO0107949830
KvK _ 201 709 44
BTW _ NL8223.72.253.B01

- Meld incidenten; Om te voorkomen dat gevoelige informatie in verkeerde handen komt, is het belangrijk om incidenten zo spoedig mogelijk na vaststelling te melden aan de IVC, deze bepaalt vervolgens welke vervolgstappen er genomen moeten worden.
- Virus: meldt (vermoeden) van een virus direct aan de IVC zodat er melding gemaakt kan worden bij de ICT servicedesk.
- Installeren van applicaties: op de laptop/telefoon die je via Bekwaam krijgt zijn de applicaties geïnstalleerd welke veilig bevonden zijn door de afdeling ICT. Indien je nieuwe plug-ins nodig hebt, doe je dit altijd in overleg met de IVC. De afdeling ICT beoordeelt of de applicatie veilig is. Indien je gebruik maakt van je eigen middelen, ga dan zorgvuldig om met het installeren van applicaties.
- Mobiel veilig werken; maak gebruik van het wifi-netwerk van je werkplek. Als je op openbare plekken werkt, zorg dat dat je verbonden bent met de mobiele hotspot van je telefoon.
  Maak nooit gebruik van openbare wifi- netwerken in hotels/restaurants/openbaar vervoer, ook niet als je voor deze netwerken moet betalen. Je kunt niet vaststellen of deze netwerken voldoende beveiligd zijn, waardoor er een risico bestaat dat onbevoegden toegang tot jouw gegevens krijgen. Op momenten dat je geen gebruik maakt van je hotspot moet je ervoor zorgen dat deze uitgeschakeld is. Ook bluetooth en roaming dienen uit te staan.
- Omgang met wachtwoorden. Bij indiensttreding ontvang je een inlogaccount tot je digitale werkomgeving. Ga zorgvuldig om met je wachtwoorden. Maak geen gebruik van de functie om de wachtwoorden automatisch in te vullen. Tevens is het verstandig jouw wachtwoord niet voor andere websites of apps te gebruiken. Geef je wachtwoorden ook niet aan anderen, ook beheerders van de ICT zullen nooit om jouw wachtwoord vragen.
- Voor het opslaan van documenten wordt gebruik gemaakt van Sharepoint en de digitale werkomgeving van de klant. Er mag geen informatie worden opgeslagen op de harde schijf. Indien het noodzakelijk is om gegevens (tijdelijk) op te slaan op de harde schijf, mogen deze gegevens niet langer dan noodzakelijk op de harde schijf staan, met een maximum van 72 uur.
- Indien het noodzakelijk is om gebruik te maken van een USB stick is het belangrijk dat hier geen informatie op wordt opgeslagen van vertrouwelijke, dan wel bedrijfsvertrouwelijke aard.
- Daar waar Bekwaam een laptop ter beschikking stelt is het niet toegestaan privé gegevens op te slaan op de harde schijf. Na inlevering van de zakelijke laptop (einde opdracht) worden alle gegevens van de harde schijf en uit applicaties gewist.
- Daar waar Bekwaam een laptop ter beschikking stelt is het niet toegestaan om een privé e-mail adres toe te voegen aan Outlook.
- Je krijgt vanuit Bekwaam een e-mailadres welke je kunt gebruiken voor de communicatie met Bekwaam en The Compliace Factory. Indien je ook een e-mailadres krijgt van de klant waarvoor je werkzaamheden verricht, is het absoluut niet toegestaan om vanuit dit e-mail adres te communiceren voor privé doeleinden. Ook voor de communicatie met Bekwaam en TCF is het niet toegestaan hiervoor het e-mailadres van de klant te gebruiken. Indien dit wel gebeurt, zal dit worden gezien als een datalek en zal dit ook als zodanig geregistreerd worden in het datalekken register.
- De gedragsregels van de klant waar je werkzaam bent, zijn onverminderd van toepassing. Mochten er conflicterende belangen zijn tussen de gedragsregels van de klant en van Bekwaam, dan verzoeken wij je dit melden bij de IVC.

Wilhelminasingel 1b _ 4818 AA Breda
info@bekwaam.com _ +31 (0)76 205 08 88
www.bekwaam.com

IBAN _ NL47RABO0107949830
KvK _ 201 709 44
BTW _ NL8223.72.253.B01

Veiligheidsincidenten kunnen telefonisch of per e-mail gemeld worden aan de IVC. Telefonische melding via 076-205 0888 en per e-mail via IVC@bekwaam.com.

Ik heb kennis genomen met bovenstaande inhoud en verklaar dat ik hiermee akkoord ben.
Naam:
Handtekening:

Datum:
Plaats:

Wilhelminasingel 1b _ 4818 AA Breda
info@bekwaam.com _ +31 (0)76 205 08 88
www.bekwaam.com

IBAN _ NL47RABO0107949830
KvK _ 201 709 44
BTW _ NL8223.72.253.B01