Bartiméus: fonds

Voor alle mensen die slechtziend of blind zijn

Gedragscode ICT gebruik Bartiméus Fonds

Medewerkers Bartiméus Fonds

Zeist, september 2022

Doel

Het Bartiméus Fonds (BF) richt zich op het waarborgen van de beschikbaarheid, vertrouwelijkheid en integriteit van zijn systemen en gegevens. Daarom moeten alle medewerkers op een verantwoordelijke, ethische en wettelijke manier te werk gaan.

Alle personeelsleden, consultants en tijdelijke medewerkers (ZZP-ers) bij BF moeten informatie kunnen beheren met zorg en discretie, zowel geschreven, elektronisch of verbaal.

Daarom moet de omgang met informatie in overeenstemming zijn met het informatiebeveiligingsbeleid van BF en met de volgende regels en uitgangspunten.

Om dit te waarborgen worden de medewerkers binnen BF getraind en bewust gemaakt van onderwerpen op het gebied van ICT-beveiliging en de AVG door middel van continue bewustwordingstrainingen.

In deze gedragscode worden de basisregels vastgelegd voor het gebruik van ICT middelen door alle medewerkers binnen BF en worden de eisen geformuleerd ten aanzien van continue bewustwording en kennis.

Regels en uitgangspunten

1. Vertrouwelijkheid

Je dient voorzichtig en discreet om te gaan met alle informatie van BF. Je mag geen informatie, systemen of netwerken raadplegen of gebruiken die niet nodig zijn voor je werk.

Je mag geen vertrouwelijke informatie delen met collega's, consultants of tijdelijke werknemers die deze informatie niet nodig hebben voor hun specifieke functie.

Je mag geen vertrouwelijke informatie delen met externe partijen, tenzij dit een duidelijk commercieel doel dient. Dit gaat altijd in overleg met de ICT-coördinator. Tevens moet de externe partij een geheimhoudingsverklaring hebben ondertekend.

2. Toegangscodes (wachtwoorden en pincodes)

Alle wachtwoorden en pincodes zijn strikt persoonlijk. Je dient een wachtwoord te hebben van minimaal 12 karakters dat zowel hoofdletters, kleine letters en cijfers bevat.

Je mag nooit wachtwoorden op post-it-briefjes, prikborden, op papier of lokaal op je computer hebben staan.

Je dient uit te loggen van je ICT-werkstation (mobiele telefoon, pc, tablet) of deze te vergrendelen telkens als je deze verlaat. Aan het eind van de dag zet je ook je scherm uit.

3. Fysieke beveiliging

Je bureau moet altijd vrij zijn van vertrouwelijke informatie (Clean Desk Policy). Vertrouwelijke informatie moet in afgesloten lades of kasten worden geplaatst om

ongeoorloofde toegang te voorkomen. Je dient je ook bewust te zijn van de zichtbaarheid van je pc-scherm. Je mag geen vertrouwelijke en gevoelige gegevens open hebben staan wanneer er onbevoegden achter je staan die jouw activiteiten over je schouder mee kunnen volgen (Clear Screen Policy).

4. Omgang met ICT middelen en documenten op externe locaties

Als je mobiele ICT-middelen meeneemt buiten het kantoor van BF, moet er een pincode of wachtwoord zijn ingesteld om te zorgen voor voldoende beveiliging tegen toegang door onbevoegden.

Als draagbare ICT-middelen (bijv. laptops of mobiele apparaten) naar het buitenland worden meegenomen is vooraf toestemming nodig van de directeur.

5. Apparatuur en software

Alle gebruikte ICT-systemen, -apparatuur of -opslagapparaten zijn door BF goedgekeurd of voldoen aan de door BF vastgestelde normen. Sluit nooit ongeautoriseerde apparatuur aan op werkstations of netwerken. Dit geldt ook voor USB-sticks en smartphones. Je mag alleen programma's installeren en downloaden waarvoor je toestemming hebt gekregen van de ICT-coördinator.

Software en apparatuur zoals computers, laptops en mobiele telefoons zijn eigendom van BF en moeten als zodanig worden behandeld. Daarom mogen ze niet worden uitgeleend aan anderen (inclusief familieleden).

Je dient de interne bestandsservers van BF te gebruiken bij het verwerken van gegevens. Het gebruik van private Cloud-gebaseerde diensten zoals Google Drive, Dropbox, OneDrive, enz. en web gebaseerde bestandsuitwisselingsdiensten is alleen toegestaan bij het ontvangen van gegevens van externe partijen. Het is niet toegestaan om gegevens van BF te uploaden naar niet-geautoriseerde diensten.

Software moet altijd worden gebruikt in overeenstemming met de licentievoorwaarden waartoe BF is toegetreden.

Het is niet toegestaan om, zonder overleg met de ICT-coördinator, software op de laptops te installeren die geen verband houdt met werk gerelateerde taken bij BF.

6. Gebruikersgegevens

De gebruikersrechten moeten worden gerespecteerd. Gebruik alleen je eigen gebruikersrechten. Je mag je gebruikersgegevens nooit delen met anderen (inclusief je werkgever).
Misbruik van gegevens en ICT-middelen kan digitale sporen nalaten die een negatieve impact kunnen hebben op de reputatie van BF.

7. Digitale activiteit

Je dient het privégebruik van internet en e-mail via de middelen van BF tot een minimum te beperken.

Privé-documenten kunnen lokaal op de computer worden opgeslagen. Lokale mappen moeten worden gemarkeerd als “privé”. Het is niet toegestaan om gevoelige persoonlijke gegevens per e-mail te versturen.

Werk gerelateerde online correspondentie mag in geen geval via geanonimiseerde communicatiekanalen plaatsvinden.

Het is ten strengste verboden om de e-mailaccounts, computers, tablets en mobiele telefoons van BF te gebruiken om sites met pornografische, racistische of andere extreme en criminele inhoud te bezoeken.
Het e-mailadres/nummer van de afzender moet worden gecontroleerd voordat onbekende links en documenten worden geopend.

8. Beveiligingsmonitoring en logging

BF respecteert de privacy van individuen en voldoet aan de wetten en regelgeving in Nederland. BF mag alle ICT-toepassingen loggen en kan in bijzondere situaties toegang eisen tot het e-mailaccount van een gebruiker of andere informatie die door werknemers, consultants en tijdelijk personeel wordt gegenereerd en opgeslagen.

9. Omgang met persoonsgegevens

Bij BF zijn we zeer gericht op de bescherming van persoonsgegevens die ons door onze medewerkers, klanten en partners worden toevertrouwd. We werken voortdurend aan de ontwikkeling en implementatie van veilige processen om een wettelijke en veilige omgang met persoonsgegevens te garanderen.

We hebben de volgende algemene uitgangspunten vastgesteld voor de correcte omgang met persoonsgegevens:

- Werknemers mogen uitsluitend toegang hebben tot persoonsgegevens die verband houden met hun werk.
- Werknemers mogen persoonsgegevens (d.w.z. door klanten of partners verzonden persoonsgegevens) alleen met andere werknemers delen als deze werk gerelateerd zijn.
- Als een e-mail met persoonsgegevens wordt doorgestuurd naar de relevante medewerker, moet de e-mail na verwerking worden verwijderd.
- Werknemers mogen persoonsgegevens niet langer dan nodig lokaal of in hun inbox opslaan. In plaats daarvan dienen zij gebruik te maken van de systemen die voor deze doeleinden zijn ontworpen.
- Medewerkers dienen periodiek hun bestanden en mappen (zowel fysiek als digitaal) door te nemen om ervoor te zorgen dat ze geen gegevens bewaren die niet meer nodig zijn.

10. Rapporteren van beveiligingsincidenten

Als je een vermoeden hebt of op de hoogte bent van beveiligingsincidenten, meld dit dan onmiddellijk aan de directe manager en de ICT-coördinator.

Voorbeelden van beveiligingsincidenten:

- Verdachte e-mails.
- E-mails met gevoelige persoonlijke informatie die naar een verkeerde ontvanger zijn gestuurd.
- Ontbrekende of verloren ICT-middelen.

Aarzel niet om contact op te nemen met je leidinggevende of ICT-coördinator als je iets vermoedt. Better safe than sorry!

Tot slot

De medewerker heeft deze overeenkomst en de daarbij gevoegde instructies gelezen en begrepen, verklaart zich akkoord met de inhoud en belooft zich aan de inhoud te conformeren.

Naam en handtekening medewerker:

Datum: