KUURNE
Sociaal Huis

Marktplein 9 ‹ 8520 Kuurne
056 73 70 11 ‹ erk.nr. 14AB/74/98051 ‹ sociaalhuis@kuurne.be ‹ www.sociaalhuiskuurne.be

Uittreksel uit de notulen van het Vast Bureau

Zitting van 22 oktober 2019.

Aanwezig: Francis Benoit, Voorzitter van het Vast Bureau
Ann Messelier, Johan Bossuyt, Francis Watteeuw, Jan Deprez, Leden Vast Bureau
Bram Deloof, Voorzitter van het Bijzonder Comité voor de Sociale Dienst
Els Persyn, Algemeen Directeur

Verontschuldigd:

Voorwerp **Personeel - wijzigen arbeidsreglement inzake gedragscode voor informatiebeheerders**

Bevoegdheid en juridische grond

Het Vast Bureau is bevoegd voor het vaststellen van het arbeidsreglement.
Deze bevoegdheid werd gedelegeerd door de OCMW-raad bij beslissing van 25 april 2019.

Feiten, context en argumentatie

Aan het arbeidsreglement moet een bijlage inzake 'gedragscode voor informatiebeheerders' worden toegevoegd.

De gedragscode belangt alle personeelsleden aan die door gebruik van een ICT-systeem toegangsrechten hebben waarbij persoonsgegevens en gevoelige informatie kunnen geconsulteerd worden.

Verwijzingen

Het arbeidsreglement, zoals vastgesteld bij beslissing van de OCMW-raad van 18 december 2019.

Adviezen en visum

Het MAT, in vergadering van 29 augustus 2019, gaat akkoord met de invoering van 'bijlage 20 - gedragscode voor informatiebeheerders'.
Het Bijzonder Onderhandelingscomité, in vergadering van 8 oktober 2019, gaat eveneens akkoord.

Besluit

Artikel 1

Bijlage 20 - gedragscode voor informatiebeheerders' wordt toegevoegd aan het arbeidsreglement:

BIJLAGE 20: Gedragscode voor informatiebeheerders

De informatiebeheerder is iedere persoon die in het kader van verantwoordelijkheden met betrekking tot een ICT-systeem over toegangsrechten beschikt die ruimer zijn dan het louter functioneel gebruik van de informatie ("superusers" of "powerusers"). Het gaat onder meer om systeembeheerders, databank administrators (DBA), informatieveiligheidsconsulenten (CISO), functionarissen voor de gegevensbescherming (DPO), software-ontwikkelaars en -beheerders, netwerk-beheerders, consultants, externe IT dienstenleveranciers2, en onderaannemers.

I. De ethische integriteit van de informatiebeheerder

I. 1 De informatiebeheerder stelt zich objectief en onpartijdig op tijdens de uitoefening van zijn/haar functie.

I. 2 De informatiebeheerder streeft ernaar (de perceptie van) persoonlijke belangenconflicten te vermijden. Wanneer deze zich toch voordoen, zal hij zijn oversten daarover onmiddellijk inlichten en hierover een formele beslissing vragen.

I. 3 De informatiebeheerder stelt zijn vaardigheden op gepaste wijze ten dienste van de organisatie en van de medewerkers van de informatiesystemen.

I. 4 De informatiebeheerder streeft ernaar in de best mogelijke verstandhouding samen te werken met alle medewerkers van de organisatie.

I. 5 De informatiebeheerder zal zijn technische vaardigheden eerlijk voorstellen en doet een beroep op bijkomende professionele (technische) bijstand indien nodig.

I. 6 De informatiebeheerder krijgt de middelen en levert voldoende inspanningen om op de hoogte te blijven van de evoluties binnen zijn/haar domein.

I. 7 De informatiebeheerder zal steeds respectvol omgaan en samenwerken met alle medewerkers (intern en extern).

I. 8 De informatiebeheerder zal met de (toezichthoudende) autoriteiten samenwerken.

II. De integriteit en de beschikbaarheid van de informatie

II. 1 De informatiebeheerder waakt over het behoorlijk functioneren van het systeem en stelt de handelingen die nodig zijn om de integriteit en de beschikbaarheid van het informatiesysteem te garanderen.

II. 2 De informatiebeheerder waakt erover dat de handelingen niet het verlies, de onbeschikbaarheid of de vernietiging van de gegevens of van de toepassingen tot gevolg hebben.

II. 3 Aangezien bepaalde handelingen van medewerkers schade kunnen berokkenen aan de integriteit of de beschikbaarheid van het computersysteem of -netwerk, of de gegevens, moet de informatiebeheerder in het kader van zijn

verantwoordelijkheden toezien op de naleving van het beleid van toepassing in de organisatie en indien nodig zijn hiërarchische meerderen op de hoogte brengen. Indien hij vaststelt dat bepaalde van deze acties niet onder het toepassingsgebied van de bestaande minimale normen vallen, brengt hij de informatieveiligheidsconsulent hiervan op de hoogte. De informatieveiligheidsconsulent zal dan de nodige maatregelen treffen in het belang van de organisatie.

II. 4 De informatiebeheerder zorgt ervoor dat de toegang tot het systeem gegarandeerd wordt aan de personen die dergelijke toegang nodig hebben in het kader van hun functie en dat de toegang tot die personen beperkt blijft.

III. Informatiebescherming

III. 1 De informatiebeheerder is zich bewust van het feit dat hij/zij toegang heeft tot grote hoeveelheden persoonsgegevens en gevoelige gegevens waarop de bepalingen inzake bescherming van het privéleven en van persoonsgegevens van toepassing zijn.

III. 2 De informatiebeheerder is zich bewust van het feit dat de persoonsgegevens en gevoelige gegevens moeten worden beschermd.

III. 3 De informatiebeheerder wijst op de risico's eigen aan zijn domein, dringt er bij de directie op aan om gepaste instructies te krijgen met betrekking tot die risico's en past technische, procedurele, communicatieve en organisatorische maatregelen toe waardoor de persoonsgegevens en gevoelige gegevens beveiligd en beschermd zijn tegen elke niet toegelaten gegevensverwerking. De informatiebeheerder houdt naast de aan verwerkingen verbonden risico's, ook rekening met de aard, de omvang, de context en de verwerkingsdoeleinden.

III. 4 De informatiebeheerder waakt erover dat ook derden en externe medewerkers de bepalingen met betrekking tot de bescherming van persoonsgegevens en gevoelige gegevens naleven.

III. 5 De informatiebeheerder mag on-line communicatie en toegangen tot bestanden controleren binnen het kader van zijn/haar bevoegdheden en mits de naleving van de wettelijke en reglementaire bepalingen.

III. 6 De informatiebeheerder gaat ervan uit dat alle informatie van de organisatie vertrouwelijk is en als dusdanig behandeld moet worden, door zichzelf als door alle medewerkers van de organisatie.

IV. Informatie- en documentatie-plicht

IV. 1 De informatiebeheerder licht alle betrokken medewerkers duidelijk en regelmatig in over hun verantwoordelijkheden bij het toegelaten gebruik van informatiesystemen via bewustmaking, opleiding en evaluaties (audits).

IV. 2 De informatiebeheerder licht naar aanleiding van een interventie zijn/haar handelingen tijdig en op een begrijpelijke manier toe opdat de betrokken medewerker(s) voldoende geïnformeerd zou zijn over de gevolgen op (het gebruik van) de informatiesystemen.

IV. 3 De informatiebeheerder waakt erover dat er steeds een geactualiseerde documentatie voorhanden is waarin het informatiesysteem (zoals ontwikkeling, hard- en software, infrastructuur) op zodanige wijze wordt beschreven dat elke betrokken persoon zich een precies en volledig totaalbeeld zou kunnen vormen. De bedoeling

ervan is een continu beheer van het informatiesysteem te garanderen. De gegevensbeschermingseffect-beoordeling maakt hier integraal deel van uit.

IV. 4 De informatiebeheerder kan vragen of problemen bespreken met andere informatiebeheerders in de bestuur en indien nodig ook in vertrouwen bespreken met de dienst informatieveiligheid van de KSZ.

Elke informatiebeheerder verklaart zich akkoord om bovenstaande gedragscodes voor informatiebeheerders na te leven.

Het bestuur kan ten alle tijde het naleven van deze gedragsregels controleren. Het niet naleven van deze gedragscodes kan leiden tot een disciplinair proces.

Artikel 2
De personeelsleden worden op de hoogte gebracht van het invoeren van bijlage 20 aan het arbeidsreglement.

Artikel 3
Een afschrift van dit besluit zal online worden neergelegd via www.arbeidsreglement.belgie.be.

Artikel 4
Deze beslissing is onderworpen aan het administratief toezicht.

Aldus beslist in bovenvermelde zitting.

Algemeen Directeur,
(get.) Els Persyn

Voorzitter van het Vast Bureau,
(get.) Francis Benoit

Voor eensluidend afschrift

Algemeen Directeur

Els Persyn

Voorzitter van het Vast Bureau

Francis Benoit