GBD-201 - Informatiebeveiligingsplan WIZ

Auteur:	**Datum/Tijd**:	**Status**:
[redacted]	maandag 23 september 2019 09:58	Gepubliceerd
Wijziging:	Dinsdag 3 december 2024 16:00	***Definitief***

Verantwoordelijke: [redacted]
Auteur: [redacted]

Sector Inwoners Gemeente Weert

Afdeling Werk, Inkomen en Zorg

Vastgesteld door College van B&W d.d. 17-december-2024

Djuma Zaaknummer: 2657893

Versie 3.0

Wijzigingsoverzicht

Datum	Wijziging	Pagina
	Initiële versie 1.0. Afgeleid van Handboek informatiebeveiliging Werk Inkomen en Zorg versie 3.0	
1-08-2015	Informatie verplaatst van het Handboek naar Informatiebeveiligings Beleid versie 2.0	Geheel document
26-03-2018	Security Officer vervangen door Chief Information Security Officer (CISO)	p. 9 en p. 19
23-09-2019	Versie 2.0. 3-jaarlijkse revisie	Geheel document
22-03-2022	Kleine actualisatie aanpassingen	
27-10-2023	Actualisatie n.a.v. nieuw IB-beleid	Geheel document
03-12-2024	Actualisatie nieuw IB-beleid	Geheel document
Dit document is een addendum op het strategisch informatiebeveiligingsbeleid 2025-2026		

Afkortingen en begrippenlijst

Begrip	
Code voor informatiebeveiliging	De Code voor Informatiebeveiliging beschrijft in 11 hoofdstukken normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging. De Code wordt uitgebracht door het Nederlands Normalisatie-instituut.
BIO	Baseline Informatieveiligheid Overheid
Afdeling WIZ	Afdeling Werk, Inkomen en Zorg
DT	Directie team gemeente Weert
Regeling SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
Divosa	is de Nederlandse vereniging van gemeentelijke managers op het terrein van participatie, werk en inkomen
AVG	Algemene Verordening Gegevensbescherming
AP	Autoriteit Persoonsgegevens
Informatie	Afdeling binnen de sector Bedrijfsvoering.
BKWI	Bureau Keteninformatisering Werk & Inkomen. Het BKWI ondersteunt en ontwikkelt met en voor ketenpartners ICT-oplossingen op functioneel en technisch gebied

Inleiding

Het Informatiebeveiligingsplan WIZ is een addendum op het informatiebeveiligingsbeleid gemeente Weert 2025-2026. In dit Informatiebeveiligingsplan worden de consequenties beschreven van de implementatie van het informatiebeveiligingsbeleid gemeente Weert 2025-2026 en de specifieke randvoorwaarden voor de afdeling WIZ en haar applicaties.

Reikwijdte

Applicaties

We maken hierbij onderscheid tussen de SUWI-applicatie en de overige applicaties waarmee de afdeling WIZ werkt zoals X-Works, Stratech Perspectief en JVS

SUWI-applicatie

De omgeving waarbinnen de normen geplaatst moet worden, wordt gedefinieerd door de volgende functies:

Suwinet-Inkijk

Direct en snel ophalen van gegevens op een gestandaardiseerde wijze via SUWINET. Inclusief de informatie van de VIP (Verificatie Informatie Persoonsbewijzen), dan wel het inlichtingenbureau.

Voor wie is Suwinet-Inkijk?

Suwinet-Inkijk is voor overheidsorganisaties die, voor het uitvoeren van hun wettelijke taken, gegevens van burgers en bedrijven nodig hebben. Suwinet-Inkijk maakt gebruik van geregistreerde gegevens van organisaties die zijn aangesloten op SUWINET.

Suwinet-Inkijk is niet vrijblijvend. Aan Suwinet-Inkijk zijn strikte regels verbonden.

Toegangsbeveiliging

Toegangsbeveiliging is een belangrijk onderdeel van Suwinet-Inkijk, niet alleen vanuit oogpunt van privacy, maar ook in relatie tot continuïteit is het van groot belang dat zeker kan worden gesteld dat alleen geautoriseerde gebruikers toegang hebben tot de SUWI-gegevens. De toegang tot Suwinet-Inkijk wordt geregeld door applicatiebeheer van de afdeling WIZ.

De formele procedure waarmee autorisatie en registratie van gebruikers tot Suwinet plaatsvindt en gecontroleerd wordt verloopt als volgt:

- Nieuwe medewerker;
- Teamleider/afdelingshoofd bepaalt aan de hand van de functieomschrijving welke autorisatie hij/zij krijgt;
- Betreffende teamleider/afdelingshoofd geeft aan applicatiebeheer wie de autorisatie tot SUWINET moet krijgen, waarbij rekening dient te worden gehouden met de functie;
- Er wordt een register/lijst van geautoriseerde medewerkers bijgehouden welke allemaal een geheimhoudingsverklaring hebben ondertekend;
- Twee maandelijks, tijdens regulier overleg Interne Controle Beveiliging (ICB), worden de accounts op actualiteit en volledigheid bekeken
- 4x per jaar vindt er een controle plaats door ICB op de BKWI gebruikersrapportage van SUWINET;
- Indien nodig, wordt naar aanleiding van de gebruikersrapportage een specifieke rapportage opgevraagd voor nader onderzoek;
- Bevindingen uit de rapportages worden vastgelegd in verslagen;
- Opvolging van de bevindingen vinden plaats tijdens het eerst volgende ICB-overleg.

Als een gebruiker voor de eerste keer inlogt, dan is hij/zij verplicht (door Suwinet-Inkijk) het wachtwoord te wijzigen. In dit geval dient het wachtwoord te voldoen aan de eisen zoals verwoord in SOP-408 Accountbeheer & Autorisaties. Aanvullende hierop geldt dat het wachtwoord voor het Suwinet-Inkijk account:

Het wachtwoord moet bestaan uit minimaal 8 tekens, waarvan in ieder geval één teken voorkomt uit elk van de onderstaande series:
o 0123456789
o ABCDEFGHIJKLMNOPQRSTUVWXYZ
o Abcdefghijklmnopqrstuvwxyz

o ~!@#$%^&*()-_=+[ ]{ }|;:,.<>/?
• Het wachtwoord mag niet gelijk zijn aan uw voornaam, uw achternaam of uw gebruikersnaam
• Het wachtwoord mag niet gelijk zijn aan één van de laatste 10 eerder gekozen wachtwoorden

Wanneer het wachtwoord van een gebruiker verloopt **(45 dagen niet gebruikt)**, verplicht Suwinet-Inkijk de gebruiker zijn/haar wachtwoord te veranderen.

Het gebruik van het account en wachtwoord is strikt persoonlijk en mogen onder geen beding worden gedeeld met anderen.

Het BKWI*, de organisatie achter Suwinet-Inkijk, rapporteert over het gebruik van de verschillende diensten op SUWINET aan de aangesloten partijen. Daartoe worden de activiteiten van SUWINET-gebruikers vastgelegd in logfiles.

Aan de hand van deze logfiles controleert het BKWI onder andere of:

- raadplegingen zijn gedaan buiten het klantenbestand,
- onevenredig veel zoekacties op 1 BSN zijn gedaan,
- iemand onevenredig veel raadplegingen doet,
- accounts zijn die niet of nauwelijks gebruik maken van Suwinet-Inkijk.

We maken gebruik van de GSD-rapportage Gemeente Weert Uitvoerend van het BKWI. Deze rapportage biedt inzicht in het gebruik van Suwinet Services door medewerkers van onze organisatie. Deze rapportage bevat vier onderdelen die achtereenvolgens het totale gebruik, het zorgvuldig gebruik, het accountbeheer en het doelmatig gebruik van Suwinet-Inkijk behandelen.

X-Works

Voor wie is *X-Works?*

X-Works biedt de klantmanagers en andere medewerkers alle informatie en ondersteuning binnen het sociaal domein, die nodig zijn om hun taken goed uit te voeren – van intake tot en met betaling en verantwoording, waarbij de uitstroom naar betaalde arbeid en een effectieve zorg vooropstaan.

Toegangsbeveiliging

Een door het afdelingshoofd/teamleider aangemelde medewerker krijgt toegang tot deze applicatie. Op basis van zijn/haar werkzaamheden krijgt hij/zij een rol toebedeeld binnen de applicatie. De autorisatie is beveiligd met naam en wachtwoord.

Het wachtwoord is door toepassing van single sign-on gemeentebreed niet opgeslagen in de applicatie. Daarnaast is de applicatie alleen te benaderen via het interne netwerk van de gemeente.

Het beheer van de applicatie is in handen van applicatiebeheer WIZ.

Via mutatietabellen is inzichtelijk te maken wie welke wijziging heeft aangebracht in bepaalde velden. Zodat achteraf altijd is vast te stellen wat de feitelijke situatie op een bepaald moment was.

Uitgangspunten Informatiebeveiliging

Het Normenkader Informatiebeveiliging SUWI gegevensuitwisseling – de sociale dienst/afdeling sociale zaken kent de volgende uitgangspunten en aannames:

De Regeling SUWI dient als basis voor het bepalen van het beveiligingsniveau voor de uitwisseling van gegevens binnen SUWI;

Het beveiligingsniveau is bepaald op basis van de betrouwbaarheidseisen die staan beschreven in bijlage XIV van de Regeling SUWI.

Het normenkader is erop gericht er zorg voor te dragen dat de verwerking en uitwisseling van persoonsgegevens tussen de SUWI-organisaties voldoet aan de wettelijke eisen.

Informatiebeveiliging is een lijnverantwoordelijkheid, conform het informatiebeveiligingsbeleid gemeente Weert 2025-2026.

Op grond van de AVG kan een cliënt bij de afdeling WIZ inzage vragen in of correctie vragen van gegevens. Zulke verzoeken vereisen een zorgvuldige behandeling. Datzelfde geldt, in nog sterkere mate, bij de verstrekking van gegevens aan derden. Deze verzoeken worden via de Privacy Officer opgepakt volgens het AVG-proces.

Naast deze privacyaspecten van de gegevensuitwisseling dienen ook algemene beveiligingsaspecten in acht te worden genomen. In artikel 13 AVG staat namelijk bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich brengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De vraag welke beveiligingsmaatregelen door gemeenten c.q. de sociale diensten/afdelingen sociale zaken moeten worden genomen in het kader van de gegevensuitwisseling die plaatsvindt via het SUWINET dient te worden beantwoord aan de hand van de maatregelen omschreven in de zogenaamde risicoklassen.

Aard van de gegevens Hoeveelheid van de gegevens	Persoonsgegevens	Bijzondere persoonsgegevens (Conform artikel 16 AVG)	Financiële en/of economische persoonsgegevens
Lage complexiteit van verwerking en Weinig persoonsgegevens	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Hoge complexiteit van verwerking en Veel persoonsgegevens	Risicoklasse I	Risicoklasse III	

Beveiligingsorganisatie

Organisatorische infrastructuur voor informatiebeveiliging

College van B&W is verantwoordelijk voor het gebruik van persoonsgegevens door medewerkers van de gemeente.

Binnen het management van de afdeling WIZ is informatiebeveiliging in gang gezet en wordt beheerst. In deze paragraaf is aangegeven op welke wijze dit wordt uitgevoerd.

Functioneel is het afdelingshoofd WIZ de informatiemanager van de afdeling WIZ.

In deze hoedanigheid is hij/zij verantwoordelijk voor informatiebeveiliging.

Op de afdeling WIZ zijn een drietal personen gezamenlijk verantwoordelijk voor de uitvoering van het beveiligingsbeleid en de daaruit voortvloeiende acties (verder aangeduid met driemanschap ICB).

Hiervoor is een driemanschap in het leven geroepen bestaande uit het afdelingshoofd, de interne controleur en één van de applicatiebeheerders.
Gezamenlijk dragen zij zorg voor het opstellen en onderhouden van dit beveiligingsplan.

Ook monitoren zij de uitvoering van de acties en aanbevelingen uit dit beveiligingsplan.

De Chief Information Security Officer (CISO) zal 2 keer per jaar de beveiliging rondom Suwinet controleren en beoordelen en rapporteren aan het hoogste management. Deze controle wordt o.a. uitgevoerd via het ENSIA-proces, waarbij de beveiliging van SUWINET geaudit wordt.

Beveiliging van toegang door derden

Zie: *SOP-402 – Applicatiebeheer*, paragraaf 6.4, *SOP-403 – Beheer van derde partijen*.

Uitbesteding

Data van de afdeling WIZ wordt grotendeels opgeslagen in de cloud. Dit geldt voor procesinformatie, persoonsgegevens en zaakgegevens. Documenten worden opgeslagen in DJUMA, wat ook een cloud

toepassing is. Werkkopieën van documenten kunnen op het netwerk van de gemeente Weert worden opgeslagen.

De beveiliging van de data bij de afdeling WIZ is deels uitbesteed. Alle data worden geback-upt, om bij dataverlies terug te kunnen vallen op de oorspronkelijke situatie. De back-upfaciliteit vindt buitenshuis plaats bij ICTNML, de IT-dienstverlener van de gemeente Weert.

Het verkeer tussen het lokale netwerk en het internet wordt beveiligd met een firewall. Deze firewall is in het beheer van ICTNML. De gemeente Weert kan via de CISO of applicatiebeheerder aanpassingen aanvragen in de firewall die relevant zijn voor de werking van de applicatie. Tevens wordt er monitoring uitgevoerd middels een SIEMSOC op de gehele omgeving van de gemeente Weert.

Classificatie en beheer van bedrijfsmiddelen

Classificatie van informatie

Zie SOP-103 – Classificatie van Informatie

In deze paragraaf wordt aangegeven op welke wijze informatie binnen de afdeling WIZ is gecategoriseerd. Binnen de afdeling WIZ wordt gewerkt met persoonsgegevens die aangemerkt kunnen worden als bijzondere persoonsgegevens zoals beschreven in de AVG. Deze gegevens kunnen niet specifiek onderscheiden worden binnen de gegevensuitwisseling en gezien het grote aantal uitwisselingen, wordt de risicoklasse van de gegevens vastgesteld op een combinatie van II en III.

Logbestanden en de gebruikersadministratie bevatten persoonsgegevens van medewerkers. De gegevens die worden vastgelegd in deze bestanden worden vastgelegd in risicoklasse I.

Voor de afdeling Werk, Inkomen en Zorg van de gemeente Weert geldt dat de gemelde registraties als volgt worden gecategoriseerd.

Soort verwerking	*Indeling in risicoklassen*
Uitkeringenadministratie	**Klasse 2 / Klasse 3**
Suwinet- Inkijk	**Klasse 2 / Klasse 3**
Sociale recherche (frauderegistratie)	**Klasse 2 / Klasse 3**

Om te voorkomen dat medewerkers van de dienst bij een eventuele crash van het netwerkgegevens over langere tijd kwijt zijn, worden dagelijks back-ups gedraaid van alle servers. Concreet betekent dit dat alle gegevens die zich op de servers bevinden (data, rapporten, beschikkingen etc.) elke avond worden opgeslagen. Het feitelijk uitvoeren van de back-ups wordt uitgevoerd door ICTNML voor de lokale data. De clouddata wordt door de cloudleverancier gebackupt. In geval van een calamiteit, wordt door het crisisteam bepaald welke processen als eerste worden hersteld, waarbij publiekzaken en het sociaal domein altijd een hoge prioriteit behoeven i.v.m. de relatie en dienstverlening naar de burgers.

Beveiligingseisen ten aanzien van personeel

Beveiligingseisen bij aanname van personeel

Zie hiervoor het intranet: *OCTO/Service Plein*

Gebruikers van geautomatiseerde systemen

Applicatiebeheer van de afdeling WIZ instrueert de individuele gebruiker over correcte omgang met ICT-toepassingen.

Binnen de afdeling WIZ wordt met betrekking tot SUWINET een gebruikershandleiding beschikbaar gesteld aan alle nieuwe gebruikers.

Nieuwsbrieven en tips met betrekking tot het gebruik van bepaalde applicaties worden gedeeld met alle gebruikers. Dit wordt via e-mail of OCTO bekend gemaakt.

Tijdens het inwerken door de naaste collega worden de nieuwe medewerkers in kennis gesteld van het gebruik van privacygevoelige informatie.

In welke situatie al dan niet informatie aan klanten en/of derden verstrekt mag worden, is ingegeven wat hierover in de PW staat.

Reageren op incidenten en storingen

In deze paragraaf is aangegeven op welke wijze de afdeling WIZ-incidenten die de beveiliging aantasten verwerkt en registreert.

Wanneer zich binnen de afdeling WIZ een storing voordoet wordt dit in eerste instantie gemeld bij applicatiebeheer. Deze beoordeeld of dit een applicatiegerelateerde of systeemtechnische melding is. In het eerste geval zal applicatiebeheer zelf de storing proberen op te lossen.

Een systeemtechnische melding wordt telefonisch doorgegeven aan ICTNML.

Zie hiervoor *SOP-418 Call- & Incident Management*.

In een escalatieprocedure is voorzien. Het afdelingshoofd WIZ zal dan contact zoeken met ICTNML.

Indien het om een informatiebeveiligingsincident gaat, wordt ICTNML gebeld conform proces en zal z.s.m. de CISO worden ingelicht.

Rapporteren van onvolkomenheden in de software

Bij de afdeling WIZ is applicatiebeheer verantwoordelijk voor X-Works, SUWINET en de overige applicaties.

Bij eventuele problemen op softwaregebied zijn zij degene die als aanspreekpunt fungeren voor de medewerkers.

Applicatiebeheer beschikt over telefoonnummers van de diverse servicedesks en helpdesk van leveranciers en overheidsorganisaties.

Storingen, wensen en gebruikersvragen kunnen zowel telefonisch als via de mail worden aangeleverd. Veelal krijg je hiervan een terugkoppeling via een call-nummer, zodat je de voortgang kunt volgen.

Bij Blinqt, de leverancier van X-Works, wordt een programmafout uiteindelijk op een meldingenlijst geplaatst.Deze worden niet meteen opgelost maar zullen gebundeld worden opgelost. Dit kan in een patch op de software of met een nieuwe release.

Betreft het een storing in de besturingssoftware of in de communicatie, dan wordt zoals in hoofdstuk 6.3 beschreven ICT ingeschakeld.

Lering trekken uit incidenten

Er is binnen de afdeling WIZ geen apart softwarepakket dat fungeert als een registratiesysteem voor incidenten. ICTNML beschikt wel over een dergelijke tool (Topdesk) en wordt zodoende gebruikt.

Fysieke beveiliging en beveiliging van de omgeving

Beveiligde ruimten

Zie hiervoor *SOP-216 – Fysieke Beveiliging en* In de SLA en TPM van ICT-NML

Fysieke beveiliging en toegang bezoekers WIZ

Bij de afdeling WIZ is een deel van het gebouw toegankelijk voor publiek. Die zonder beperkingen te betreden zijn voor bezoekers.

De hoofdingang (bezoekersingang)

1. Bezoek (zowel aangekondigd als onaangekondigd) dient zich te melden bij de receptie.

De wachtruimten voor de balies en de spreekkamers is voor publiek vrij toegankelijk.

In de wachtruimten wordt door het AOT (Alarm Opvolg Team) opgetreden bij dreigende situaties.

In de spreekkamers is het meubilair gezekerd. De deuren zijn via aparte sloten beveiligd.

De personeelsingang en de werkruimten worden beveiligd door middel van een badgelezer.

Beheer van communicatie- en bedieningsprocessen

Bedieningsprocedures en verantwoordelijkheden

In deze paragraaf is beschreven welke procedures er gelden binnen de afdeling WIZ op het gebied van aanpassingen, incidenten en functiescheiding op ICT-gebied.
Bijna alle werkprocessen die gebruikt worden in het primaire proces van de afdeling WIZ, zijn gedocumenteerd met behulp van werkinstructies en werkbeschrijvingen.

Wijzigingen in deze processen leiden tot gewijzigde instructies. Op deze manier hebben de medewerkers van de afdeling WIZ altijd de beschikking over bijgewerkte instructies en beschrijvingen om de werkzaamheden uit te voeren.

De implementatie van nieuwe releases wordt in samenspraak met ICT uitgevoerd. In overleg met de afdeling WIZ wordt een datum geprikt om tot feitelijke installatie over te gaan. Dit zal eerst in een testomgeving worden uitgevoerd. Na een succesvolle test wordt dezelfde procedure herhaald maar dan in de productieomgeving.

Dit geldt voor alle primaire applicaties.

Wanneer op ICT-gebied veranderingen plaatsvinden worden de medewerkers van de dienst daarover in kennis gesteld. Bij kleinere ingrepen via de e-mail, bij projecten met een grotere impact via het afdelingshoofd van de afdeling WIZ.

Enkel medewerkers van de ICT zijn bevoegd om wijzigingen in de ICT-infrastructuur aan te brengen. Op deze manier wordt voorkomen dat op verschillende plaatsen binnen de organisatie wijzigingen plaatsvinden en kunnen de zaken beheerst worden.

Iedere medewerker van de afdeling WIZ heeft enkel toegang tot ICT-voorzieningen die noodzakelijk zijn voor de uitoefening van zijn/haar werkzaamheden.

Er is een duidelijke functiescheiding.

Per functionaris verschillen, indien van toepassing, de autorisaties. Op deze manier wordt de privacy gewaarborgd en wordt het principe need-to-know toegepast.

Achteraf en ook vooraf (nog voordat er een besluit is genomen) vindt controle plaats op het gebied van de rechtmatigheid van de primaire processen. Deze controle wordt uitgevoerd door de kwaliteitsmedewerker WIZ (vooraf en achteraf) en de Intern Controleur (steekproefsgewijs achteraf).

Systeemplanning en acceptatie

Aangegeven wordt op welke manier nieuwe patches en releases worden geïmplementeerd.
Bij ICT wordt periodiek bekeken of de capaciteit van de verschillende servers van de gemeente nog voldoende is. De medewerkers van de afdeling WIZ hebben in deze geen rol.

Nieuwe releases en updates worden meteen in de testomgeving geïnstalleerd, en pas na een test vrijgegeven voor productie.

Acceptatie gebeurt zowel door applicatiebeheer als door gebruikers die vooraf benaderd zijn om de nieuwe release te beoordelen. Op basis van hun werk/discipline worden gebruikers benaderd om de geboden oplossingen van de leverancier te testen.

Toegangsbeveiliging

Beleid ten aanzien van toegangsbeveiliging

Zie SOP-408 - Accountbeheer & Authorisaties.

Binnen de afdeling WIZ is vastgelegd dat enkel personen die binding hebben met de primaire processen toegang krijgen tot SUWINET en de overige applicaties. Ondersteunende afdelingen hebben in principe geen toegang tot SUWINET. In het kader van de informatievoorziening ontvangt iedere medewerker enkel autorisaties voor de voor hem belangrijke applicaties.

Continuïteitsmanagement

Zie SOP-205 – Disaster Recovery

Naleving

ICB (interne controle beveiliging)

Binnen de afdeling WIZ is een driemanschap ICB (interne controle beveiliging) ingesteld bestaande uit:

het afdelingshoofd, de beleidsmedewerker IC, en een applicatiebeheerder.

Deze hebben elke twee maanden overleg over informatiebeveiliging. Tijdens dit overleg worden operationele veranderingen op de afdeling besproken. 4 keer per jaar wordt het BKWI-rapport, dat elk kwartaal door de applicatiebeheerder wordt opgevraagd, besproken. De analyse/ bevindingen

worden in een verslag / rapport vastgelegd. Evident dat daarnaast op landelijke en regionale incidenten alert en adequaat gereageerd wordt**.**

In opdracht van de VNG heeft de IBD (Informatiebeveiligingsdienst voor gemeenten) een baseline informatiebeveiliging overheid (BIO).

Dit basisnormenkader informatieveiligheid voor overheid stelt ons in staat om te meten of we de basis op orde hebben en of we voldoen aan normen en wettelijke voorschriften op het gebeid van informatiebeveiliging.

Samen met de rapportages gebruik Suwinet services en de door applicatiebeheer geregistreerde opmerkingen vormt dit de basis voor het ICB-overleg.

Bijlagen

1. 10 gouden regels
2. Autorisatiematrix

Bijlage 1) Tien gouden regels: voor het gebruik van informatie, informatiesystemen en netwerken.

Wij vragen even om jouw aandacht!

Afhankelijk van jouw functie heb jij toegang tot diverse informatiesystemen binnen de afdeling WIZ. Wij willen je erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen. Met deze *tien gouden regels* vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van je functie binnen de afdeling WIZ.

1. **Wachtwoorden zijn strikt persoonlijk**

Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden of een collega en bewaar ze op een *veilige* plek, dus *niet* in je agenda of op een geel briefje!

2. **Melden van beveiligingsincidenten**

Softwarematige beveiligingsincidenten meld je zo snel als mogelijk bij ICTNML en de CISO. Voorbeelden van een dergelijk incident is een virusmelding op het systeem.

Een ander beveiligingsincident bijvoorbeeld een deur die op slot had moeten zijn maar niet op slot is, meld je bij je teamleider/afdelingshoofd.

3. **Geheimhoudingsplicht**

Binnen de sociale dienst/afdeling sociale zaken wordt veel met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (AVG). In de wet SUWI en in de CAO zijn daarom geheimhoudingsbepalingen opgenomen die inhouden dat je de persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die vanuit je werkzaamheden bekend worden, evenals overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat geheimhouding verplicht is.

4. **Gedragscode Internet- en e-mailgebruik**

Er is geen gedragscode voor Internet- en e-mailgebruik die aangeven hoe de medewerkers van de afdeling WIZ behoren om te gaan met Internet en e-mail op de werkplek.

E-mail-verkeer geldt inmiddels als algemeen geaccepteerde correspondentie, gelijk aan brieven. E-mails kunnen, mits de betrouwbaarheid van het e-mailadres voldoende is aangetoond, gelden als bewijsstuk.

Bovenstaande alinea is enkel van toepassing voor e-mail-verkeer tussen de afdeling WIZ en instanties!

Contactpersonen kunnen door middel van het verzenden van e-mail op een snelle manier informatie uitwisselen over individuele klanten.

E-mail-verkeer tussen klanten en medewerkers van de afdeling WIZ wordt ten zeerste afgeraden omdat deze correspondentie niet centraal wordt geregistreerd (voorzetting huidige werkwijze).

E-mails die klanten versturen aan hun contactpersoon worden niet gezien als bewijsstuk.

5. **Kennisnemen van het informatiebeveiligingsbeleid**

Het binnen de afdeling WIZ geldende informatiebeveiligingsbeleid en de bijbehorende richtlijnen, instructies en protocollen zijn op iedereen in onze organisatie van toepassing. Vraag je leidinggevende voor meer informatie hierover.

6. **Gegevensverstrekking aan derden via de telefoon**

Het uitgangspunt is dat er niet aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dat betekent dat er ook geen telefonische informatie over klanten wordt verstrekt aan personen of instanties die beweren namens de betrokkene te bellen. Vragen dienen schriftelijk bij de afdeling WIZ te worden ingediend. Enkel in uitzonderlijke gevallen kan informatie verstrekt worden aan derden, indien de identiteit van deze voldoende vastgesteld kan worden (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie **niet** mogelijk is.

7. **Clear desk/ clear screen policy**

De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegde niet in jouw afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je werkstation bewust dient te vergrendelen met behulp van de screensaver (toetscombinatie (Windowsvlag + L) wanneer jij je werkplek verlaat. Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau/spreekkamer of in een niet afsluitbare kast blijven liggen.

8. **Geen vertrouwelijke gegevens in de prullenbak**

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de afdeling WIZ. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Daarom zijn er speciale gekenmerkte papiercontainers binnen de afdeling WIZ aanwezig (de blauwe containers). Maak hiervan gebruik en stop vertrouwelijke gegevens *nooit* in de prullenbak of in een bak op je kamer die bestemd is voor oud-papier.

9. **Aanspreken van onbekende personen**

Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat zij daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag, wat hij of zij hier komt doen. Nieuwe collega's, uitzendkrachten of ander ingehuurd personeel stellen het op prijs om aangesproken te worden en op deze manier contacten te kunnen leggen. Echter, personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Wijs hun beleeft, maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleidt ze daar naartoe.

10. **Haast, stress, werkdrukte vs. informatiebeveiliging**

Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdrukte hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk binnen de afdeling WIZ en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus – je cliënten vertrouwen erop!

Bijlage 2) autorisatiematrix

Weert, 17 december 2024

Burgemeester en wethouders van Weert,

Namens deze,

Het hoofd van de afdeling Werk, Inkomen en Zorg