GBTwente

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 934

25 september 2023

Officiële uitgave van de gemeenschappelijke regeling Gemeenschappelijke Regeling Gemeentelijk Belastingkantoor Twente

Addendum Strategisch Informatiebeveiligingsbeleid GBTwente 2023 tot 2026

Voorstel voor het algemeen bestuur van GBTwente
Van Het dagelijks bestuur van GBTwente
Vergaderdatum 12 juli 2023

Voorstel
Kennisnemen van het addendum bij het Strategisch Informatiebeveiligingsbeleid GBTwente.

Toelichting
Op 5 april heeft het dagelijks bestuur van GBTwente het Strategisch Informatiebeveiligings-beleid GBTwente 2023 tot 2026 vastgesteld. Vanuit de DigID audit zijn echter een aantal aanvullende eisen gesteld waaraan een Strategisch Informatiebeveiligingsbeleid moet voldoen. Aan deze aanvullende eisen wordt voldaan door het bijgevoegde addendum.

Bijlage
Bijlage E: Addendum bij Strategisch Informatiebeveiligingsbeleid GBTwente 2023 -2026: DigiD-uitwerking norm B.01

Besluit
Het algemeen bestuur van de gemeenschappelijke regeling Gemeentelijk Belastingkantoor Twente heeft kennis genomen van het addendum bij het Strategisch Informatiebeveiligings- beleid GBTwente.

Ondertekening
Secretaris,
De heer J.A.G. Cloosterman
.....
Voorzitter,
Mevrouw E. Zinkweg-Ankone
.....

Bijlage E Addendum bij Strategisch Informatiebeveiligingsbeleid GBTwente 2023 -2026: DigiD-uitwerking norm B.01

In aanvulling op bovengenoemd informatiebeveiligingsbeleid (dat integraal van toepassing is op al onze DigiD-aansluitingen) zijn voor DigiD de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen
• We conformeren ons aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD versie 3.0.
• Jaarlijks wordt dit normenstelsel in het kader van de DigID audit door een externe auditor en CISO getoetst.
• Over deze toetsing vindt verantwoording plaats naar Logius (verticaal) en naar de directeur (horizontaal)) verantwoording plaats.

Eigenaarschap
• Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende manager, de manager Bedrijfsvoering, eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer
• Per DigiD-aansluiting zijn door de manager Bedrijfsvoering twee functioneel beheerders [Bianca ten Berge en Nick Duursema] aangewezen die de verantwoordelijkheid hebben de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
• Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, tav DNSSEC) en de beoordeelde releases (C.08).
• Tweemaal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk manager, te weten het manager Bedrijfsvoering.

Technisch
• Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.