



Algemeen Bestuur

VERGADERDATUM

14 oktober 2022

STUKDATUM

5 oktober 2022

PROCES

Ondersteunen

ONDERWERP

Strategisch Informatiebeveiligings-
beleid GBLT 2022-2025

STELLERS

Arjan de Wit en
Gertjan Post

EIGENAAR

Johnny Blankvoort

VERTROUWELIJK

Nee

Voorstel

Rubriek: *Ter info*

Het algemeen bestuur wordt gevraagd kennis te nemen van het voorliggende strategisch informatiebeveiligingsbeleid GBLT 2022-2025.

Samenvatting

Beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zijn van groot belang. Hoe we deze aspecten bij GBLT borgen wordt vastgesteld in het strategisch informatiebeveiligingsbeleid. Het strategisch informatiebeveiligingsbeleid van GBLT voor de jaren 2022-2025 wordt gebruikt als basis voor de verdere invulling van het tactische informatiebeveiligingsplan en daarmee geeft het richting aan de verdere invulling van het informatiebeveiligingsbeleid op operationeel niveau.

Stappen in de besluitvorming

Het strategisch informatiebeveiligingsbeleid GBLT 2022-2025 is voorbesproken in het ABC&P overleg van 3 mei 2022. Op 1 juni 2022 en 14 september 2022 is het strategisch informatiebeveiligingsbeleid GBLT 2022-2025 ter goedkeuring aan het MT aangeboden. De opmerkingen en aanvullingen zijn verwerkt in deze definitieve versie. Het strategisch informatiebeveiligingsbeleid is vastgesteld in het dagelijks bestuur van 5 oktober 2022 en wordt ter informatie aangeboden aan het algemeen bestuur.

Toelichting

Zie het strategisch informatiebeveiligingsbeleid GBLT 2022-2025 in de bijlage.

Personele gevolgen

GBLT houdt zich aan de wet. Informatie over klanten, deelnemers en medewerkers wordt zo zorgvuldig als mogelijk behandeld. Aandacht hiervoor hoort bij de proactieve houding van iedere medewerker, tegelijkertijd worden er niet meer maatregelen genomen dan noodzakelijk om het ondernemende en creatieve karakter van GBLT niet te frustreren.

Informatiebeveiliging is ieders verantwoordelijkheid en een lijnverantwoordelijkheid. Proceseigenaren dragen de primaire verantwoordelijkheid voor een goede informatiebeveiliging binnen hun proces. Alle



informatiesystemen worden geclassificeerd op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid; deze classificatie bepaalt het niveau van de beveiligingsmaatregelen.

Financiële gevolgen

Eventuele financiële gevolgen volgen uit het nog op te stellen informatiebeveiligingsplan.

Architectuurtoets

N.v.t.

Juridische gevolgen

GBLT is sinds 1 januari 2019 verplicht de Baseline Informatiebeveiliging Overheid (BIO) toe te passen.

Publicatie

Na vaststelling van het strategisch informatiebeveiligingsbeleid GBLT 2022–2025 door het Dagelijks Bestuur wordt het gepubliceerd op www.overheid.nl.

Communicatie

Communicatie over en bewustwording van informatiebeveiliging binnen GBLT is belangrijk. Na vaststelling van het strategisch informatiebeveiligingsbeleid GBLT 2022–2025 door het Dagelijks Bestuur wordt hierover gecommuniceerd via Loek.

Het Dagelijkse Bestuur wordt via bestuursrapportages geïnformeerd over de mate waarin invulling is gegeven aan het strategische informatiebeveiligingsbeleid.

Gevolgen voor privacy en informatiebeveiligingsrisico's

Eventuele gevolgen voor (het wegnemen van) informatiebeveiligingsrisico's volgen uit het nog op te stellen informatiebeveiligingsplan.

Andere uitvoeringsgevolgen en risico's

N.v.t.

Evaluatie

Het strategisch informatiebeveiligingsbeleid GBLT 2022–2025 bestrijkt 3 jaar. Daarna wordt het strategisch informatiebeveiligingsbeleid weer geactualiseerd.

Bijlagen

Strategisch Informatiebeveiligingsbeleid GBLT 2022–2025 v1.02