LOGGING BELEID

VGGM

Veiligheids- en Gezondheidsregio Gelderland-Midden

www.vggm.nl

Versie informatie

Versie	Datum	Auteur	Aanpassing
0.1	14-4-2020	[redacted]	Concept
0.2	11-9-2020	[redacted]	Concept, opnieuw opgemaakt op basis van de Handreiking Aanwijzing Logging van de IBD
1.0	18-9-2020	[redacted]	Definitief

Distributielijst

Versie	Datum	Verzonden aan
0.1	14-4-2020	[redacted]
0.2	11-9-2020	[redacted]
1.0	18-9-2020	Publicatie op Alfresco

Gerelateerde documenten

Versie	Datum	Document
1.3	Juli 2019	Informatiebeveiligingsbeleid VGGM 2019
		https://cip-overheid.nl/media/1169/bid-operationale-producten-bir-015-logging-beleid-10.pdf

Beleidsuitgangspunten Logging VGGM

Ten behoeve van de beveiliging van informatie is er een logging-beleid voor alle ICT-voorzieningen. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie tot logging genomen moeten worden. VGGM hanteert de volgende beleidsuitgangspunten welke zijn ontleend aan de NEN7510:2017 en de Baseline Informatiebeveiliging Overheid (BIO) en aanvullend zijn op het informatiebeveiligingsbeleid. Dit beleid is van toepassing op de ICT-voorzieningen welke in het beheer zijn van VGGM. Indien er sprake is van *Software-as-a-Service*, zullen er afspraken over logging gemaakt worden met de betreffende leverancier.

Uitgangspunten logging

[redacted]

:

- [redacted]

3. [redacted]

[redacted]

Controle van het beleid op systeemgebruik

Er zijn binnen VGGM procedures vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een logboek door bijvoorbeeld beheerders.

[redacted]

Bescherming van informatie in logbestanden

Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:

1. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
2. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
3. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
4. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
5. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het ‘vier ogen’ principe toegepast worden.
6. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de

systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.

7. Het goed functioneren van de logging wordt continue gemonitord voor essentiële systemen.
8. Controle op opslag van de logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is).

Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van VGGM behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

1. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.