

Beleidsdocument koppelingen derden ICT

Versie 0.3 (26-10-2022)

Inhoud

1. Toegang tot systemen voor support	2
1.1. Toegang via Team Viewer	2
1.2. Toegang op locatie	2
1.3. Toegang via een IPsec verbinding	2
2. Afname van een cloud dienst (SaaS)	2
2.1. Systemen up-to-date	2
2.2. Bescherming van de data	2
2.3. Datadumps	2
3. On-premise appliance	3
3.1. Eenmalige installatie	3
3.2. Volledig gemanaged	3
4. Software updates	3
4.1. Windows updates interne servers	3
4.2. Common Vulnerabilities and Exposures (CVE)	3
5. Uitwisseling bestanden	3
5.1. Bestanden vanuit de gemeente Almelo	3
5.2. Management informatie	3
6. Mailen namens de gemeente Almelo	4
7. IPsec verbinding	4
8. Authenticatie	4
8.1. Multi-Factor Authentication (MFA)	5
8.2. Single Sign-On (SSO)	5
9. Overige eisen	5

1. Toegang tot systemen voor support

Toegang tot de systemen van de gemeente Almelo voor externen wordt alleen verleend op afstand middels Team Viewer of op locatie.

1.1. Toegang via Team Viewer

Een Team Viewer sessie wordt minimaal 24 uur van te voren gepland met de betreffende ICT medewerker van de gemeente Almelo. De medewerker van de gemeente Almelo moet gedurende de hele sessie meekijken.

1.2. Toegang op locatie

Eventuele toegang tot de systemen op locatie wordt minimaal 24 uur van te voren aangevraagd. In overleg met de betreffende ICT medewerker van de gemeente Almelo wordt een geschikt moment afgesproken om op locatie te komen. De gemeente Almelo medewerker moet gedurende werkzaamheden toezicht houden.

1.3. Toegang via een IPsec verbinding

In sommige gevallen zal er worden gekozen om een IPsec verbinding op te zetten tussen de gemeente en de externe partij (zie punt 7). In dat geval kan er voor worden gekozen om deze IPsec verbinding ook te gebruiken voor de externe toegang.

2. Afname van een cloud dienst (SaaS)

Onder een cloud dienst wordt bedoeld een dienst of oplossing die volledig bij de externe partij staat en niet onder het beheer valt van de gemeente, ofwel een SaaS oplossing.

2.1. Systemen up-to-date

Bij de afname van een SaaS oplossing moet de leverancier er voor zorgen dat de systemen up-to-date zijn en beschermd zijn tegen de nieuwste virussen en zwakheden in de systemen. (zie punt 4.2)

2.2. Bescherming van de data

De data die bij de externe leverancier wordt opgeslagen mag alleen beschikbaar zijn voor de gemeente Almelo. Bij blijf van (mogelijke) toegankelijkheid voor anderen moet dit direct gemeld worden aan de gemeente Almelo.

2.3. Datadumps

Bij databases moeten met regelmaat datadumps beschikbaar worden gesteld (zie 5.2)

3. On-premise appliance

Bij een on-premise appliance onderscheiden we 2 soorten.

3.1. Eenmalige installatie

Support op basis van facturatie. Toegang gebeurt op basis van punt 1

3.2. Volledig gemanaged

Hierbij blijft de externe partij volledig verantwoordelijk voor de appliance en de benodigde software en security updates (zie punt 4.2)

De OS versie van de appliance mag maximaal 1 major versie achter lopen.

Eventueel kan er een onderhoudscontract worden opgesteld tbv installatie updates

Voor het financiële systeem gaat het om een SAAS applicatie.

4. Software updates

Updates en patches zijn er om de functionaliteit en de beveiliging te verbeteren, en mogen daarom nooit als een belemmering voor de functionaliteit van een dienst of stuk software worden gezien.

4.1. Windows updates interne servers

De gemeente Almelo volgt het update schema van Microsoft (12 per jaar). Waarbij de laatste Windows updates worden uitgerold op de servers. Software van leveranciers mag functioneel geen last hebben van deze updates. Is dit wel het geval dan komt de leverancier binnen 3 weken met een oplossing op de betreffende updates wel door te kunnen voeren.

4.2. Common Vulnerabilities and Exposures (CVE)

Een leverancier dient bij het bekendmaken van een CVE die van toepassing kan zijn op de geleverde dienst/software binnen 3 weken met een patch of update te komen die deze CVE tegen gaat.

5. Uitwisseling bestanden

5.1. Bestanden vanuit de gemeente Almelo

Voor de uitwisseling van bestanden naar derden gebruikt de gemeente Almelo momenteel Citrix ShareFile. Deze is bereikbaar op <https://gemeentealmelo.sharefile.eu>

Deze oplossing wordt medio 2022 vervangen door Ondrive/Teams of/Of SmartLockR.

5.2. Management informatie

Voor het verschaffen van management informatie is het nodig dat er data dumps van databases beschikbaar worden gesteld. De datadumps kunnen op meerdere manieren bij ons binnen komen. Op volgorde van voorkeur zijn dat:

- De bestanden worden door de externe partij op de ShareFile omgeving van de gemeente Almelo geplaatst
- De bestanden worden door de gemeente Almelo middels SFTP opgehaald bij de externe partij. De externe partij zal hiervoor dus een SFTP locatie beschikbaar moeten stellen.
- De bestanden kunnen worden overgedragen via een IPsec verbinding. (zie punt 7)
- Geautomatiseerd voorkeur via SFTP. Incidenteel via SF.

6. Mailen namens de gemeente Almelo

Als een dienst of oplossing buiten de gemeente staat en er moet vanuit de oplossing gemaild worden namens de gemeente Almelo, dus met een @almelo.nl adres, dan moet aan het volgende worden voldaan:

- De leverancier moet vooraf een SPF record of maximaal één mailserver doorgeven welke wij kunnen opnemen in ons SPF record.
- De leverancier moet de mail kunnen beveiligen met een DKIM signature waarbij de public DKIM key wordt opgenomen in de DNS van de gemeente.

Moderne standaarden zoals DNSSEC moeten gevolgd worden.

7. IPsec verbinding

In bepaalde gevallen is het wenselijk om een IPsec verbinding op te zetten met de externe partij. De gemeente zal hiervoor een document aanleveren voor het bepalen van de gewenste instellingen van de IPsec verbinding. Criteria voor een IPsec verbinding zijn:

- Er moet continue veel data worden uitgewisseld wat niet via een SSL connectie kan. Denk bijvoorbeeld aan SQL data.
- Er moet monitoring plaatsvinden op bepaalde interne systemen, onderdeel van een appliance

8. Authenticatie

Bij een inlog mogelijkheid die vanaf het internet bereikbaar is eist de gemeente Almelo meer dan alleen een gebruikersnaam en password. Daarom hanteren we de volgende vormen van authenticatie.

8.1. Multi-Factor Authentication (MFA)

Multi-factor authenticatie is een combinatie van meerdere factoren om de identiteit van een persoon vast te stellen. De gemeente Almelo gaat uit van een combinatie van 2 verschillende factoren.

- **Iets wat je weet:** username, password, ID nummer
- **Iets wat je hebt:** een telefoon, SMS code, authenticator app, token, toegangspas, IP adres, certificaat.
- **Iets wat je bent:** Iris scan, vingerafdruk, stemherkenning
- **Waar je bent:** GPS coördinaten

8.2. Single Sign-On (SSO)

- Single Sign-On gebeurt bij voorkeur op basis van Azure ADFS.
- Bij een on-premise appliance moet er een AD/LDAP koppeling worden gelegd voor authenticatie.

9. Overige eisen

- Webapplicatie moeten werken in Edge Chromium of Google Chrome.
- De applicatie moet werken in een Citrix Xenapp omgeving beheerd met Ivanti Workspace manager.
- Eventuele distributie middels Ivanti Automation manager of Microsoft Intune.
- Naast Citrix moet de applicatie werken op de lokale Windows 10/11 (of hoger) notebooks, en MAC OS 12.x (of hoger) omgeving beheerd door MS Intune.
- Bij een mobiele app/site Iphone/Ipad OS van 15 of hoger beheerd door MS Intune.
- Software wordt gescand met Cisco AMP Antivirus.
- Een verwerkersovereenkomst moet worden opgesteld.
- Architectuur platen moeten vooraf worden aangeleverd, waarbij duidelijk is welke servers/applicaties met elkaar moeten communiceren en over welke (TCP/UDP) poorten deze communicatie plaats vindt. Voorkeur via Blue Dolphin (Archimate) of Visio
- Software integratie met de office suite moet kunnen werken met de Office 365 click-to-run.
- IPv6
- Data staat in de EEG.
- VNG Eisen
- GIBIT Inkoopvoorwaarden
- BIO
- AVG
- WMEBV (per 1-2-2023)
- Een medewerker van de gemeente Almelo hoeft zich slechts eenmalig aan te melden bij de Identity Provider (Single Sign-on). Nieuwe software notie van te hebben en de medewerker niet nogmaals om inloggegevens te vragen. Het gebruik van IdP initiated SSO is niet toegestaan.