



OKTOBER 2024 | VERSIE 2.6

Team Automatisering
Standaarden ICT-Infrastructuur

Documentgegevens

Team Automatisering – Standaarden ICT-Infrastructuur uitgegeven door

Bedrijfsgegevens

Bedrijf	Gemeente Emmen Raadhuisplein 1 7811 AP Emmen
Afdeling	Team Automatisering

Documentgegevens

Titel	Team Automatisering – Standaarden ICT-Infrastructuur
Bestandsnaam	Standaarden ICT-Infrastructuur v2.6.docx
Locatie	https://werksamen.sharepoint.com/sites/sps-EMM-KB-AUT/Gedeelde documenten/Werkafspraken/ICTstandaarden/Standaarden ICT-Infrastructuur v2.6.docx
Status	<input type="checkbox"/> Concept <input checked="" type="checkbox"/> Definitief
Classificatie	<input checked="" type="checkbox"/> Openbaar <input checked="" type="checkbox"/> Intern <input checked="" type="checkbox"/> Klant <input checked="" type="checkbox"/> Vertrouwelijk
Datum	woensdag 20 november 2024
Versie	2.6
Aantal pagina's	20

Document opsteller(s)

Naam	Afdeling	Functie
George de Vries	Team Automatisering	A. Architect
Frank Heemsbergen	Team Automatisering	Beleidsadviseur

Document reviewer(s)

Naam	Afdeling	Functie
Duncan den Boer	Team Automatisering	Teamleider
Anke Lübbers	Team Automatisering	Service Level Manager
Marcel Meijer	Team Automatisering	Coördinator Team AUT
Peter Mijnheer	Team Informatisering	I-Regisseur

Versiebeheer

Versie	Datum	Auteur
2.1	14-06-2023	Coördinator Back Office

Wijziging historie (vanaf versie 1.0)

Versie	Datum	Auteur	Beschrijving
1.5	11-07-2022	George de Vries	Initiële opzet
1.6	25-07-2022	Frank Heemsbergen	Review en toevoegingen
1.9	06-12-2022	George de Vries	Goedgekeurde nieuwe eisen toegevoegd
2.0	06-12-2022	George de Vries	Definitieve versie
2.1	17-5-2023	Frank Heemsbergen	Tekstuele aanpassingen, versienummers vervangen door N-2
2.2	13-09-2023	George de Vries	Nieuwe aanvullingen en/of inzichten
2.5	17-06-2024	George de Vries	Leesbaarheid, MS Graph, Internet en Beveiliging
2.6	20-11-2024	George de Vries	Internet en beveiliging verplaatst naar H4

Documentverwijzing

Versie	Datum	Auteur	Beschrijving
1.3.13	19-01-2022	Marcel Meijer	Standaarden ICT-Infrastructuur

Inhoudsopgave

1	Inleiding	4
1.1	Aanleiding	4
1.2	Afbakening	4
2	Leeswijzer	5
3	Eisen	6
3.1	Techniek	6
3.2	Applicaties	7
3.3	Database	8
3.4	Algemeen	8
4	Eisen en wensen overzicht	9
4.1	Internet en Beveiliging	10
4.1.1	Bescherming tegen e-mailphishing	11
4.1.2	Mailservers	11
4.1.3	DNSSEC	11
4.1.4	IPv6 en IPv4	11
4.1.5	TLS	11
4.1.6	HTTPS en HSTS	11
4.1.7	WiFi	11
4.1.8	Webapplicaties	11
4.1.9	Website	11
4.1.10	CVD	11
4.1.11	Cookiewet	11
5	Citrix infrastructuur	12
5.1	Automation	12
5.2	Dataopslag	12
5.3	Werkplekken	12
5.4	Randapparatuur	12
6	Applicaties	13
6.1	Standaard kantoor applicaties	13
6.2	Content redirection	13
6.3	Microsoft Application Virtualization (AppV)	13
6.4	Security voorwaarden	14
7	Protocol remote access voor externen	15
8	MS Graph	16
8.1	Wenselijkheid binnen de Werksamen tenant	17

1 Inleiding

Dit document beschrijft de ICT-standaarden van de gemeente Emmen. Deze ICT-standaarden worden gebruikt als onderdeel van een programma van eisen bij de aanschaf van informatiesystemen en applicaties en ter toetsing bij updates/upgrades van bestaande informatiesystemen en applicaties.

TEAM-Automatisering is verantwoordelijk voor een goed werkende ICT infrastructuur van de gemeenten Borger-Odoorn, Coevorden, Emmen en overige klanten.

1.1 Aanleiding

Het opstellen van dit ICT-Infrastructuur document valt onder I&A van de gemeente Emmen. Dit document dient als onderdeel op het Programma van Eisen (PvE) en dient ook beschouwd te worden als eisen van het team Automatisering.

1.2 Afbakening

Dit document is van toepassing bij nieuwe toepassingen en kan ter ondersteuning worden gebruikt bij bestaande toepassingen. Informatie die tijdens de voorbereiding van dit document niet kan worden gedefinieerd, wordt aangeduid als "nader te bepalen" (NTB) of "te bevestigen" (TB), wat tijdens de totstandkoming wordt bepaald en vastgelegd.

2 Leeswijzer

In dit document worden de huidige ICT-standaarden beschreven, die door TEAM-Automatisering van de gemeente Emmen worden geaccepteerd en ondersteund.

Hoofdstuk 1	Inleiding – het hoe en waarom dit document is opgesteld.
Hoofdstuk 2	Leeswijzer – geeft aan waar men snel informatie kan vinden.
Hoofdstuk 3	Eisen – eisen die gelden voor een on-premise omgeving.
Hoofdstuk 4	Eisen en wensen overzicht – overzicht van eisen en wensen voor on-premise en SaaS omgevingen.
Hoofdstuk 5	Citrix Infrastructuur – geeft aan hoe in basis de Citrix omgeving is opgebouwd
Hoofdstuk 6	Applicaties – geeft aan op welke wijze de applicaties worden aangeboden.
Hoofdstuk 7	Protocol remote access externen – geeft aan welke regels er gelden voor remote toegang tot de systemen van de gemeente Emmen.
Hoofdstuk 8	MS Graph – geeft aan op welke wijze gemeente Emmen (BOCE) omgaat met MS Graph voor SaaS applicaties.

3 Eisen

In dit hoofdstuk worden de eisen beschreven die alleen van toepassing zijn op de on-premise omgeving. In het volgende hoofdstuk worden de eisen en wensen beschreven die voor oplossingen in een on-premise en/of SaaS-omgeving van toepassing zijn.

3.1 Techniek

In onderstaande tabel staan de technische eisen benoemd die gelden voor de ICT-infrastructuur zoals die door de gemeente Emmen beheerd wordt.

Tabel 1 Eisen t.o.v. Techniek

Component	Type	Versie
Operating Systeem	Windows Server	De software moet een van de laatste 3 versies zijn (N, N-1 en N-2)
	Citrix Provisioning	
	Citrix Virtual Apps and Desktops	
	Microsoft Application Virtualization	
	Ivanti Workspace Control	
Programmatuur	Microsoft Office 365	
	Microsoft Edge	
	Google Chrome enterprise	
	Corsa	
	Oracle client	
	Oracle Sql*net	
	Jsharp	
Plugins	MSXML	
	DirectX	
	.NET Frameworks	
	Crystal Report Viewer	
	Oracle Java	
	SmartLockr	
	e-Suite plugin Outlook & Word versie	
	Visual Studio prerequisites	
	Acrobat Reader DC	
Tools	CutePDF Writer	
	Crystal Smart Viewer for ActiveX	
	Microsoft Visual C++ 2017 Microsoft Visual C++ 2019 Microsoft Visual C++ 2022	
	Remote Admin Tools	
	XenDesktop MediaPack	
	PIA	
	Powershell	
	MS Defender	
	Time Zone	+1
	Landinstelling	NL
	Toetsenbord	US international
Instellingen	Datum- tijdnnotatie	24 uren klok
	Getalweergave	1.000,00
Verbindingen	Bekabeling	Glasvezel – Extern singlemode 9/125 µ; Intern multimode 62,5/125 µ. UTP cat. 6
	Datalink	Ethernet
	Protocol	TCP/IP
	Internet access	HTTP (poort 80), HTTPS

		(poort 443), FTP (poort 20-21)
Telefonie	Protocol	Voip. Standaard toestel Alcatel 4068
	Mobiel toestel	iPhone

3.2 Applicaties

In onderstaande tabellen (tabel 2 en tabel 3) staan de (technische) applicatie eisen benoemd die gelden voor de ICT-infrastructuur zoals die door de gemeente Emmen beheerd wordt.

Tabel 2 Infrastructuur eisen t.o.v. Applicaties

Component	Type	Versie
Operating Systeem	Windows Server (2022/2019/2016)	De software moet een van de laatste 3 versies zijn (N, N-1 en N-2)
	Oracle Enterprise Linux 64 bit 8.x of hoger	
Services	IIS	
	Oracle Weblogic	

Tabel 3 Applicatie eisen

Applicatie eis #	Omschrijving
appe01	De applicatie moet minimaal voldoen aan technische eisen §3.1
appe02	De applicatie werkt op basis van terminal server / Citrix en is multiuser.
appe03	De applicatie maakt geen gebruik van voorzieningen als dongles en hardware-verificatie.
appe04	Applicaties moeten Microsoft App-V compatible zijn.
appe05	Data dat lokaal op de systeemschijf/c-schijf van de server komt te staan wordt niet geback-up't en zal bij een schoonmaakactie van de server worden gewist. Vandaar dat (tijdelijke) data niet lokaal op de systeemschijf/c-schijf wordt opgeslagen.
appe06	Individuele aanpassingen ten behoeve van een applicatie mogen niet in de standaard KA omgeving doorgevoerd.
appe07	Rechten die de toepassing/applicatie nodig heeft mogen alleen op een applicatie-netwerkschijf gezet worden.
appe08	Lokaal op een Citrix server heeft een applicatie de volgende rechten: read en execute.
appe09	Gebruikers kunnen via de applicatie geen modificaties lokaal op een Citrix server uitvoeren (m.u.v. de profieldirectory).
appe10	Applicatie op een applicatieserver wordt uitsluitend geïnstalleerd onder een speciaal gebruikersaccount, die door TEAM-Automatisering wordt gedefinieerd.
appe11	De applicatie maakt alleen gebruik van Microsoft-gecertificeerde drivers.
appe12	TEAM-Automatisering installeert hotfixes e.d. z.s.m. maar uiterlijk binnen 1 maand na uitgifte. Indien dit tot problemen leidt t.a.v. de applicatie, dan moet de leverancier van de applicatie binnen een maand hiervoor een geschikte oplossing leveren. Er wordt hierin een proactieve houding verwacht van de leverancier.
appe13	Indien een applicatie een verbinding opzet met (web)servers buiten de ICT-infrastructuur van de gemeente Emmen, dan moet de leverancier aangegeven hoe er naar buiten gecommuniceerd moet worden. Hierbij moet de leverancier exact aangeven van en waar naar toe gecommuniceerd gaat worden (IP-nummers, protocollen en poorten). Op basis van deze gegevens kan worden beoordeeld of de verbinding naar buiten is toegestaan.
appe14	Remote support wordt onder strikte voorwaarden toegestaan. (Zie protocol remote access voor externen).
appe15	Licensering van applicaties moet zodanig zijn dat het niet in conflict is met de genoemde flexibele structuur.
appe16	T.b.v. software dat op een dedicated applicatie server wordt geïnstalleerd wordt er een speciaal gebruikersaccount beschikbaar gesteld. Dit account wordt op basis van gegevens van de leverancier geparametriseerd.

Appe17	Geen internet voor applicatieservers. Als een applicatie verbinding met internet nodig heeft, dan loopt dat via onze proxyserver. Dit is vanuit security-aspect common practice.
Appe18	Bij de installatie moet rekening gehouden worden met de partitie-indeling zoals deze door TEAM-Automatisering is opgesteld

3.3 Database

De eisen genoemd in de tabellen 4 en 5 zijn van toepassing op de databases die worden beheerd binnen de ICT-infrastructuur van de gemeente Emmen.

Tabel 4 Infrastructuur eisen t.o.v. databases

Component	Type	Versie
Oracle	Oracle Enterprise Linux 64 bit	9.x/8.x
	Oracle 64-bit Standard Edition	23c.x/21c.x
	Oracle SQL*Net Listener	20002
	NLS_LANG	DUTCH_THE NETHERLANDS.AL32UTF8
	SGA	1 GB
	AUDIT_TRAIL	DB
	ARCHIVING	ON
	FLASHBACK	ON
SQL	Windows Server	Windows 2019/2022
	MS-SQL	2022/2019

Tabel 5 Database eisen

Database eis #	Omschrijving
dbe01	Database-servers worden alleen gebruikt als database server. Applicatie processen moeten op de zogenaamde applicatieserver(s) worden geïnstalleerd.
dbe02	De connectie met de Oracle databases wordt verzorgd met behulp van sql*net.
dbe03	Het datamodel van de database van de applicatie moet ter beschikking worden gesteld aan de gemeente Emmen. Het model moet zodanig zijn dat de integriteit van de data door middel van functies in de database gegarandeerd wordt.
dbe04	De database van de applicatie moet toegankelijk zijn voor gemeente brede voorzieningen, voor zowel adaptoren als contra adaptoren.
dbe05	Alleen bovenstaande type databases worden ondersteund. Andere typen databases in combinatie met andere besturingssystemen worden door de afdeling TEAM-Automatisering niet ondersteund.

3.4 Algemeen

Tabel 6 Algemene eisen

Algemene eis #	Omschrijving
alge01	Infrastructurele voorzieningen worden door de afdeling TEAM-Automatisering beoordeeld en gerealiseerd.
alge02	Infrastructurele componenten worden uitsluitend door TEAM-Automatisering aangeschaft.
algo3	Overall waar toegang tot nodig is dient ondersteuning te bieden voor SSO (Microsoft AD) en MFA (Microsoft Authenticator).
algo4	Om vendor lock-in te voorkomen zal er altijd van tevoren een exit plan uitgewerkt moeten zijn. Hier zal de leverancier volledige medewerking aan verlenen.

4 Eisen en wensen overzicht

Onderstaand overzicht bevat eisen en wensen die voor oplossingen in een on-premise en/of SaaS-omgeving van toepassing zijn.

Categorie	#	Omschrijving	Eis/Wens	Local	SaaS
Technologie	To1	Oplossing werkt conflictloos binnen browsers: Edge (primair) en Chrome.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	To2	User interface is responsive	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	To3	Oplossing heeft weinig bandbreedte nodig	Wens	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	To4	Oplossing betreft proven technology vanuit ons perspectief	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interoperabiliteit	Io1	Integraties verlopen via een door ons ondersteund Integratie platform, conform standaarden voor veilige uitwisseling	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Io2	Door ons ondersteunde Integraties & koppelingen tussen SaaS oplossingen zijn volledig gedocumenteerd. Eigenaarschap is belegd	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Toegang en autorisatie	TA01	Toegang applicaties buiten netwerk op basis van de door ons ondersteunde Multi Factor Authentication (MFA)	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA02	Het platform ondersteunt de door de Team Automatisering ondersteunde single sign-on (SSO).	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA03	Wachtwoorden worden gehasht opgeslagen, minimaal met SHA-256.	Eis	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	TA04	Wachtwoorden worden niet op het scherm weergegeven	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA05	Wachtwoordbeleid is configureerbaar	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA06	Elke gebruiker heeft een persoonsgebonden inlogaccount met een unieke gebruikersnaam (één digitale identiteit)	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA07	Het systeem heeft autorisatieniveaus op basis van rol gebaseerd	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TA08	Toegang voor niet-medewerkers (bijv. uitzendkrachten) met een juist profiel is (mits doelmatig) te realiseren	Wens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data	Do1	De organisaties waaraan we dienstverlening leveren zijn eigenaar van hun eigen data.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do2	Gegevens zijn direct indien noodzakelijk toegankelijk buiten applicatie om voor Team Automatisering t.b.v. rapportages/integraties/back-up	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do3	Eenmalige opslag van gegevens binnen de oplossing	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do4	Data-uitwisseling conform standaarden die door Team Automatisering geaccepteerd zijn	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do5	Integriteit: Gegevens zijn juist, actueel, betrouwbaar (in 1x goed) en herleidbaar	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do6	Mogelijkheid tot vergrendeling dataverkeer configureerbaar	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do7	Dataopslag binnen EER bij voorkeur binnen Nederlands grenzen	Eis	<input type="checkbox"/>	<input checked="" type="checkbox"/>

	Do8	API's moeten goed beschreven zijn	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Do9	API's moeten alle data kunnen uitlezen, inlezen en muteren.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	D10	Er moet voldaan worden aan algoritmen volgens ministerie van Binnenlandse zaken*	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Beschikbaarheid	Bo1	7x24, minimaal 99,7%, (max downtime) moet ondersteund worden	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Bo2	Wijzigingen voor bedrijfskritische applicaties doorlopen altijd het TAP proces	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security & Compliance	SCo1	Oplossing voldoet aan Nederlandse wet- en regelgeving.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SCo2	Privacy enhancing technologies zijn ingezet: sterke hedendaagse encryptie, het liefst geen third party producten in broncode maar indien niet mogelijk dan third party producten vermelden.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SCo3	Hardening: niet gebruikte functies staan uit, poorten die niet worden gebruikt zijn uitgeschakeld.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Auditing	Ao1	De leverancier is minimaal ISO2700x gecertificeerd	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ao2	Leverancier sluit verwerkersovereenkomst af	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ao3	Leverancier garandeert dat alle informatie binnen de EER wordt opgeslagen	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ao4	Leverancier werkt, indien gevraagd, mee aan een PIA (Privacy Impact Assessment)	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ao5	Auditering vindt geregeld, structureel en periodiek plaats om de omgeving te toetsen aan wet en regelgeving aangaande beveiliging en beschikbaarheid.	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Monitoring & Logging	MLo1	Non-repudiation (docs/handelingen) alle handelingen binnen systemen zijn onweerlegbaar	Wens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	MLo2	Aanvallen, afwijkingen van de normalsituatie detecteren en veilig versturen naar een centrale monitoring omgeving	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	MLo3	Automatisch loggen bij afwijkingen en hierover ook rapporteren naar centrale monitoring omgeving. Voorkeur heeft API van waaruit men centraal kan monitoren	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	MLo4	Metingen over gebruik van onderdelen vanuit de applicatie. Voorkeur heeft API van waaruit men centraal kan monitoren	Eis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

* Voor meer informatie over publicatiestandaard [algoritmes](#), check hier de meeste recente [handleiding algoritmeregister](#).

4.1 Internet en Beveiliging

We willen de veiligheid, bescherming persoonsgegevens, toegankelijkheid, (bouw)kwaliteit en transparantie waarborgen en ons houden aan de onderstaande eisen en richtlijnen voor gemeenten en door rijksoverheid vastgesteld.

4.1.1 Bescherming tegen e-mailphishing

[Sender Policy Framework \(SPF\)](#)

[DomainKeys Identified Mail \(DKIM\)](#)

[Domain-based Message Authentication, Reporting & Conformance \(DMARC\)](#)

4.1.2 Mailservers

[Beveiligde verbinding tussen mailservers \(STARTTLS en DANE\)](#)

4.1.3 DNSSEC

[Domeinnaambeveiliging \(DNSSEC\)](#)

4.1.4 IPv6 en IPv4

[Adressering van ICT-systemen binnen een netwerk \(IPv6 en IPv4\):](#)

4.1.5 TLS

[Beveiligde internetverbinding \(TLS\)](#)

4.1.6 HTTPS en HSTS

[Beveiligde websiteverbinding \(HTTPS&HSTS\)](#)

4.1.7 WiFi

[Beveiligde WiFi-netwerken \(WPA2 Enterprise\)](#)

4.1.8 Webapplicaties

[ICT-Beveiligingsrichtlijnen voor Webapplicaties](#)

4.1.9 Website

[Toegankelijkheid websites \(EN301549 en WCAG2.1\)](#)

4.1.10 CVD

[Coordinated Vulnerability Disclosure \(CVD\)](#)

4.1.11 Cookiewet

[Telecommunicatiewet \(Cookiewet\)](#)

5 Citrix infrastructuur

Gemeente Emmen en haar partnerorganisaties en klanten maken o.a. gebruik van flexplekken. Daarnaast wordt ook vanuit huis gewerkt. Om dit te realiseren worden alle applicaties aangeboden door middel van het terminal-server/Citrix-concept. Dit betekent dat alle applicaties op basis van terminal-server/Citrix moeten werken en daardoor multiuser moeten zijn. Huidige omgeving valt onder de noemer **Virtuele Werkplek**.

Om een optimale beschikbaarheid, continuïteit en betrouwbaarheid van de Citrix-infrastructuur te garanderen dienen de servers in de Citrix-farm gelijk te zijn geïnstalleerd/geconfigureerd. Om hieraan te voldoen is dit proces bij de gemeente Emmen volledig geautomatiseerd.

5.1 Automation

Door de hele Citrix omgeving/applicaties door middel van Automation uit te rollen en applicaties te virtualiseren is het back-uppen van Citrix-servers overbodig. In geval van problemen wordt de betreffende server opnieuw uitgerold en in productie genomen. Doordat de omgeving geautomatiseerd uitgerold wordt, kunnen mutaties en/of aanpassingen niet handmatig uitgevoerd worden zonder dat ze opgeslagen worden.

Het Operating System (OS) en de standaard Kantoor Automatisering (KA) worden geautomatiseerd uitgerold. Middels een zgn. 'golden image' wordt het operating system (Nu Windows 2019) met Microsoft MCS ingericht.

Additionele applicaties en configuratie worden met afterjobs door Ivanti Automation Manager geïnstalleerd. Dit gebeurt elke nacht, na de dagelijkse herstart.

Diverse applicaties worden door middel van application virtualisation (Microsoft App-V) aangeboden.

5.2 Dataopslag

De servers zijn voorzien van één of meerdere netwerk(san-)schijven. Hierop installeert TEAM-Automatisering zoveel mogelijk de applicaties. De data die een applicatie genereert wordt opgeslagen in een database. Andere data, zoals gegenereerde documenten e.d. moeten op de applicatiedata netwerk-(san)schijf worden opgeslagen. De netwerk-(san)schijven worden geback-uppt. Data dat lokaal op de systeemschijf/c:-schijf van de server komt te staan wordt in principe niet geback-uppt en zal bij een schoonmaakactie van de server worden gewist.

5.3 Werkplekken

Alle gebruikers die gebruik maken van de infrastructuur hebben de beschikking over een standaard werkplek die bestaat uit een thin client of een replicator met 2 monitoren, toetsenbord en muis. De ondersteunde beeldschermresolutie is 1920x1080. De thin client bevat geen applicatiesoftware, maar wel besturingssoftware en geldt alleen als ontvangst- en zendstation van en naar de server toe.

5.4 Randapparatuur

Alle randapparatuur moet Microsoft gecertificeerd zijn en passen binnen de multiuser Citrix-omgeving.

6 Applicaties

TEAM-Automatisering onderscheidt een aantal classificaties met betrekking tot de indeling van de applicaties.

- Standaard KA applicaties
- Content Redirection Silo applicaties
- Virtuele applicaties

6.1 Standaard kantoor applicaties

De standaard Kantoor Automatisering (KA) is de basis van de Citrix-server. De standaard KA bestaat uit een Windows-installatie en de Office Suite met een aantal standaard tools. In de standaard KA omgeving staan de basis applicaties die alle medewerkers tot hun beschikking krijgen.

De uitrol van de standaard KA omgeving is een image, dat compleet met operating system, office suite en tools wordt uitgerold. Individuele aanpassingen ten behoeve van een applicatie worden niet in de standaard KA omgeving doorgevoerd. De servers die voor de standaard KA omgeving gebruikt worden noemen we desktop servers. De sessies van de gebruikers worden via de standaard KA omgeving verdeeld over de desktop servers en daarop worden de verschillende KA applicaties opgestart.

In technische eisen staan de versies van de onderdelen waarmee rekening gehouden moet worden. Hierbij moet worden opgemerkt dat met name bij internet toepassingen/applicaties de versie van Microsoft Edge en de benodigde plugins e.d. goed wordt gecontroleerd.

Indien blijkt dat voor het werkend krijgen van een applicatie extra instellingen en/of aanpassingen gerealiseerd moeten worden in Microsoft Edge, dan zal dit door TEAM-Automatisering op haalbaarheid worden onderzocht.

6.2 Content redirection

In de content redirections silo staan applicaties, die als basis gebruik maken van de componenten uit de standaard KA omgeving. Bijvoorbeeld een met behulp van Microsoft Access gebouwde toepassing/applicatie, dat op basis van de functionele gegevens van Microsoft Access wordt opgestart. Deze toepassingen/applicaties worden op de standaard KA servers opgestart en moeten minimaal voldoen aan de specificaties die in §3.1 staan. Bij het opstarten van de toepassing/applicatie kunnen extra additionele zaken geregeld moeten worden om het werkend te maken. Zoals instellingen in de user register, kopiëren van bestanden e.d.

6.3 Microsoft Application Virtualization (AppV)

Toepassingen/applicaties worden aangeboden m.b.v. Microsoft Application Virtualization (App-V). Microsoft App-V brengt een virtualisatie laag aan tussen het OS en de applicatie. Hierdoor is het mogelijk om applicaties van elkaar te isoleren en is het niet langer nodig de applicaties fysiek lokaal te installeren. Het voordeel hiervan is dat de applicatie direct - in een geïsoleerde omgeving - op de desktop server opstart. Indien de applicatie koppelingen heeft met andere applicaties dan moeten die in een gezamenlijke, geïsoleerde, Microsoft App-V omgeving gezet worden. Van belang is dus dat de onderlinge koppelingen (xml, stuf, enz.) van te voren bekend zijn. De te installeren applicaties dienen Microsoft App-V compatible te zijn.

TEAM-Automatisering maakt bij het virtualiseren van de applicaties het volgende onderscheid:

- applicaties die volledig op een applicatie-netwerkschijf staan
- applicaties die deels op een applicatie-netwerkschijf staan

- applicaties die volledig lokaal staan

Het streven is om de applicaties zoveel mogelijk op een applicatie-netwerkschijf te zetten. Dit heeft als voordeel dat updates en aanpassingen kunnen worden uitgevoerd zonder een nieuwe virtuele applicatie gebouwd moet worden. Dat kan per geval verschillend zijn en moet per toepassing/applicatie worden beoordeeld.

Mutaties aan applicaties (aanpassingen van instellingen en/of dll enz.) die lokaal staan kunnen niet zomaar worden doorgevoerd. De methode hiervoor is dat er een nieuwe virtuele applicatie van gemaakt moet worden of de bestaande virtuele applicatie wordt aangepast. Daarna vindt de uitrol plaats.

Rechten die de applicatie nodig heeft worden alleen op een applicatie-netwerkschijf gezet. Lokaal op een Citrix-server heeft een applicatie de volgende rechten: read en execute. Gebruikers kunnen via de applicatie geen modificaties lokaal op een Citrix-server uitvoeren (met uitzondering van de profieldirectory).

6.4 Security voorwaarden

TEAM-Automatisering maakt gebruik van de marktconforme security-standaarden. Alle systemen zijn uitgerust met virus-scanners. Hotfixes en patches worden zo snel mogelijk naar uitlevering geïnstalleerd. De verbindingen van buiten naar binnen (en andersom) worden, basis van vaste regels, geregisseerd door een firewall.

Leveranciers kunnen op afstand toegang krijgen tot de ICT-Infrastructuur. Daartoe wordt door de applicatiebeheerder een sessie geïnitieerd. De sessie vindt plaats onder toezicht en met de rechten en mogelijkheden van de initiator. De toegang op afstand is uitsluitend bedoeld om incidenten te verhelpen of een probleemanalyse uit te voeren. Het uitvoeren van installatiewerkzaamheden kan alleen na goedkeuring van de RFC / Change.

7 Protocol remote access voor externen

Remote Access voor externen heeft tot doel om externe partijen een beveiligde en gecontroleerde toegang te verstrekken tot het gemeentelijke netwerk en de gemeentelijke informatiebronnen.

Remote Access voorziet in de behoefte om externe partijen te laten werken op de ICT voorzieningen van de klanten waar Team Automatisering in voorziet. De externe partij neemt daarvoor de sessie over van de medewerker die het Remote Access heeft geïnitieerd. De externe partij beschikt daardoor over de benodigde rechten en mogelijkheden van de initiator (meestal applicatiebeheer of functioneel beheer). De initiator heeft te allen tijde de mogelijkheid de activiteit van de externe partij te onderbreken en desgewenst de sessie te beëindigen.

Remote Access is uitsluitend bedoeld om incidenten te verhelpen of een probleemanalyse uit te voeren. Het uitvoeren van installatiewerkzaamheden met behulp van Remote Access is ter beoordeling van changemanagement.

Beveiliging:

- Remote Access wordt altijd geïnitieerd door een medewerker van Team Automatisering;
- Remote Access is op verzoek van de teamleider toegekend aan medewerkers die functioneel beheerder, applicatiebeheerder of technisch beheerder zijn.
- Remote Access vindt plaats onder verantwoordelijkheid van de initiator. In het algemeen is dit de applicatie- of functioneel beheerder;
- Remote Access vindt plaats onder toezicht van de initiator. In het algemeen is dit de applicatie- of functioneel beheerder;
- Indien Remote Access wordt gebruikt voor het GBA (Key2burgerzaken) of voor gegevensverzamelingen waar het GBA gebruikt van maakt dan is de procedure 6.1.11 'Remote Access' van het Handboek Beveiliging Burgerzaken van toepassing.
- De eigenaren van de gemeentelijke informatiesystemen zijn verplicht een geheimhoudingscontract aan te gaan met de externe leverancier alvorens remote acces wordt toegekend.

8 MS Graph

Het probleem met Microsoft Graph API laat zich in één statement beschrijven;

MS Graph API is uit zichzelf niet volledig compliant met de uitgangspunten “Least privilege” en “data minimalisatie”. (Of andersom: is deels compliant).

Aanvullend statement is, dat de logging van acties die via de MS Graph API worden uitgevoerd niet vrij eenvoudig inzichtelijk zijn en dus moeilijker controleerbaar/auditeerbaar zijn.

Kort uitgelegd:

Microsoft Graph API is een set van functies waarmee allerlei verschillende acties uitgevoerd kunnen worden op de tenant. Bijvoorbeeld het uitlezen van de eigenschappen van een gebruiker in Entra ID. Of het uitlezen van de agenda van een gebruiker in Exchange. En zo zijn er nog vele andere acties en functies die met de Graph API uitgevoerd kunnen worden op de tenant.

De Microsoft Graph API functies maken gebruik van permissions (rechten) om toegang te krijgen tot de verschillende onderdelen. Er zijn 2 typen permissions te onderscheiden:

Delegated permissions: dit zijn rechten die “uit naam” van de ingelogde gebruiker gegevens kan inzien, bewerken of zaken kan uitvoeren, afhankelijk van de ingestelde permissions.

Application permissions: dit zijn rechten die zijn verleend aan een SAAS-applicatie en kan zonder tussenkomst van een gebruiker gegevens inzien bewerken of zaken uitvoeren, afhankelijk van de ingestelde permissions.

Wanneer gebruik wordt gemaakt van application permissions is het risico reëel dat de SAAS applicatie toegang krijgt tot resources waar het geen toegang tot moet krijgen. Dit omdat application permissions rechtstreeks tussen SAAS-applicatie en Tenant kunnen communiceren zonder rekening te houden met de geldende rechtenstructuur. Dus de “Least privilege” en “data minimalisatie” principes zijn niet van toepassing op application permissions.

Het inperken van application permissions kan in beperkte mate. Voor application permissions die bewerkingen willen uitvoeren die te maken hebben met Exchange, dus bijvoorbeeld het uitlezen van kalenders of het verzenden van mail. Deze bewerkingen binnen Exchange kunnen wel worden beveiligd middels een policy waardoor alleen dergelijke bewerkingen kunnen worden gedaan voor een bepaalde groep gebruikers. Deze methodiek is ook door Microsoft beschreven en wordt ook ingezet.

Voor application permissions die bewerkingen doen op Entra ID, Teams, SharePoint en dergelijke is op dit moment geen goede oplossing bekend om dit te kunnen inperken voor een bepaalde groep gebruikers.

Delegated permissions hebben de voorkeur wanneer bewerkingen op onze tenant nodig zijn door een SAAS-applicatie. Omdat deze permissions worden uitgevoerd onder het account van de gebruiker, blijft de rechtenstructuur in stand. De ingesteld delegated permission heeft alleen toegang tot gegevens en bronnen waar de gebruiker ook toegang tot heeft. Dit betekent dat de “Least privilege” en “data minimalisatie” principes wel van toepassing zijn op delegated permissions

Binnen een App registration of Enterprise app waar delegated of application permissions worden ingesteld maken we de app alleen beschikbaar voor de groep gebruikers waarvoor deze applicatie beschikbaar gemaakt moet worden. Waarmee we gebruikers alleen toegang geven tot applicaties waar zij ook gebruik van mogen maken. Echter wanneer application permissions worden ingesteld gaat dit principe niet op omdat de ingestelde permissions rechtstreeks toegang hebben tot alle resources. Bij delegated permissions blijft dit principe wel in stand.

Gebruiker van SAAS applicaties kunnen zelf geen consent (goedkeuring) geven op het instellen van permissions. Binnen onze tenant is dit altijd iets wat door de global admin wordt gedaan. Voor zowel delegated als application permissions. De global admin doet een check op de permissions die ingesteld moeten worden en kan beoordelen of deze wel of niet gewenst zijn. Indien er permissions zijn die niet gewenst zijn zoals application permissions zullen er passende maatregelen moeten worden genomen zoals:

- De Enterprise app en/of App registration zal niet worden geactiveerd en er wordt geen consent afgegeven op de permissions;
- De niet gewenste permissions worden ingetrokken, hierdoor kan functionaliteit in de SAAS applicatie niet meer werken;

Er wordt overlegd met de leverancier van de software welke oplossingen eventueel wel mogelijk zijn om de principes “Least privilege” en “data minimalisatie” na te kunnen leven.

8.1 Wenselijkheid binnen de Werksamen tenant

Een overzicht van verschillende Microsoft Graph permissions, waarbij we aangeven welke permissions ongewenst zijn en we niet toelaten op onze tenant, tot permissions die wij “veilig” genoeg achten en het meest compliant zijn aan de principes van least privileged access en data minimalisatie.

MS Graph permissions matrix van ongewenst naar gewenst				
Ongewenst	>	>	>	Gewenst
5	4	3	2	1

Bovenstaand afgebeelde matrix geeft weer welke niveaus van MS graph permissions welke wij hebben vastgesteld van ongewenst (5) naar gewenst (1). Hieronder volgt per categorie uitleg over de permissions en waarom deze in een desbetreffende categorie vallen.

5

Application permissions welke aangemerkt zijn als “gevaarlijk” (*zie ook bronnen onderaan dit document) omdat sommige van deze rechten het mogelijk maken om gebruikers additionele verhoogde rechten aan zich zelf toe te wijzen of geven toegang op het hoogste niveau tot verschillende resources binnen de tenant. Deze rechten (zie onderstaande tabel) zullen **geen** admin consent krijgen op onze tenant. Deze rechten zijn niet compliant en voldoen niet aan de principes van least privileged access en data-minimalisatie.

MS Graph permission	Reden geen Autorisatie
Directory.Read.All	Geeft toegang tot gegevens in alle mappen, ongeacht de gegevensclassificatie. Dit geeft in het bijzonder toegang tot Office 365-groepen met verborgen lidmaatschap.
Groups.Read.All	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap.
GroupMember.Read.All	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap
Groups.ReadWrite.All	Geeft schrijftoegang aan alle groepen.
User.ReadWrite.All	Geeft schrijftoegang voor alle gebruikers
Member.Read.Hidden	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap.
Files.Read.All	Hiermee wordt leesttoegang verleend tot alle SharePoint Online en OneDrive for Business bestanden.
Update_device_attributes	Intune bij de gemeente Emmen is ingeperkt en deze permissie geeft de mogelijkheid om elk apparaat dat Intune beheert bij te werken.
Update_device_health	Intune bij de gemeente Emmen is ingeperkt en deze permissie geeft de mogelijkheid om elk apparaat dat Intune beheert bij te werken.
ActivityFeed.Read	Geeft brede toegang tot alle Teams-kanalen.
AppRoleAssignment.ReadWrite.All	Met deze applicatierol kan de gebruiker of applicatie extra privileges toekennen aan zichzelf en aan andere applicaties.
RoleManagement.ReadWrite.Directory	Deze applicatierol bevat ook het recht om admin rechten toe te kennen. Hiermee wordt het mogelijk gemaakt om andere applicatierollen met verhoogde rechten toe te wijzen.

4

Rechten die gegevens m.b.t. de identiteit van gebruikers beschikbaar maken voor een derden app. Er zijn 6 admin rechten die afhankelijk van de permissie alle gegevens inzichtelijk maken en niet zijn af te schermen. Daarnaast zijn er 3 rechten vanuit een gebruikersperspectief (Delegated) die mogelijk ook teveel gegevens beschikbaar kunnen maken (echter beperkt zich dit alleen tot waar de gebruiker ook daadwerkelijk toegang tot heeft)

Als onderstaande application permissions benodigd zijn omwille van functionaliteit, dan moet dit worden gedocumenteerd in het ABD (Applicatie Beheer Document). Daarnaast moet er toestemming zijn vanuit de andere gebruikers (klanten en gemeenten) van de tenant, dat hun gegevens inzichtelijk/toegankelijk zijn door derden. Ook moet altijd worden onderzocht of de gevraagde permissies wel daadwerkelijk noodzakelijk zijn en dat minder uitgebreide permissies wellicht ook volstaan.

MS Graph permission	Toelichting
Member.Read.Hidden MSGraph: User.Read.All MSGraph: Group.Read.All MSGraph: Group.Write.All MSGraph: Directory.ReadWrite.All MSGraph: Directory.Read.All	Application permissions waarmee identiteitsinformatie over onze Entra ID tenant kan worden opgevraagd.
MSGraph: User.Read MSGraph: User.ReadBasic.All MSGraph: Directory.AccessAsUser.All	Gebruikersrechten waarmee identiteitsinformatie over onze Entra ID tenant kan worden opgevraagd.*

*Hoewel deze rechten wellicht meer informatie kan blootgeven dan noodzakelijk, worden deze gedaan vanuit een gebruikersperspectief en geeft alleen gegevens over de ingelogde gebruiker waaronder deze permissions worden uitgevoerd.

3

Rechten waar we een admin consent voor aangeven maar alleen onder specifieke omstandigheden. Deze rechten zijn middels een policy in te perken of via aanvullende rechten.

API & Permission Scope	Toelichting
MSGraph: Mail.Read MSGraph: Mail.ReadBasic MSGraph: Mail.ReadBasic.All MSGraph: Mail.ReadWrite.All MSGraph: Mail.Send MSGraph: MailboxSettings.Read MSGraph:	Ongepaste lees- en/of schrijftoegang rechten, waarmee toegang wordt verleend tot de mailboxen van alle gebruikers. Gebruik de volgende instructies om deze rechten voor specifieke groepen/gebruikers te beveiligen: Limiting application

MailboxSettings.ReadWrite MSGraph: Calendars.Read MSGraph: Calendars.ReadWrite MSGraph: Contacts.Read MSGraph: Contacts.ReadWrite Office 365 Exchange Online: full_access_as_app	permissions to specific Exchange Online mailboxes - Microsoft Graph Microsoft Learn
MSGraph: Sites.FullControl.All MSGraph: Sites.Manage.All MSGraph: Sites.Read.All MSGraph: Sites.ReadWrite.All	Ongepaste lees- en/of schrijftoegang rechten waarmee toegang wordt verleend aan alle Sharepoint Online sites. Gebruik: Controlling app access on a specific SharePoint site collections is now available in Microsoft Graph - Microsoft 365 Developer Blog

2

Wanneer gebruikerssynchronisatie tussen de tenant en derde partij wenselijk is, geven wij de voorkeur voor het inrichten van een runbook (het maken van een geautomatiseerde oplossing) in Azure. Daarbij stellen we als eis dat de gebruikerssynchronisatie wordt gedaan op een Entra ID groep of gesyncte AD-groep waarin de gebruikers lid van zijn die ten behoeve van de app gesynct moeten worden. Daarnaast moet de beveiliging voldoen aan de meest recente (beveiligings-)standaarden van Microsoft.

1

De voorkeur qua rechten gaat uit naar Delegated permissions. Deze rechten worden uitgevoerd uit naam van de gebruiker en de voor hem of haar geldende rechtenstructuur. En voldoet het meest aan de principes van least privileged access en data-minimalisatie.