

M365

Scenario's, praktische antwoorden en tips



VNG Realisatie in samenwerking met de werkgroep M365 bestaande uit minimaal 10 organisaties die samen dit document gevuld hebben vanuit hun huidige ervaring.

Nassaulaan 12

2514 JS Den Haag

Juni 2023

Inhoudsopgave

1. Aanleiding	5
1.1. Wat is Microsoft Teams?	5
1.2. Wat is SharePoint?	5
1.3. Status document	5
2. Toelichting op de inhoud van de hoofdstukken	7
3. Inleiding	8
4. Scenario's voor Teams	9
4.1. Korte beschrijving scenario's	9
4.2. Scenario 1: Samenwerken in Teams	10
4.3. Scenario 2: Archiveren in Teams	14
4.4. Scenario 3: Zaakgericht werken in Teams	18
4.5. Conclusie	19
5. Beheren van informatie in een team	21
5.1. Uitgangspunten	21
5.2. Processen voor Informatiebeheer	21
5.3. Inrichtingsfase	21
5.4. Gebruiksfase	23
5.5. Bewaarfase	24
5.6. Governance, Organisatie en rollen	25
5.7. Kwaliteitszorg	26
6. Inrichten van een team	27
6.1. Regelen van randvoorwaarden	27
6.2. Aandachtspunten en tips bij het aanmaken van een team	27
7. Bewaarbeleid	33
7.1. Metadata-schema	33
7.2. Welke metadata is noodzakelijk om uw bewaarbeleid uit te voeren?	33
7.3. Waarderen	34
7.4. Bepalen bewaartermijn en vernietigingsdatum Retentie (herwaarderen)	38
7.5. Classificeren	39
8. Kwaliteit inrichting	40
8.1. Kwaliteitscontrole via Records Management (Disposition)	40
8.2. Kwaliteitscontrole via eDiscovery tooling	40
8.3. Kwaliteitscontrole via Purview logs	41
9. Toegankelijkheid	42
9.1. Vinden van informatie: Zoekfunctie	42
9.2. Openstellen van informatie	42
9.3. Beveiligen van informatie	44
9.4. Toegankelijkheid op termijn	47
10. De functionaliteit van M365	48
10.1. Mogelijkheden voor workflows	48
10.2. Functionaliteit voor vernietigen: hoe doen we dat?	48
10.3. Functionaliteit voor overbrengen	48
11. Gebruikers (Adoptie en gebruik)	49
11.1. Kleine, middelgrote of grote gemeentelijke organisatie, maakt dat uit?	49
11.2. Inrichten van rechten binnen de MS365 - E5 omgeving	49
11.3. Gebruikers binnen de M365 – E5 omgeving	49
Bijlage 1. Voorbeeld van een gemeente Hilversum (CONCEPT)	52

Bijlage 2.	RASCI tabel Werken met TEAMS	56
Bijlage 3.	Uitgebreide inhoudsopgave	58
Bijlage 4.	Gemeente Noordwijk – Beleid en inrichting TEAMS.....	61
Bijlage 5.	Gemeente Noordwijk – Directievoorstel instemmen beleid en inrichting TEAMS	62
Bijlage 6.	Gemeente Noordwijk – Onderbouwing E5 licentie	63
Bijlage 7.	Gemeente Noordwijk – Uitvoeringsdocument inrichting Teams.....	64
Bijlage 8.	Gemeente Zwolle – Autorisatiematrix.....	65

1. Aanleiding

Microsoft, en dan met name Teams, was in 2019 vooral een product waar projecten in samenwerkten. Maar met de vlucht van thuiswerken vanaf 2020 is het product bij veel organisaties bijna een vervanging voor het gehele werkproces en de weergave daarvan geworden. Kennis van producten was er door de vliegende start te weinig waardoor organisaties zich nu afvragen of ze geen nieuwe C schijf hebben ontketend. De werkgroep M365 is in augustus 2022 gestart met alle vragen, die er lagen vanuit het werkveld documentaire informatievoorziening, te beantwoorden. Tijdens het beantwoorden van de vragen kwam al snel naar voren dat het cruciaal is om als organisatie te besluiten hoe zij M365 wil gebruiken. Is het een samenwerkingsplatform, doet het ook iets aan archivering of was het idee een vervanging voor het zaaksysteem te creëren? Veel organisaties bezinnen zich nu op een herinrichting, een mooi moment om die keuze bewust te maken en vervolgens te kiezen in de stappen die volgen.

Voor u ligt een document, tot stand gekomen met gemeenten die ook zoekend zijn naar een goede inrichting. Het document is inhoudelijk gecontroleerd. Mocht u toch onvolkomenheden aantreffen dan vragen we u die door te geven via gripopinformatie@vng.nl

1.1. Wat is Microsoft Teams?

Met Microsoft Teams kunt u chatten en vergaderen en u kunt een team aanmaken om gestructureerd samen te werken met personen aan een bepaald doel. Binnen deze chats, vergaderingen of Teams kunt u tegelijkertijd samenwerken aan bestanden en kunt u gesprekken voeren via chatberichten, audio- of videogesprekken.

1.2. Wat is SharePoint?

SharePoint is een platform waar u websites kunt bouwen binnen uw organisatie. Het bestaat al wat langer dan Microsoft Teams, dus misschien heeft u het al eens gezien of ervan gehoord. Met SharePoint kunt u Teamsites maken waarin u bijvoorbeeld alle mappen en bestanden van een bepaald team kunt opslaan. Deze SharePoint Teamsites vervangen vaak een lokale server of een server in de cloud, zoals een gedeelde F-schijf. U kunt ook een communicatiesite maken waarop nieuwsupdates, gebeurtenissen of evenementen gedeeld worden met iedereen binnen de organisatie. U kunt zo'n communicatiesite vergelijken met een intranet.

Zoals u merkt zit er redelijk wat overlap in de twee Microsoft-applicaties. Beiden bieden ze de mogelijkheid om samen te werken met anderen aan bestanden. In dit document richten we ons op Teams.

1.3 Status document

Dit document is geschreven door organisaties die al bezig zijn met het inrichten van een Teams omgeving. In 2022 heeft er een webinar plaatsgevonden waarbij organisaties die nog niet begonnen waren informatie wilden over een grote hoeveelheid onderwerpen. Hierop is in juli 2022 de werkgroep gestart. Echter hierbij willen we meegeven dat Microsoft als product in ontwikkeling blijft. Dit document zet aan tot keuzes en maakt dat u de diverse onderwerpen bij het inrichten van Microsoft niet vergeet. Maar het document is geschreven dóór organisaties vóór organisaties, het document is geen Microsoft handleiding. We hebben het document op verschillende manieren bij Microsoft aangeboden met het verzoek het te toetsen op de mogelijkheden die wij niet beschreven hebben. Microsoft heeft tot op heden, juni 2023, geen reactie gegeven. Ze hebben wel aangegeven dat de insteek zeer specifiek is en dat Microsoft er nooit zo naar kijkt. Wel hebben ze aangegeven er

mee aan de slag te willen gaan maar hebben geen termijn genoemd. Zodra zij met een reactie komen zullen we het document aanpassen. Tot die tijd: mocht u fouten ontdekken, betere manieren kennen om iets op te lossen of willen bijdragen aan bepaalde punten dan is ons verzoek: meldt het via gripopinformatie@vng.nl.

2. Toelichting op de inhoud van de hoofdstukken

1. Aanleiding

2. Toelichting op de inhoud van de hoofdstukken

3. Inleiding

4. Scenario's voor Teams

Er zijn verschillende manieren waarop u Teams kunt positioneren als het gaat over het beheren van informatie. Elke manier stelt andere eisen aan de inrichting van techniek en de organisatie. We lichten drie verschillende scenario's toe.

5. Beheren van informatie in een team

De processen voor informatiebeheer volgen de levenscyclus van een informatieobject. In Microsoft Teams zijn dit zowel een Team, een Kanaal als de documenten en registraties daarbinnen. We beschrijven welke processen moeten worden georganiseerd, welke activiteiten moeten worden uitgevoerd om grip te houden op de verwerkte informatie in M365 en wie waarvoor verantwoordelijk is.

6. Inrichten van een team

Bij het samenwerken in een team wordt informatie verwerkt. Het proces is vaak minder gestructureerd en de informatie is vooraf lastiger te definiëren. Het is wel mogelijk om bij het inrichten van het team al rekening te houden met een aantal randvoorwaarden voor meer grip op informatie. Dit helpt om gebruikers al tijdens het samenwerken de informatie te laten structureren. Ook geeft het mogelijkheden om het beheer beter uit te voeren.

Dit hoofdstuk beschrijft de aandachtspunten bij het inrichten van een team en geeft tips voor hoe u dit op een goede manier kan realiseren.

7. Bewaarbeleid

Grip op informatie begint met het formuleren van bewaarbeleid. Zo bepaalt u hoe informatie wordt bewaard. Dat geldt ook voor de informatie die binnen M365 wordt verwerkt. We beschrijven wat u in uw bewaarbeleid zou moeten opnemen en hoe u zorgt dat binnen M365 het beleid kan worden uitgevoerd.

8. Kwaliteit inrichting

De zorg voor kwaliteit houdt niet op bij een goede inrichting van een Team. Het vraagt om voortdurend monitoren, ondersteunen en sturen van gebruik en zorg voor het goed toegankelijk houden van de informatie. Hiervoor moeten zowel een geschikte organisatie als hulpmiddelen aanwezig zijn. Welke tools zijn hiervoor beschikbaar in M365 en hoe zorgt u dat u die goed kan gebruiken?

9. Toegankelijkheid

Informatie heeft alleen waarde als het verantwoord gebruikt kan blijven worden. We moeten dus zorgen dat de informatie die in M365 wordt bewaard voldoet aan de eisen voor duurzame toegankelijkheid. Dit hoofdstuk beschrijft de twee kanten hiervan: het openstellen van informatie en het beveiligen van informatie en geeft tips hoe u dit binnen M365 kan regelen.

10. De functionaliteit van Microsoft 365

Wat is nu eigenlijk M365, welke onderdelen zitten daarin en hoe verhouden ze zich tot Teams. Waar staat de informatie van al die onderdelen en welke tooling is er om deze informatie ook duurzaam toegankelijk te beheren en tijdig te vernietigen?

11. Gebruikers (Adoptie en gebruik)

Voor de inrichting van MS365 is het nodig om een aantal zaken goed op orde te krijgen. Het werkt optimaal als er een aantal stappen genomen wordt. Dan gaat het over het meenemen van een organisatie in en het maken van afspraken over het werken met Teams, afspraken over het opslaan van documenten en de manier waarop het beheer ingericht wordt.

3. Inleiding

Het is gewoon een feit: in M365 en met name via Teams wordt door gemeenten heel erg veel informatie verwerkt. Een groot deel daarvan moet bewaard of op tijd vernietigd worden. Het is niet mogelijk om deze verplichting uit te voeren zonder de informatie te structureren als deze ontstaat of wordt aangepast.

Gemeenten moeten daarom in actie komen om zo te voorkomen dat over een aantal jaren zoveel informatie aanwezig is in M365, dat verantwoord beheer niet meer mogelijk is. Het is belangrijk dat informatiebeheerders op zijn minst het minimale doen om voldoende grip te houden op deze informatie: niets doen is geen optie.

Hoe pakt u dit dan aan en wat heeft u nodig? Welke keuzes kunt u maken? Dat zijn vragen waar we een antwoord geven.

Doel van dit document:

- a. een document met praktische tips voor gemeenten (en andere organisaties) die beschrijft wat er nodig is om grip te krijgen op de informatie die wordt verwerkt en bewaard in Teams en M365 (binnen de eigen infrastructuur). Hierbij gaat het om het beschrijven van de technische inrichting, de organisatie en de competenties van de informatiebeheerders en gebruikers;
- b. het beschrijven van informatiebeheer en archivering in de context van Teams en M365. We geven de achtergrond, die voor velen misschien al bekend is, maar hier focussen we op de belangrijkste resultaten die gerealiseerd moeten worden in M365.

We hebben een aantal onderwerpen uitgewerkt die het maken van goede keuzes ondersteunen. We werken zoveel mogelijk vanuit de standaard functionaliteiten van M365. Een uitgangspunt is dat maatwerk minimaal wordt toegepast. De meeste gemeenten gebruiken M365 en door het minimaliseren van maatwerk of specifieke tooling kunnen we maximaal profiteren van de kennis en ervaring van al onze collega's bij andere gemeenten.

M365 is een pakket met veel verschillende functionaliteiten. Teams is een veelgebruikt onderdeel, maar ook Sharepoint en Exchange (e-mail) zijn onderdeel hiervan. We hebben een apart hoofdstuk waarin we beschrijven waar M365 uit bestaat.

In dit document spreken we vooral over Teams als voorkant voor de gebruikers. Bij de verwerking van de informatie wordt daarmee de andere functionaliteit van M365 op de achtergrond gebruikt. Het is natuurlijk ook mogelijk om de andere onderdelen direct aan de gebruikers aan te bieden. Het informatiebeheer en de archivering zijn van toepassing op heel M365, maar vragen dan mogelijk nog aanvullende inrichting.

4. Scenario's voor Teams

Er zijn verschillende manieren waarop u Teams kunt positioneren als het gaat over het beheren van informatie. Elke manier stelt andere eisen aan de inrichting van techniek en de organisatie. We lichten drie verschillende scenario's toe.

4.1. Korte beschrijving scenario's

Scope beschrijven: samenwerken in relatie tot goed archiefbeheer.

Scenario	Korte toelichting
Samenwerken in Teams	Teams wordt ingezet voor samenwerking. De informatie is beperkte tijd toegankelijk en wordt slechts minimaal archieftechnisch beheerd. Archiefwaardige informatie wordt in het zaakstelsel (of een processysteem) beheerd.
Archiveren in Teams	De informatie die binnen Teams ontstaat of wordt gebruikt wordt hierin archiefwaardig beheerd. Met name intern getriggerde en kennis gerelateerde processen kunnen nu in Teams gearchiveerd worden. Denk aan: beleid, onderzoek, rapportage en projecten. Dienstverlenende en sturende processen zitten in het zaakstelsel of een processysteem.
Zaakgericht werken in Teams	Teams is ingericht als een volwaardig zaakstelsel waarin ook de dienstverlenende en sturende processen behandeld en beheerd worden.

N.B. OneDrive is buiten scope. OneDrive is de locatie waar u uw persoonlijke werkbestanden kunt opslaan. Deze zijn privé tenzij u beslist ze te delen.

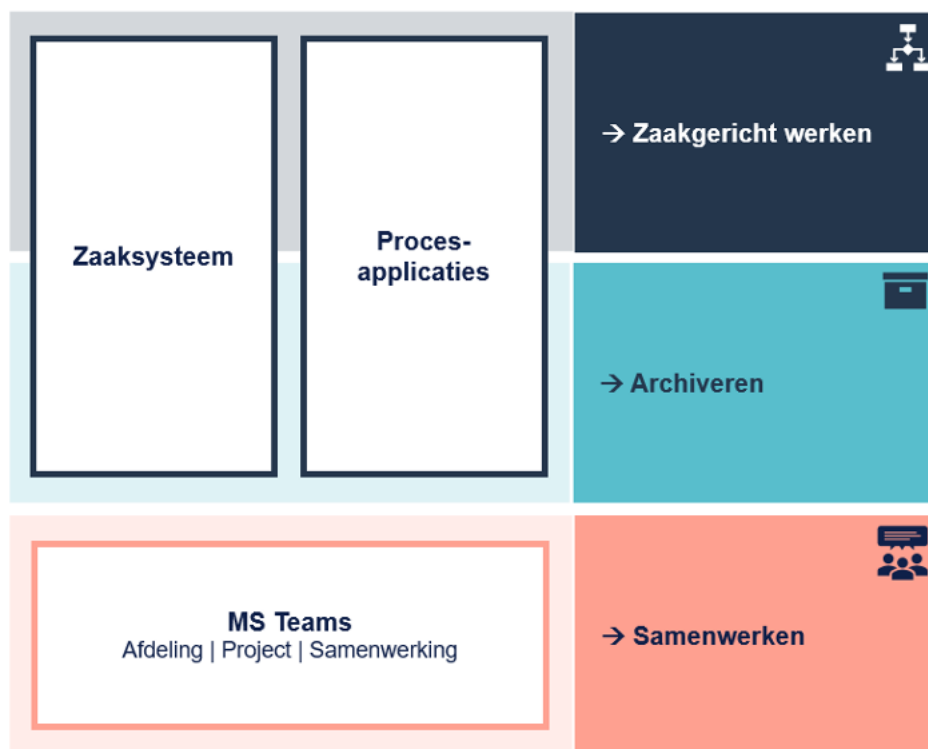
Ook buiten scope is een eventueel plug in met Word, Excel, PowerPoint en Outlook waarbij nieuwe (gecreëerde) documenten of (bijlagen in) mail direct in het zaakstelsel kan worden opgeslagen. Of andersom vanuit de Office omgeving documenten uit het zaakstelsel geopend, bewerkt en opgeslagen kunnen worden.

4.2. Scenario 1: Samenwerken in Teams

4.2.1 Het informatielandschap

Teams wordt in dit scenario ingezet voor samenwerking binnen afdelingen, projecten of andere vormen van samenwerken. De informatie is beperkte tijd toegankelijk en wordt slechts minimaal archief technisch beheerd. Archiefwaardige informatie wordt opgeslagen in het zaakstelsel of procesapplicatie.

In het zaakstelsel wordt digitaal en zaakgericht gewerkt. Het zaakstelsel voldoet aan alle eisen voor duurzame bewaring van informatie. Bij zaakgericht werken is 'archiving by design' en 'privacy by design' het uitgangspunt. In een procesapplicatie wordt doorgaans zaak- of taakgericht gewerkt. Een applicatie kan echter ook cliënt of object georiënteerd zijn ingericht.



In dit scenario beschrijven we het gebruik van drie templates in MS Teams. Uiteraard is dit slechts een voorbeeld en kan dit door een organisatie naar eigen inzicht ingericht worden.

- **Afdeling**
is samenwerking binnen de afdeling, (kern)team of cluster. Dit is een besloten team waar alleen de medewerkers van die organisatie-eenheid aan deelnemen.
- **Project**
is een tijdelijke samenwerking gericht op het opleveren van een uniek resultaat vaak begrensd in tijd en middelen (met interne collega's en/of externe gasten). Voor een programma kan ook het template 'project' gebruikt worden.
- **Samenwerking**
betreft samenwerking met interne collega's en/of externe gasten. Bijvoorbeeld voor terugkerend afdeling overstijgend, organisatie breed of regionaal overleg waarbij de vergaderstukken in Teams worden gedeeld.

4.2.2 Welke informatie zit in welk systeem

Wat moet in het zaaksysteem?

Alle archiefwaardige informatie met een definitieve status dient in het zaaksysteem (of in een archiefwaardige procesapplicatie) te worden gearcheveerd als:

- het correspondentie betreft met burger/bedrijf/ketenpartner;
- het een formeel intern verzoek, advies of besluit(vorming) betreft (bijvoorbeeld een besluit van college en/of raad, algemeen bestuur en/of dagelijks bestuur);
- het een bindende afspraak bevat, vaak is deze formeel ondertekend (bijvoorbeeld beschikkingen, vergunningen, contracten en overeenkomsten);

Wat mag in Teams?

- Alle documenten in conceptfase.
- Alle documenten met een definitieve status die niet voldoen aan de voorwaarden waarbij er in het zaaksysteem moet worden gearcheveerd.

Voorbeelden: werkoverleg, werkinstructies, opleidingsmateriaal, werk- en vakantieroosters, externe wet- en regelgeving van uw taakveld, kleinschalige projecten binnen uw eigen team bijv. ter verbetering van de eigen processen/dienstverlening, communicatie uiting intern, evenement organisatie, geschenk melding, representatie, training personeel.

Aandachtspunt: in Teams horen geen persoonsgegevens. Dit vraagt namelijk extra beheer. Als een gebruiker wel persoonsgegevens gebruikt moet hij de versie - na archivering in het zaaksysteem - in Teams verwijderen.

Let op: medewerkers zullen veelal gebruik blijven maken van de informatie in Teams als ze deze willen hergebruiken. De aanwezigheid van alle informatieobjecten in Teams is eindig en wordt na verloop van tijd vernietigd. Deze zijn dan niet meer op die plaats beschikbaar voor de medewerkers.

4.2.3 Rollen, verantwoordelijkheden en bevoegdheden

Teamlid

- Slaait informatie op de juiste plaats (in de juiste applicatie en in de juiste structuur conform de afspraken binnen de organisatie) op.
- Slaait informatie in Teams in de juiste structuur met een heldere naamgeving op zodat anderen het gemakkelijk kunnen terugvinden en interpreteren.
- Slaait archiefwaardige informatie op in het zaaksysteem.

Teameigenaar

- Kiest de juiste 'template', bijv. Afdeling, Project, Samenwerking.
- Structureert de informatie m.b.v. kanalen en mappen.
- Bewaakt dat teamleden informatie op de juiste plaats gestructureerd opslaan voorzien van een heldere naam.
- Stimuleert en bewaakt dat archiefwaardige informatie wordt opgeslagen in het zaaksysteem. Let op: bij een project draagt de teameigenaar zelf zorg voor het archiveren van het project in het zaaksysteem.
- Sluit een kanaal of team in Teams tijdig af.

- Past de teamleden aan bij wijzigingen in de Teamsamenstelling. Dit geldt ook voor het eigenaarschap.

Recordmanager/adviseur informatiebeheer

- Richt een minimaal beheerregime voor Teams in.
- Beoordeelt een aanvraag voor een nieuw team o.b.v. archiefkaders.
- Begeleidt medewerkers in het juiste gebruik van Teams met betrekking tot archiefbeheer.
- Heeft rechten om in Teams te zoeken (afdeling, project, samenwerking).
- Toetst of de informatie op de juiste plaats is opgeslagen.
- Bewaakt of informatie in een (ook afgesloten of verwijderd) team correct gearchiveerd is in het zaaksysteem.
- Zorgt voor tijdige vernietiging van informatie.

Functioneel beheerder

- Beoordeelt een aanvraag voor een nieuw team o.b.v. Informatietechnologische kaders.
- Past de teamleden aan bij wijzigingen in de samenstelling van een afdeling (bij in-, door- en uitstroom van medewerkers). Dit kan geautomatiseerd worden ingericht.
- Is back up voor het aanpassen van de teameigenaar en teamleden als teameigenaar in gebreke blijft.
- Bewaakt de toegang voor gastgebruikers (zijn ze nog actief?).

4.2.4 Informatiebeheerprocessen

Identificeren	Teameigenaar en teamleden beoordelen welke informatie archiefwaardig is en in het zaaksysteem (of procesapplicatie) moet worden bewaard. Om dit consequent goed te laten plaats vinden moet archiefbewustzijn worden ontwikkeld in de organisatie. Mogelijk zou u ook binnen uw organisatie kunnen afspreken om te realiteren: dus in het zaaksysteem te verwijzen naar Teams en andersom. Zodat bij een verkeerde inschatting van de archiefwaardigheid van de informatie die nog wel vindbaar is.
Archiveren en waarden	<ul style="list-style-type: none"> • Teameigenaar en/of teamlid zet een kopie van de informatie in het zaaksysteem (of procesapplicatie) met het juiste resultaat. • Teameigenaar en/of teamlid verwijdert indien nodig handmatig informatie in Teams.
Vernietigen	<ul style="list-style-type: none"> • Teameigenaar en/of teamlid schoont, sluit af of verwijdert tijdig het team na het archiveren van relevante informatie in het zaaksysteem (of procesapplicatie). • Recordmanager richt een minimaal beheerregime in dat zorgt dat informatie in Teams op tijd vernietigd wordt. Beheersmaatregel kan bijvoorbeeld zijn dat informatie na 10 jaar na ontstaan verwijderd wordt. In het beheerregime dienen de procedure en voorwaarden voor vernietiging nader uitgewerkt te worden. • Recordmanager vernietigt tijdig informatie die hiervoor in aanmerking komt.
Overbrengen	Vindt niet plaats vanuit Teams.
Preserveren	Vindt niet plaats vanuit Teams.
Kwaliteitsbewaking en –zorg	<ul style="list-style-type: none"> • Recordmanager toetst of op de juiste manier met informatie in Teams wordt omgegaan, koppelt terug en zorgt voor herstel. • Recordmanager toetst of alle archiefwaardige informatie is ondergebracht in zaak- of processystemen. • Monitoren op inactieve sites en sites zonder eigenaar.

Publiceren en hergebruik	<ul style="list-style-type: none"> • Actief publiceren van informatie is een verantwoordelijkheid van de medewerker. Dit is niet voor Teams van toepassing omdat de definitieve versie in het zaak- of processysteem staat. • Duurzame toegankelijkheid ten behoeve van verantwoording en hergebruik is geborgd middels het zaak- of processysteem. Wel moet er rekening mee worden gehouden dat de informatie in Teams ook toegankelijk moet kunnen zijn voor intern hergebruik. Specifiek moet er aandacht zijn voor het beantwoorden van WOO verzoeken en verzoeken inzage gebruik persoonsgegevens.
--------------------------	---

4.2.5 Archiveringseisen en benodigde functionaliteiten en componenten

	<ul style="list-style-type: none"> • Licentie MS 365
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Minimaal E3 licentie.
	<ul style="list-style-type: none"> • Kopiëren naar zaakstelsysteem en evt. procesapplicaties
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Er is minimaal een functie (zie hoofdstuk 7) waarmee een gebruiker eenvoudig (een set aan) informatie kan kopiëren naar het zaakstelsysteem en evt. procesapplicaties als nieuwe zaak of toevoeging op een bestaande zaak. ○ <u>Optioneel: uitgebreide koppeling met zaakstelsysteem en evt. processysteem</u> Een uitgebreide koppeling of integratie met het zaakstelsysteem geeft gebruikers meer gemak en zorgt ervoor dat meer informatie onder archiefregime komt. Functies van de koppeling: <ul style="list-style-type: none"> - Starten van een team of kanaal vanuit een lopende zaak in het zaakstelsysteem. - Een document vanuit Teams direct opslaan in het zaakstelsysteem. - Een team of kanaal automatisch als gestructureerde zaak opslaan in het zaakstelsysteem. - Een actieve link in Teams maken naar informatie in een zaak- of processysteem (en vice versa).
	<ul style="list-style-type: none"> • Vindbaar
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Er is een zoekfunctie waarmee alle informatieobjecten binnen Teams vindbaar zijn binnen redelijke tijd en inspanning. Bijvoorbeeld voor WOO en AVG verzoeken.
	<ul style="list-style-type: none"> • Export (sturingsinformatie)
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Er is een overzicht van alle Teams en de mate van activiteit voor bewaking kwaliteit en gebruik. ○ Er is een overzicht van verwijderde Teams waarmee de recordmanager kan bewaken of de informatie goed is gearchiveerd in het zaakstelsysteem.
	<ul style="list-style-type: none"> • Inzagerecht
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Een informatieobject is toegankelijk voor iedereen die op basis van regelgeving en beleid inzagerecht heeft. Ofwel het gebruikersbeheer is op orde.
	<ul style="list-style-type: none"> • Beveiliging
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Aanbeveling: documenten, na het archiveren in het zaakstelsysteem, op niet bewerkbaar zetten, zodat ze beveiligd zijn tegen onbedoelde wijzigingen.
	<ul style="list-style-type: none"> • Metagegevens
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ De weergave en export van elk informatieobject bevat een minimale set aan metadata, inclusief de context, zodat bij het overzetten ervan naar een ander systeem deze ook met de juiste kwaliteit kan worden geregistreerd.
	<ul style="list-style-type: none"> • Vernietiging
	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Informatieobjecten worden niet eerder en niet later vernietigd dan is aangegeven in de selectielijst.

4.3. Scenario 2: Archiveren in Teams

4.3.1 Het informatielandschap

De informatie die binnen Teams ontstaat of wordt gebruikt, wordt in Teams archiefwaardig beheerd. Dit scenario is interessant voor kenniswerkers. Intern getriggerde processen waarbij co-creatie, projectmatig werken en kennismanagement een rol spelen kunnen in Teams gearchiveerd worden. Denk aan: beleidsvoorbereiding, projecten, onderzoeken en interne rapportages. Dienstverlenende en sturende processen worden afgehandeld in het zaakstelsel of in een procesapplicatie.



4.3.2 Welke informatie zit in welk systeem

Wat moet in het zaakstelsel?

Alle archiefwaardige informatie met een definitieve status dient in het zaakstelsel (of in een archiefwaardige procesapplicatie) te worden gearchiveerd als:

- het correspondentie betreft met burger/bedrijf/ketenpartner;
- het een formeel intern verzoek, advies of besluit(vorming) betreft (bijvoorbeeld een besluit van college en/of raad, algemeen bestuur en/of dagelijks bestuur);
- het een bindende afspraak bevat, vaak is deze formeel ondertekend (bijvoorbeeld beschikkingen, vergunningen, contracten en overeenkomsten);

Met uitzondering van beleidsvoorbereiding, project, samenwerking, onderzoek en interne rapportages.

Wat mag in Teams?

- Alle documenten in conceptfase.
- Alle documenten met een definitieve status die niet voldoen aan de voorwaarden waarbij er in het zaakstelsel moet worden gearchiveerd behalve documenten m.b.t. beleidsvoorbereiding,

projecten, onderzoeken, interne rapportages en vergaderstukken van afdelingoverstijgend, organisatie breed of regionaal overleg.

4.3.3 Rollen, verantwoordelijkheden en bevoegdheden

Teamlid

- Slaat informatie op de juiste plaats (in de juiste applicatie en in de juiste structuur conform de afspraken binnen de organisatie) op.
- Slaat informatie in Teams in de juiste structuur met de juiste metadata en een heldere naamgeving op zodat anderen het gemakkelijk kunnen terugvinden en interpreteren.
- Zorgt dat bij behandeling in een ander (zaak- of proces-) systeem de benodigde informatie wordt meegegeven. Het vermelden van een gerelateerd zaaknummer in Teams helpt om beter integraal te beheren.

Teameigenaar

- Kiest de juiste 'template', bijv. Afdeling, Project, Samenwerking.
- Structureert de informatie m.b.v. kanalen en mappen.
- Bewaakt dat teamleden informatie op de juiste plaats gestructureerd opslaan voorzien van metadata en een heldere naam.
- Sluit een kanaal of team in Teams tijdig af.
- Past de teamleden aan bij wijzigingen in de Teamsamenstelling. Dit geldt ook voor het eigenaarschap.

Recordmanager/adviseur informatiebeheer

- Richt het beheerregime in voor elk van de verschillende soorten informatie.
- Beoordeelt een aanvraag voor een nieuw team o.b.v. archiefkaders.
- Begeleidt medewerkers in het juiste gebruik van Teams met betrekking tot archiefbeheer.
- Heeft rechten om in Teams te zoeken (afdeling, project, samenwerking).
- Toetst of de informatie op de juiste plaats en in de juiste structuur met de juiste metadata is opgeslagen.
- Bewaakt of informatie in een (ook afgesloten of verwijderd) team correct gearchiveerd is.
- Zorgt voor tijdige vernietiging of overbrenging van informatie.

Functioneel beheerder

- Beoordeelt een aanvraag voor een nieuw team o.b.v. I&A kaders.
- Past de teamleden aan bij wijzigingen in de samenstelling van een afdeling (bij in-, door- en uitstroom van medewerkers). Dit kan geautomatiseerd worden ingericht. Een jaarlijkse controle op de juistheid van de autorisaties blijft noodzakelijk.
- Is back up voor het aanpassen van de teameigenaar en teamleden als teameigenaar in gebreke blijft.
- Bewaakt de toegang voor gastgebruikers.

4.3.4 Informatiebeheerprocessen

Identificeren	Teameigenaar en teamleden beoordelen welke informatie archiefwaardig is en in welke applicatie deze moet worden opgeslagen. Om dit consequent goed te laten plaatsvinden moet archiefbewustzijn worden ontwikkeld in de organisatie.
Archiveren en waarderen	<ul style="list-style-type: none"> • Teameigenaar en/of teamlid kopieert informatie die betrekking heeft op zijn project en centraal ontvangen en geregistreerd is in het zaaksysteem naar Teams. • Teameigenaar en/of teamlid verwijdert/schoont indien nodig handmatig informatie in Teams. • Teamleider en/of teamlid geven in Teams aan hoelang de informatie bewaard moet worden. • Recordmanager voert beheer uit op zaken met een conditionele bewaartermijn. De teameigenaar voorziet in informatie hierover. • Teameigenaar sluit tijdig het team af en bepaalt voor wie de informatie toegankelijk is.
Vernietigen	<ul style="list-style-type: none"> • Recordmanager richt een beheerregime in m.b.v. templates, documentensets en kanalen. Bij project en samenwerking worden bijv. resultaattypen ingericht conform de Selectielijst. In het beheerregime dienen de procedure en voorwaarden voor vernietiging nader uitgewerkt te worden. • Recordmanager vernietigt tijdig informatie die hiervoor in aanmerking komt. • Recordmanager doet check op relatie met hotspots en zorgt dat die sites uitgezonderd worden van vernietiging.
Overbrengen	Recordmanager brengt informatie tijdig over die hiervoor in aanmerking komt.
Preserveren	Recordmanager neemt tijdig maatregelen voor het preserveren van de informatie.
Kwaliteitsbewaking en –zorg	<ul style="list-style-type: none"> • Recordmanager toetst of op de juiste manier met informatie in Teams wordt omgegaan, koppelt terug en zorgt voor herstel. • Recordmanager toetst of, indien van toepassing, de juiste relatie is gelegd met zaken in het zaaksysteem (bijv. voorbereiding in Teams en besluitvorming in het zaaksysteem) en of eenzelfde bewaartermijn is aangegeven. • Monitoren op inactieve sites en sites zonder eigenaar.
Publiceren en hergebruik	<ul style="list-style-type: none"> • Actief publiceren van informatie is een verantwoordelijkheid van de medewerker. • Recordmanager zorgt dat de informatie duurzaam toegankelijk is voor verantwoording en hergebruik.

4.3.5 Archiveringseisen[1] en benodigde functionaliteiten en componenten

<ul style="list-style-type: none"> • Licentie MS 365 	<ul style="list-style-type: none"> o E5 licentie met geavanceerde compliance. Noodzakelijk zijn: Advanced eDiscovery, Advanced Audit, Automatisch bewaarbeleid en vertrouwelijkheidslabels
<ul style="list-style-type: none"> • Kopiëren naar zaaksysteem en evt. procesapplicaties 	<ul style="list-style-type: none"> o Er is minimaal een functie waarmee een gebruiker eenvoudig (een set aan) informatie kan kopiëren naar het zaaksysteem en evt. procesapplicaties als nieuwe zaak of toevoeging op een bestaande zaak. o Gewenst is ook de functie om een actieve link in Teams te maken naar informatie in een zaak- of processysteem (en vice versa). o Een uitgebreide koppeling of integratie met het zaaksysteem en evt. processysteem is niet noodzakelijk.
<ul style="list-style-type: none"> • Vindbaar 	

	<ul style="list-style-type: none"> o Er is een zoekfunctie over het zaakstelsel en Teams heen waarmee alle informatieobjecten vindbaar zijn, binnen redelijke tijd en inspanning.
	<ul style="list-style-type: none"> • Weergave
	<ul style="list-style-type: none"> o Van elk informatieobject is een weergave beschikbaar, binnen redelijke tijd en inspanning.
	<ul style="list-style-type: none"> • Export
	<ul style="list-style-type: none"> o Van elk informatieobject is een export beschikbaar, binnen redelijke tijd en inspanning (voor bijvoorbeeld migratie). o Er is een overzicht van alle Teams met activiteit voor bewaking kwaliteit en gebruik. o Er is een overzicht van verwijderde Teams waarmee de recordmanager kan bewaken of de informatie goed is gearchiveerd in het zaakstelsel.
	<ul style="list-style-type: none"> • Inzagerecht
	<ul style="list-style-type: none"> o Een informatieobject is toegankelijk voor iedereen die op basis van regelgeving en beleid inzagerecht heeft.
	<ul style="list-style-type: none"> • Beveiliging
	<ul style="list-style-type: none"> o Informatieobjecten zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen. Conform de geldende standaarden voor informatiebeveiliging.
	<ul style="list-style-type: none"> • Standaardformaat
	<ul style="list-style-type: none"> o De export van een informatieobject voldoet aan een open standaardformaat.
	<ul style="list-style-type: none"> • Metagegevens
	<ul style="list-style-type: none"> o De weergave en export van elk informatieobject dat niet gearchiveerd wordt in Teams bevat een minimale set aan metadata, inclusief de context, zodat bij het overzetten ervan naar een ander systeem deze ook met de juiste kwaliteit kan worden geregistreerd. o De weergave en export van elk informatieobject dat wél in Teams wordt gearchiveerd bevat minimaal volledige en actuele metagegevens zoals voorgeschreven in de Richtlijn Metagegevens Overheidsinformatie.
	<ul style="list-style-type: none"> • Vernietiging
	<ul style="list-style-type: none"> o Informatieobjecten worden niet eerder en niet later vernietigd dan is aangegeven in de selectielijst. o Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar.
	<ul style="list-style-type: none"> • Overbrenging
	<ul style="list-style-type: none"> o Een blijvend te bewaren informatieobject wordt binnen twintig jaar (op termijn 10 jaar) overgebracht naar een archiefbewaarplaats.

4.4. Scenario 3: Zaakgericht werken in Teams

4.4.1 Het informatielandschap

Teams is in dit scenario ingericht als een volwaardig zaakstelsel waarin ook de dienstverlenende en sturende processen behandeld worden.



4.4.2 Archiveringseisen en benodigde functionaliteiten en componenten

Ook voor dit scenario is een E5 licentie van MS 365 benodigd met geavanceerde compliance. Noodzakelijk zijn: [Advanced eDiscovery](#), Advanced Audit, Automatisch bewaarbeleid en [vertrouwelijkheidslabels](#).

Aanvullend op hetgeen in paragraaf 3.5 beschreven staat dient voor dit scenario het volgende ingericht te worden (opsomming is niet uitputtend):

Beschrijving	Toelichting
Formulieren	Extern en intern als frontend voor burger en gebruiker
Statusinformatie voor de burger	PIP, APPS/DSO, Mijn overheid, Mijn gemeente
Registratie van klantcontacten	KCC Antwoord, Portaal en klantbegeleiding/afspraken
Registratie van post en e-mail	Welke centraal ontvangen wordt via de postbus, balie en centrale mailbox
Registratie van What's app, twitter, SMS, chatbot	
Werkvoorraad	
Zaak afhandeling	Generiek Zaakafhandelcomponent (GZAC)
Zaken	Zaken API, Zakenregister en zaaktype-inrichting conform DSP/ZTC
Zoeken	Zoek API

Beheer van zaken en zaaktypen	Let op: archiefvernietiging, archiefoverbrenging en bewaartermijnen volgens Selectielijst
Documentsjablonen	
Bestuurlijke besluitvorming	
Contractbeheer	
Koppeling met BRP en Handelsregister	Haal Centraal BRP API, KVK API, Objecten API
Vervanging van archiefbescheiden	Koppeling met scan apparatuur
Versturen van een ontvangstbevestiging	
Voortgangsbewaking	
Digitale handtekening	Enkelvoudig en meervoudig

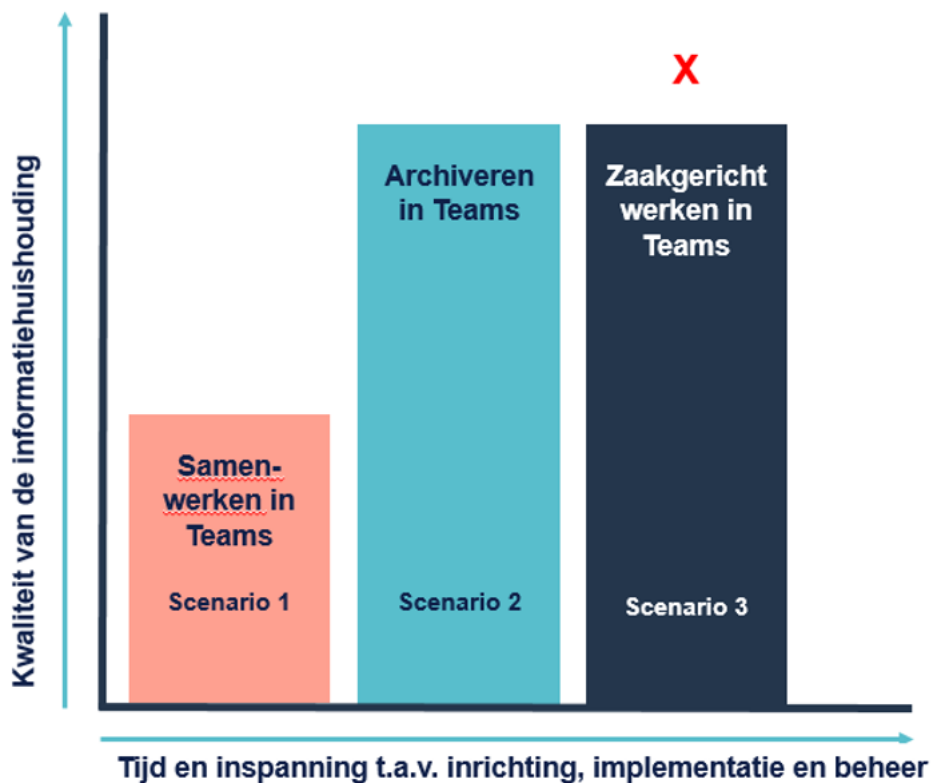
4.4.3 Advies scenario 3

Dit scenario is complex. Experts ontraden om MS Teams in te richten als zaakstelsel. Het behoeft maatwerk, kan niet gebouwd worden met standaard componenten, past niet in de Common Ground gedachte. Dit scenario is om deze reden niet gewenst en niet nader uitgewerkt.

De markt kent ook zaaksystemen die volledig ontwikkeld zijn met bouwblokken uit het M365 platform met een goede integratie met het product MS Teams. Teams is hierbij een aanvulling op het zaakstelsel voor die taken of producten die zich minder goed lenen voor zaakgericht werken en archiveren. Teams staat hierbij volledig los van het zaakstelsel. Ofwel het zaakstelsel staat op zichzelf en is daarmee onder te brengen in scenario 2.

4.5. Conclusie

Zoals eerder is beschreven ontraden wij scenario 3 'Zaakgericht werken in Teams'. Naast de eerdergenoemde nadelen kost het relatief veel tijd en inspanning om Teams in te richten voor zaakgericht werken. De kwaliteit van de informatiehuishouding stijgt hier niet mee. We zien wel een duidelijk verschil tussen scenario 1 en 2. Hoe meer tijd en inspanning in de inrichting, implementatie en het beheer gestopt wordt hoe hoger de kwaliteit van de informatiehuishouding. Ook het gebruiksgemak is in scenario 2 hoger als in scenario 1 omdat een gebruiker in scenario 1 bewust moet archiveren in het zaakstelsel. Scenario 2 'Samenwerken in Teams' kan ook een opmaat zijn naar het scenario 'Archiveren in Teams'.



Binnen het scenario 'Archiveren in Teams' zijn verschillende keuzes te maken. Deze keuzes hebben niet of nauwelijks invloed op de beschreven rollen, verantwoordelijkheden, bevoegdheden, informatiebeheerprocessen, archiveringseisen en benodigde functionaliteiten en componenten. Ze hebben wel invloed op welke informatie in welk systeem zit (dit raakt de gebruiker) en het beheerregime voor de verschillende soorten informatie (dit raakt de recordmanager en kan ook eisen stellen aan de gebruiker).

Hieronder staan de belangrijkste voor- en nadelen van de verschillende scenario's op een rij. Iedere organisatie kan zelf de afweging maken welk scenario het beste past en evt. in welk tempo evt. doorontwikkeling gewenst is.

	Samenwerken in Teams	Archiveren in Teams	Zaakgericht werken in Teams
Inspanning en tijd t.a.v. inrichting en implementatie	+	-	--
Inspanning en tijd t.a.v. beheer	+	-	--
Informatie bewaren aan de bron	-	+	+
Gebruiksvriendelijk	+	++	++
Gebruikers dienen (een set aan) documenten bewust over te zetten naar het zaakstelsel (of procesapplicatie).	-	++	++
De mate waarin in 1 systeem gewerkt kan worden	-	+	++
Complexiteit inrichting	0	0	--
...			

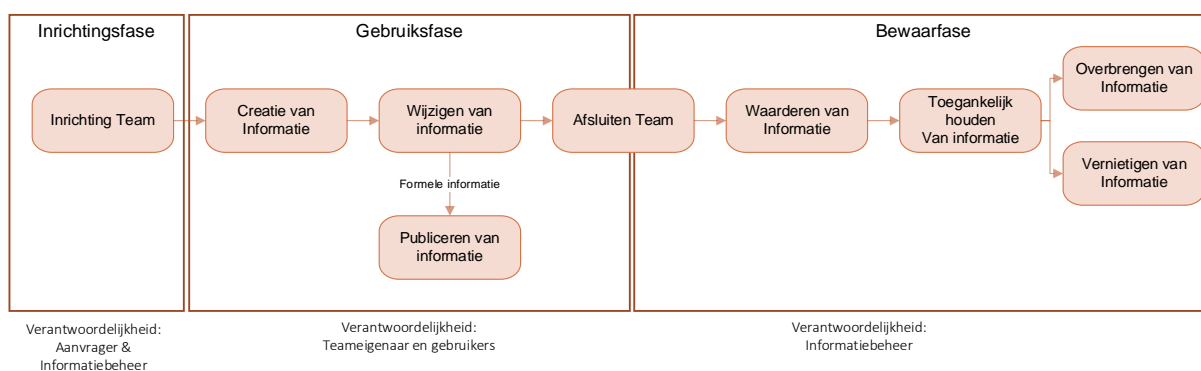
5. Beheren van informatie in een team

De processen voor informatiebeheer volgen de levenscyclus van een informatieobject. In Microsoft Teams zijn dit zowel een Team, een Kanaal als de documenten en registraties daarbinnen. We beschrijven welke processen moeten worden georganiseerd, welke activiteiten moeten worden uitgevoerd om grip te houden op de verwerkte informatie in M365 en wie waarvoor verantwoordelijk is.

5.1. Uitgangspunten

Voor het beheren van informatie worden verschillende processen uitgevoerd. Deze processen realiseren de levenscyclus van de informatieobjecten en de context - een documentenset - waar deze in zijn verwerkt.

Het onderstaande schema beschrijft van de levenscyclus van een Team en informatieobjecten in relatie tot de uit te voeren processen.



5.2. Processen voor Informatiebeheer

Informatiebeheer is het beheren van de verzameling, de opslag, het bewaren/vernietigen en het onderhoud van informatie in al haar vormen. We gaan uit van het werken in MS Teams. Teams is echter een verzameling van verschillende applicaties, zoals bijvoorbeeld SharePoint. Als het belangrijk is zullen we ook verwijzen naar die specifieke applicaties.

Meer uitleg over de opbouw van Teams en M365 staat in hoofdstuk 10

De processen zijn opgedeeld in drie fasen:

- Inrichtingsfase
- Gebruiksfase
- Bewaarfase

5.3. Inrichtingsfase

Bij het openen van een Team is het belangrijk om te zorgen dat informatie in een passende structuur kan worden verwerkt. Het uitgangspunt is dat de gebruiker met zo weinig mogelijk inspanning de informatie die wordt verwerkt op een goede manier kan vastleggen. Dit vraagt om een samenspel van de aanvrager van het Team, Informatiebeheer en functioneel beheer M365.

In [Hoofdstuk 6](#) zijn voor het inrichten van een Team een aantal randvoorwaarden en tips beschreven.

5.3.1 Aanvragen Team

Een Team wordt aangevraagd door een gebruiker. Bij de aanvraag van een Team moet informatie worden meegegeven waarmee bepaald wordt welk bewaarbeleid van toepassing zal zijn en wat een passende inrichting is voor het Team.

Een goede naam en eventueel een toelichting maken voor Team is erg belangrijk. Deze maakt het vinden van informatie voor gebruikers eenvoudig en beschrijft de context van de informatie die daarbinnen wordt verwerkt.

Bij de aanvraag moet ook de eigenaar van het Team worden opgegeven. In de gebruiksfase is deze eigenaar verantwoordelijk voor de juiste verwerking van de informatie en het nakomen van de gebruiksvoorwaarden.

5.3.2 Beoordeling van de aanvraag

Informatiebeheer beoordeelt de aanvraag. Het is belangrijk om te bepalen of Teams wel de juiste plaats is om in te werken. Dit is afhankelijk van het scenario voor M365 dat is gekozen. Voor bepaalde bedrijfsprocessen zal bijvoorbeeld gewerkt moeten worden in een proces- of zaaksysteem.

Vervolgens wordt bepaald wat het bewaarbeleid is en welke kaders voor het structureren van de informatie van toepassing zijn. In het bewaarbeleid bepaalt u ook welke metadata nodig is om goed beheer uit te voeren. Hierbij moet u wel rekening houden met de administratieve last voor de gebruikers. Zie ook [6.2.9](#).

Meer uitleg over de inhoud van het bewaarbeleid staat in [hoofdstuk 7](#).

Het kan belangrijk zijn om specifieke statussen van informatie vast te leggen. Bijvoorbeeld als een formele versie herkenbaar moet blijven. Dit vraagt om aanvullende afspraken en kan een reden zijn voor het gebruik van SharePoint documentsets.

Een gebruiker kan behoefte hebben aan het gebruik van andere apps, waardoor informatie niet alleen in de standaard SharePoint en Exchange wordt bewaard. In het bewaarbeleid en de beheerprocessen moet rekening gehouden worden met de gevolgen hiervan.

5.3.3 Inrichten van het Team

Het Team wordt daarna aangemaakt met de vereiste en gewenste functionaliteit voor zowel het gebruik als het beheer. Hierbij wordt rekening gehouden met de specifieke eisen voor informatiebeheer. Het inrichten van het Team wordt gedaan door Functioneel beheer. Door Informatiebeheer vindt een kwaliteitstoets plaats op de inrichting voordat deze beschikbaar wordt gesteld.

Het is aan te raden om enkele [sjablonen](#) in te richten die als standaard kunnen worden gebruikt. Hiermee kunt u de basis eenvoudig toepassen en is het alleen nodig om wisselende informatie aan te passen.

Houdt er rekening mee dat het in deze fase nog niet mogelijk om al precies te weten welke informatie zal worden verwerkt en te bepalen hoe deze moet worden vastgelegd. Een deel zal bepaald worden in de gebruiksfase.

In de gebruiksfase is ruimte nodig om in een team kanalen aan te laten maken en zelf gebruikers, vertrouwelijkheid etc. aan te passen. Zo krijgt u een team dat bij de samenwerking past. De verantwoordelijkheid hiervoor ligt bij de Team-eigenaar.

5.3.4 Beschikbaar stellen van het Team

Het team wordt beschikbaar gesteld aan de eigenaar. Deze krijgt ook nog informatie over de gebruiksvoorwaarden.

Belangrijk bij de overdracht is te zorgen dat de eigenaar en gebruikers weten welke specifieke metadata vastgelegd moet worden en hoe ze dit kunnen doen.

5.4. Gebruiksfase

5.4.1 Creatie van informatie

In de gebruiksfase werken gebruikers samen en maken, delen en wijzigen informatie in documenten en berichten. Voortdurend worden informatieobjecten gecreëerd, toegestuurd of op andere wijzen verwerkt. Bij het werken in Teams worden deze op de achtergrond door SharePoint voorzien van diverse (standaard)kenmerken. Dit is de metadata die we voor goed informatiebeheer nodig hebben.

Het kan nodig zijn dat gebruikers extra kenmerken aan de informatieobjecten toevoegen. Hiermee zijn deze bijvoorbeeld voor andere gebruikers makkelijker terug te vinden. Met name moet ervoor gezorgd worden dat die metadata wordt toegevoegd die nodig is om informatie te kunnen waarderen en te voorzien van het juiste bewaarbeleid.

De gebruiker kan metadata vanuit Teams aan een bestand toekennen, maar ook bijv. in Word of een andere MS Office-applicatie via het eigenschappenvenster.

5.4.2 Wijzigen van informatie

Een belangrijke reden voor het gebruik van Teams is om samen documenten te maken. Dit betekent dat de documenten door gebruikers veel worden aangepast. Doordat op de achtergrond met SharePoint wordt gewerkt, is versiebeheer standaard ingericht. Deze metadata hoeft de gebruiker niet apart vast te leggen.

Als gebruikt gemaakt wordt van document statussen, zullen deze moeten worden vastgelegd.

Gebruikers kunnen in deze fase ook informatie verwijderen. Binnen Teams komt deze dan in de prullenbak. Hierop is ook beheer en retentie mogelijk. Zie hiervoor 6.2.8

5.4.3 Verantwoordelijkheden tijdens de gebruiksfase

De Teameigenaar is verantwoordelijk voor de juiste verwerking van informatie tijdens de gebruiksfase. Deze bepaald welke informatie wordt verwerkt en zorgt dat dit rechtmatig gebeurt. Hierbij hoort ook het geven van toegangsrechten aan gebruikers.

Informatiebeheer heeft in deze fase een rol als adviseur en kwaliteitsbewaker.

5.5. Bewaarfase

5.5.1 Afsluiten Team

De teameigenaar sluit een Team of kanaal af als er niet meer in gewerkt gaat worden. Hierdoor kan de informatie niet meer worden aangepast door de gebruikers.

5.5.2 Waardering / kwaliteitscontrole

Na het afsluiten voert Informatiebeheer een kwaliteitscontrole uit. Ze beoordeelt of het dossier compleet is en wijst de juiste bewaartermijn toe aan de informatie. Zo nodig wordt aan de Teameigenaar gevraagd om ontbrekende of onjuiste informatie aan te vullen.

Informatiebeheer stelt de bewaartermijn van de informatie in.

Daarna wordt het definitief afgesloten en daarmee gearchiveerd. Hiermee is de informatie definitief en kan niet meer aangepast worden.

5.5.3 Toegankelijk houden van informatie (bewaren)

Nu het team en alle informatieobjecten definitief zijn afgesloten en de bewaartermijn is gestart moet informatiebeheer zorgen dat er geen wijzigingen meer worden toegebracht aan de informatie en de informatie in geordende staat toegankelijk blijft. Dit vraagt om monitoring van de informatie en tijdig herkennen als beheer nodig is.

5.5.4 Vernietiging

Vernietigen van een informatieobject betekent dat de gegevens waaruit het informatieobject bestaat niet meer zijn te reconstrueren. Hierdoor is het informatieobject als geheel niet meer toegankelijk te maken. Dit geldt ook voor aanwezige backups van de informatieobjecten en bijbehorende metadata.

Periodiek maakt Informatiebeheer een lijst met alle informatie waarvan de bewaartermijn is verstreken. Deze lijst wordt conform de vernietigingsprocedures beoordeeld en vastgesteld. Zo nodig wordt van informatie de bewaartermijn aangepast en van de vernietigingslijst gehaald. Denk bijvoorbeeld aan langer bewaren in verband met een Hot spot, bezwaar of beroep of vroegtijdige vernietiging in verband met de AVG.

Vervolgens wordt alle informatie op de vastgestelde vernietigingslijst verwijderd uit M365.

De functionaliteit voor vernietigen binnen M365 is beschreven in 10.2

Nb. Houdt er bij vernietigen rekening mee dat ook informatie over dit onderwerp op een andere plaats kan zijn bewaard. Zorg ervoor dat ook daar een vernietigingsprocedure start en die informatie wordt vernietigd.

5.5.5 Overbrengen/exporteren

Het is vanuit de archiefwet verplicht om overheidsinformatie die blijvend bewaard moet worden na uiterlijk twintig jaar aan een daarvoor aangewezen archiefbewaarplaats over te dragen (Bron: Nationaal Archief).

Om de informatie over te brengen wordt een export gemaakt die voldoet aan de eisen van de archiefdienst. Hiervoor moeten de volgende stappen worden doorlopen:

1. Identificeren van de over te brengen informatie
2. Verzamelen van de over te brengen informatie
3. Maken Exportbestand
4. Overbrengen naar archiefbewaarplaats.
5. Opstellen van een migratieverklaring
6. Verwijderen van de betreffende informatie uit M365

Nb. Houdt er bij overbrengen rekening mee dat ook informatie over dit onderwerp op een andere plaats kan zijn bewaard. Zorg ervoor dat deze ook wordt overgebracht naar de archiefbewaarplaats

5.6. Governance, Organisatie en rollen

5.6.1 Overwegingen voor informatie-governance

Bij het verwerken van informatie moet rekening gehouden worden met wettelijke en functionele kaders. Belangrijke wettelijke kaders zijn de AVG, de archiefwet en de BIO. Bij het gebruik van Teams zal ook de zorg georganiseerd moeten worden, zodat dit ook in het gebruik aan die kaders voldoet. Hiervoor richten we processen in en organiseren we taken, verantwoordelijkheden en bevoegdheden in verschillende rollen.

In het kort zijn de rollen en hun verantwoordelijkheden:

Teameigenaar

Is verantwoordelijk voor:

- de verwerking van informatie binnen het Team en neemt alle benodigde maatregelen om te zorgen dat vooraf afspraken gemaakt worden over de geldende kaders en ziet toe op de naleving hiervan.
- het goed structureren van de informatie in de gebruiksfase.

Teamlid

Is verantwoordelijk voor het verwerken en registreren van informatie zoals is afgesproken.

Recordmanager / Adviseur informatiebeheer

Is verantwoordelijk voor:

- het opstellen van de informatiebeheerkaders voor het werken in Teams, zowel generiek als gericht op specifieke aangevraagde Teams;
- het formuleren van het bewaarbeleid;
- het goed inrichten van een Team conform die kaders.

Adviseert:

- aan teamleden en -eigenaren over het structureren van informatie bij het werken in Teams
- aan Teameigenaren over verbetering van de vastlegging van informatie.

Bewaakt:

- of informatie op de juiste wijze is vastgelegd;
- of Teams op tijd en juist zijn afgesloten.

Voert archiefbeheerprocessen uit.

Directie

Is verantwoordelijk voor:

- het vaststellen van het bewaarbeleid;
- het vaststellen van de (informatiebeheer)kaders voor het werken in Teams;
- de kwaliteit van de verwerking van informatie in Teams.

Functioneel beheerder

- Boordeelt een aanvraag voor een nieuw team op basis van I&A kaders.
- Bewaakt het toegangsbeleid.
- Ondersteund in het gebruik van Teams.
- Richt een aangevraagd team in conform de specificaties.

Archiefinspecteur

- Adviseert over de juistheid van de inrichting van Teams met betrekking tot de archiefwet.

Nadere uitwerking van deze rollen is nog wel nodig. De exacte inhoud van de rollen is voor een deel afhankelijk van het scenario voor het beheer van informatie in Teams, zoals beschreven in hoofdstuk 4.

Het is verstandig om de governance uit te werken in een RASCI tabel. Mogelijk kan die voor alle gemeenten als basisstandaard worden gebruikt. Zie hiervoor Bijlage 2.

5.7. Kwaliteitszorg

Toezicht houden is een voortdurende aandacht van audit, verbetervoorstellen op inhoud en organisatie. Zie ook de tekst bij 8.

6. Inrichten van een team

6.1. Regelen van randvoorwaarden

Bij het samenwerken in een team wordt informatie verwerkt. Het proces is vaak minder gestructureerd en de informatie is vooraf lastiger te definiëren. Het is wel mogelijk om bij het inrichten van het team al rekening te houden met een aantal randvoorwaarden voor meer grip op informatie. Dit helpt om gebruikers al tijdens het samenwerken de informatie te laten structureren. Ook geeft het mogelijkheden om het beheer beter uit te voeren.

Dit hoofdstuk beschrijft de aandachtspunten bij het inrichten van een team en geeft tips voor hoe u dit op een goede manier kunt realiseren.

6.2. Aandachtspunten en tips bij het aanmaken van een team

Via [M365-ondersteuning](#) is te lezen hoe een nieuw team aangemaakt kan worden.

Bij het aanmaken van een nieuw Team zijn de volgende aandachtspunten van toepassing:

- rollen toekennen en bijbehorende rechten;
- naamgeving;
- interne en/of externe toegang;
- vertrouwelijkheid;
- retentie inrichten;
- gebruik apps;
- standaard sjablonen;
- Prullenbak;
- gebruik van metadatamodellen.

De technische eisen en mogelijkheden voor de inrichting van bovengenoemde aandachtspunten zijn te lezen in functioneel beheer ([hoofdstuk 5](#)).

6.2.1 Rollen

Bij het aanmaken van een nieuw Team zijn er drie rollen, die aan een teamlid gegeven kunnen worden; eigenaar, lid of gast. Voor meer informatie zie: [De mogelijkheden voor teameigenaren, leden en gasten in Teams](#). Aan een rol kunnen rechten (machtigingen) worden gegeven.

Voor het informatiebeheerproces is het belangrijk te bepalen of elk teamlid informatie mag toevoegen, delen en/of verwijderen.

Tip

- Per Team bepalen of er één of meerdere eigenaren moeten zijn.
- Bepalen welke rechten wenselijk zijn bij welke rol en wellicht per soort Team.

Advies

Benoem 2 eigenaren per team. Als er dan één vertrekt is er nog iemand die de verantwoordelijkheid heeft en kan beslissen.

6.2.2 Naamgeving

U kunt een naamgevingsbeleid voor groepen gebruiken om een consistente naamgevingsstrategie af te dwingen voor groepen die aangemaakt worden in uw organisatie. Door met een dergelijke strategie te werken is het voor de gebruiker inzichtelijker en makkelijker te beheren voor de functioneel beheerder. Het geeft ook beter inzicht in het soort Team en de daarbij behorende eisen/wensen, zoals retentie.

Tip

U kunt voor- of achtervoegsels gebruiken bij het aanmaken van een nieuwe Team. De voor-/achtervoegsels kunnen bestaan uit vaste tekenreeksen of gebruikerskenmerken die worden vervangen op basis van de gebruiker die de groep maakt. Zo kunt u bijvoorbeeld het doel of de kenmerken van de samenwerking in de naamgeving opnemen.

Advies

Stel naamgevingsbeleid op, zodat het voor de gebruikers duidelijk en voor de functioneel beheerder makkelijker te beheren is.

6.2.3 Toegang

Naast het intern gebruik van MS Teams is het belangrijk om keuzes te maken over gasttoegang en extern toegang. Voor meer informatie zie: [Beleidsadviezen voor het beveiligen van Teams-chats, -groepen en -bestanden](#).

Voor het informatiebeheerproces is het belangrijk te bepalen of er extern informatie mag worden gedownload, gedeeld, toegevoegd en/of verwijderd.

Tip

Het is belangrijk om bij het inrichten van een nieuw Team het toestaan van externe deelnemers te bepalen.

Advies

Maak een aantal standaard Teams (templates) aan met bijvoorbeeld een provisioningtool. Met een provisioning tool kunt u geautomatiseerd Teams of sites uitrollen op basis van een vooraf gedefinieerde structuur.

6.2.4 Vertrouwelijkheid

Vertrouwelijkheid kan op diverse niveaus ingericht worden; Team-, kanaal-, rol- of op bestandsniveau.

Voor het zeer gevoelige beveiligingsniveau kan een gevoeligheidslabel gebruikt worden om het team te classificeren. Dit label kan ook worden gebruikt om afzonderlijke bestanden in deze of andere Teams te classificeren en te versleutelen.

Voor het informatiebeheerproces is het belangrijk om vooraf met bijvoorbeeld beleid te bepalen hoe de classificatie van informatie in Teams moet worden ingericht.

Tip

U kunt bij het aanmaken van een Team de vertrouwelijkheid bepalen. Dit kan vanuit een standaard template of specifiek voor dit Team ingericht worden. U kunt er ook voor kiezen om de vertrouwelijkheid per document door de gebruiker te laten bepalen.

Advies

Maak een aantal standaard Teams (templates) aan met bijvoorbeeld een provisioningtool waarbij de vertrouwelijkheid per soort Team is bepaald. Alleen bij uitzonderingen de vertrouwelijkheid door de gebruiker laten bepalen.

6.2.5 Inrichten Retentie en vernietiging

Met retentie bepaalt u hoe lang iets aanwezig moet zijn binnen de registratie. Het gaat dus over het managen van bewaartermijnen en de vernietigingsdatum.

Informatieobjecten worden niet eerder en niet later vernietigd dan is aangegeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar. (Bron: Nationaal Archief)

In het bewaarbeleid stelt u vast of u archivering wilt toepassen, voor welke informatie en op welke locaties. Dat heeft alleen maar zin als u retentie ook in kunt richten in MS Teams. Dit is mogelijk met retentielabels (Zie ook paragraaf 'afsluiten'.)

Over de manier waarop u deze retentielabels kunt inrichten staan tips in **Error! Reference source not found.**

Tip

Wanneer u werkt met standaard Teams kunt u bij het maken hiervan retentielabels inrichten.

Als u al retentielabels toevoegt aan een Team of kanaal voordat een team in gebruik wordt genomen, kunt u ervoor zorgen dat alle informatie daarbinnen ook een bewaartermijn meekrijgt. Dit is een reden om het aanmaken van Teams niet vrij te laten binnen de organisatie, maar Informatiebeheer een rol te laten spelen bij het aanmaken van nieuwe Teams. Voorkom dus dat gebruikers zelfstandig een Team aanmaken.

Maak een aantal standaard Template Teams met retentielabels.

6.2.5.1 Bepalen bewaartermijn en retentielabels

Er is een keuze m.b.t. de inrichting van uw systeem die effect heeft op hoe u bewaartermijnen aan informatie koppelt. Zie kopje hieronder. Daarnaast moet u bij de inrichting van uw omgeving de juiste bewaartermijnen aan de juiste processen koppelen. Dit dient vastgelegd te worden en keuzes dienen beargumenteerd te worden (en gearhiveerd).

Keuzes en risico's

- Als u bij de start (de inrichting van uw systeem) gekozen hebt voor documentsets, heeft u waarschijnlijk een goede inrichting om uw bewaartermijnen direct aan de documentsets te hangen. Wanneer u hebt gekozen voor een inrichting op basis van sites en subhubs, ligt dat mogelijk ingewikkelder.
- Kies de juiste bewaartermijn.
- Beleg de rollen omtrent de afsluiting van uw dossier: wordt bijvoorbeeld het dossier afgesloten door de behandelend ambtenaar of door een medewerker informatie- en archiefbeheer?

- Beschrijf uw afsluitingsproces, inclusief rollen en verantwoordelijkheden.
- Maak een keuze of u binnen de SharePoint-omgeving uw afgesloten zaken wel of niet wilt verplaatsen naar een RMA-achtige omgeving, waar ook andere autorisaties gelden (toegang DIV).
- Als de informatiebeheerprocessen niet goed zijn ingericht, is de kans aanwezig dat informatie gaat zwerven en niet op tijd wordt vernietigd, wat in strijd is met de Archiefwet en de AVG.

Welke functionaliteiten heeft u nodig?

- Vaste toekenning van bewaartermijnen per Team, kanaal of informatieobject, ongeacht de inrichtingskeuzes.
- Bevriezen van informatie, informatie in statische fase brengen, waarbij informatie definitief is en niet meer aangepast kan/mag worden.
- Functie om een dossier als “afgesloten” aan te merken (vinkje of knop of andere optie).
- Vorm van signalering wanneer een dossier al X termijn niet is geopend/aangepast, zodat DIV kan checken of het dossier niet afgesloten had moeten worden en zij dit alsnog kunnen regelen.
- Geautomatiseerde check op compleetheid metadata en documenten.

6.2.6 Apps

In de Teams App Store zijn ruim 700 apps beschikbaar, die toegevoegd kunnen worden aan MS Teams. Voor het informatiebeheerproces is het belangrijk om vooraf te bepalen of deze Apps onderdeel uit mogen maken van of ondersteunend mogen zijn aan een werkproces dat uitgevoerd wordt met MS Teams.

Daarbij is voor informatiebeheer belangrijk om te bepalen welke informatie in deze Apps wordt verwerkt en of u hierbij kunt voldoen aan de eisen voor informatiebeheer. Neem deze apps ook op in uw bewaarbeleid. Een toelichting op een aantal veelgebruikte apps en de plaats waar de informatie wordt bewaard is te vinden in hoofdstuk **Error! Reference source not found.**

Tip

U kunt als organisatie vooraf bepalen welke apps toegevoegd mogen worden. U kunt standaard apps toevoegen aan een Team of de gebruiker laten bepalen op basis van een beperkte lijst.

Zorg ervoor dat bij gebruik van een App de informatie gegenereerd met die App in uw Team wordt opgeslagen en niet in de App zelf of zorg dat u de bron van de App kunt beheren.

Zorg dat u grip houdt op informatie waar u grip op moet houden. Dat kan ook anders dan in Teams zijn. Bijvoorbeeld de posts (chatberichten) worden opgeslagen in Exchange, bij de mail.

6.2.7 Sjablonen

Een Team kan aangemaakt worden op basis van een sjabloon. Binnen MS Teams zijn sjablonen aanwezig voor bijvoorbeeld projectmanagement, eventmanagement en financiële samenwerking. Beheerders kunnen aangepaste sjablonen voor uw organisatie maken. Het voordeel van sjablonen is dat u de basis van bestanden er goed in kunt zetten en alleen de wisselende informatie aan hoeft te passen. Voor het informatiebeheerproces is het belangrijk om vooraf te bepalen of en welke sjablonen gebruikt gaan worden en daarin te zorgen voor een goede inrichting voor zowel de gebruiker als voor informatiebeheer.

Tip

Bij het gebruik van sjablonen kunt u vooraf bepalen welke informatie u in de Team wilt verwerken.

Voeg aan een standaard Team één of meerdere sjablonen toe. Het werkt gemakkelijker voor de gebruiker. Ook geeft dit uniformiteit.

6.2.8 Prullenbak

De Prullenbak bevat een vangnet voor situaties wanneer gebruikers bestanden, versies van bestanden, lijstitems, bibliotheken, lijsten en mappen van een site verwijderen. Wanneer gebruikers een van deze items van een site verwijderen, worden die in de Prullenbak geplaatst.

Als het bestand uit de Prullenbak van de site wordt verwijderd, wordt het verzonden naar de siteverzameling of de tweede Prullenbak, waar een beheerder van de siteverzameling het kan terugzetten of definitief verwijderen.

Voor het informatiebeheerproces is het belangrijk om vooraf te bepalen of een lid van een Team informatie mag verwijderen. Daarnaast is het belangrijk om te bepalen hoelang een item in de prullenbak moet blijven en wat er daarna mee mag gebeuren.

Tip

Bepaal of een gebruiker informatie uit een Team mag verwijderen. En zo ja; bepaal waar de verwijderde informatie heen gaat. Bepaal of deze informatie direct permanent verwijderd mag worden of dat deze nog verzonden wordt naar een siteverzameling.

Advies

Geef de eigenaar van een Team de rechten om informatie te verwijderen. Laat de verwijderde informatie verzenden naar een siteverzameling waar de functioneel beheerder de rechten krijgt om deze terug te plaatsen of definitief te verwijderen.

6.2.9 Metadata

Voor informatiebeheer is het van belang dat gestandaardiseerde metadataschema's binnen de bestaande structuur kunnen worden toegevoegd. Wat betreft de metagegevens is het zo dat attributen in MS365 verschillende namen (labels) en waarden kunnen hebben.

Bij het bepalen van het metadataschema is het belangrijk om rekening te houden met de administratieve last voor de gebruiker. In de praktijk blijkt dat als teveel extra gegevens moeten worden toegevoegd, de gebruiker dit niet of niet nauwkeurig doet. Daarmee daalt de kwaliteit van de registratie en groeit de weerstand tegen het gebruik van Teams. Een goed advies is om zoveel mogelijk de metadata automatisch toe te laten kennen.

Metadata wordt gebruikt voor het bepalen van het bewaarbeleid en de retentieperiode. Ook bij de overbrenging naar het statisch archief zijn deze noodzakelijk. In dat geval is het goed om een mapping te hebben met een metadatamodel als TMLO of MDTO.

Een mapping is er op gericht om overeenstemming te verkrijgen over de betekenis en de waarden van attributen in MS365, waarbij MDTO als spreekwoordelijke vertaalsteen gebruikt kan worden. Bij een uitwisseling (bijvoorbeeld bij migratie of overbrenging) zijn minimaal de verplichte MDTO-attributen aanwezig en voorzien van waarden.

Tip

	Keuze	Risico
Aanmaken nieuw Team	Gebruiker of beheerder	Gebruiker: * Kans op wildgroei * onvoldoende oog voor archivering, privacy, BIO, etc. *Kans op lastig beheer en kwaliteitszorg Beheerder: * Extra werkzaamheden * Vertraging in proces * Kans op olifantenpaadjes zoals gedeelde mappen in OneDrive en bestanden delen in Teams-Chat
	Privé, openbaar of extern kunnen delen	Privé: * Niet zichtbaar voor organisatie Openbaar: * Zichtbaar voor organisatie Extern: * (Onbewust) informatie extern delen
	Naamgeving eigenaar Team/beheerder	Eigenaar: * Kans op wildgroei * Niet overzichtelijk Beheerder: * Extra werkzaamheden * Vertraging in proces
	Advies bij aanmaken nieuw team	Meerdere beheerders, waaronder een of meerdere IM/-DIVERS, gebruik van provisioningtool/Teams templates en leid beheerders op.
Rechten rollen	Eigenaar of lid	Onduidelijkheid over rollen en bijbehorende rechten Eigenaar moet rol overdragen als deze bijvoorbeeld organisatie verlaat. Bij leesrechten kan bijvoorbeeld ook geen tekst gekopieerd worden. Te weinig rechten kan vertraging geven in proces. Te veel rechten kan voor bijvoorbeeld (onbewust) verwijdering van informatie zorgen.
Apps toevoegen	Welke apps mag gebruiker toevoegen?	Er zijn apps goedgekeurd door MS en ook niet goedgekeurde apps kunnen aan een Team worden toegevoegd. Er zijn apps waarbij informatie in die app wordt opgeslagen en niet in de Team komen.

6.2.10 En dan nog dit

Advies

Houd de autorisaties op informatie actueel (verwijzing naar BIO). Pas deze aan wanneer iemand vertrekt of een andere functie krijgt. Zo blijft vertrouwelijke informatie beschermd. Zorg dat de functioneel beheerder kan monitoren op deze wijzigingen.

Vooraf bij gastgebruikers is het belangrijk om in de gaten te houden dat deze nog actief deelnemen, zodat tijdig de toegang kan worden afgesloten als deze niet meer nodig is.

7. Bewaarbeleid

Grip op informatie begint met het formuleren van bewaarbeleid. Zo bepaalt u hoe informatie wordt bewaard. Dat geldt ook voor de informatie die binnen M365 wordt verwerkt. We beschrijven wat u in uw bewaarbeleid zou moeten opnemen en hoe u zorgt dat binnen M365 het beleid wordt kan worden uitgevoerd.

Voor goed informatiebeheer heeft iedere overheidsorganisatie een vastgesteld bewaarbeleid nodig waarin de keuzes omtrent bewaren, vernietigen en bewaaromstandigheden worden vastgelegd.

Dit kan overlap hebben met de M365-functie “Bewaarbeleid”, maar dit hoeft niet zo te zijn. De gegeven opties in dit hoofdstuk zijn beschikbaar met een E3 licentie, wanneer een E5 licentie nodig is staat dit aangegeven.

7.1. Metadata-schema

7.2. Welke metadata is noodzakelijk om uw bewaarbeleid uit te voeren?

Metadata voor duurzame toegankelijkheid worden uitgedrukt in de standaard MDTO. Uitgangspunt is dat de organisatie zelf moet bepalen wat MDTO conform is (minimaal of volledig).^[1] Tevens kan gekozen worden voor TMLO en Records in Context. Hierbij wordt geadviseerd om een mapping te maken waarin beschreven wordt welke waarden gebruikt worden in het gekozen metadataschema en welke in de M365-omgeving.

Maak van tevoren, bij het maken van een organisatiebreed metadataschema, afspraken met de betreffende afdelingen over de toe te voegen metadata en met uw archiefinspecteur, wanneer er sprake is van overdracht naar een e-depot. Maak waar de gekozen metadatastandaard daarin niet voorziet gebruik van aanvullende (gecontroleerde) termensets en keuzelijsten.

M365 zal bij de meeste organisaties worden ingezet voor het ondersteunen van programma's of projecten. Het inrichten van M365 om volledig de conventies van het zaakgericht werken, en dus de informatiemodellen RGBZ en ImZTC, te volgen ligt in deze gevallen minder voor de hand.^[2] Wordt M365 daarentegen (ook) ingezet om primaire processen te ondersteunen, dan is inrichting van M365 volgens deze informatiemodellen het overwegen waard.

In M365 wordt een aantal metadata al standaard toegevoegd:

- Auteur
- Aangemaakt op
- Gewijzigd op
- Aangemaakt door
- Gewijzigd door
- Bestandstype
- Versiegeschiedenis
- Grootte van het document

Bij het verslepen van een document naar Teams wordt de naam ook automatisch meegenomen. Bij het vanuit Teams een document aanmaken, zal de naam door de behandelaar nog moeten worden toegevoegd.

Naast deze standaard set aan metadata biedt M365 nog meerdere metadatavelden die wel of niet aangezet kunnen worden. Denk hierbij aan retentielabels en velden over auteursrecht. Daarnaast is

het mogelijk om zelf metadatavelden toe te voegen en in te richten. Een veld dat niet in M365 zit maar wel wordt aangeraden om aan te maken, is (op dossierniveau) een veld 'einddatum' en een veld 'periode' of 'procestermijn'. Op basis van deze velden kunnen retentielabels toegekend worden, waardoor de bewaartermijn op het juiste moment start. Let bij het aanwijzen van in te vullen metadatavelden op mogelijke overlap tussen velden, zoals 'naam', 'titel' en 'onderwerp' en leg vast welk veld wel of niet wordt gebruikt en waarvoor.

7.3. Waarderen

7.3.1 Uitgangspunten

M365 wordt gebruikt als een informatiebeheersysteem: Informatie in M365 moet beheerd worden. Dit betekent dat een groot deel van de informatie uit de M365-omgeving op den duur vernietigd zal kunnen worden en een deel is permanent te bewaren materiaal.

7.3.2 Archiefwet- en regelgeving

Bij het inrichten van informatiebeheersystemen waarin waardering plaatsvindt, is het van belang om uit te gaan van relevante wet- en regelgeving. Dat zijn in dit geval de Archiefwet, bijbehorend Archiefbesluit en de Archiefverordening, maar ook de (gemeentelijke of provinciale) Selectielijsten en de Hotspotmonitor of passages in specifieke wetten over de bewaartermijn.

Door deze officiële stukken als uitgangspunt te nemen, wordt geborgd dat de juiste, actuele bewaartermijn aan informatie wordt gekoppeld. Let hierbij op dat u de mogelijkheid behoudt bewaartermijnen aan te passen, bijvoorbeeld wanneer er sprake is van een Hotspot of precedentzaak dan wel dat er sprake is van een unieke situatie of gebeurtenis (denk aan iets met koninklijk huis o.i.d.).

Daarnaast stellen de Archiefwet- en regelgeving verschillende eisen aan het vastleggen, zoeken, vernietigen en overbrengen van dossiers en documenten. Zo wilt u bijvoorbeeld uw zaak/dossier kunnen afsluiten, er een bewaartermijn aan kunnen toekennen o.b.v. het resultaat van de afhandeling en de zaak op volledigheid kunnen controleren.

Het toepassen van een Selectielijst is een belangrijke voorwaarde voor vernietigen en bewaren. Ook wanneer M365 niet gebruikt wordt als zaakstelsel maar als samenwerkingsomgeving, dient er rekening gehouden te worden met vernietiging in M365 en correcte migratie naar een archiefsysteem.

Advies

We adviseren om de Archiefwet- en regelgeving en bijbehorende Selectielijsten en Hotspotmonitor mee te nemen bij de inrichting van M365.

7.3.3 Definitie dossier of zaak

Wanneer u uw M365-omgeving à la een zaakstelsel wilt inrichten, is het verstandig om van tevoren te definiëren welk element in M365 wordt aangemerkt als dossier of zaak. Er zijn hierin verschillende keuzes. Zo is het mogelijk om per zaaktype een bibliotheek of subsite in te richten, waaronder verschillende mappen met dossiers gehangen worden. De bibliotheek die als dossier geldt, kan worden ingericht als documentset. Aan deze documentset kan een retentielabel gehangen worden. Het is ook mogelijk om een subsite te maken waarbij u voor ieder proces een hub-subsite (site onder een site) in te richten, waarbij pas op het laatste niveau mappen komen kijken. Op deze manier richt u een site in als zaak.

Tip

Houd er bij de inrichting wel rekening mee dat u op bibliotheek max 5000 uitzonderingen (afwijkende autorisaties) op de autorisatie van de bibliotheek kunt maken.

Advies

We bevelen aan om hubsites en hub-subsites in te richten als zaak (wanneer u M365 zaakgericht wilt inzetten), om zo het overzicht en de eenheid van uw zaak by design in te richten en te bewaken. Hoe u dat doet vindt u hier: <https://support.microsoft.com/nl-nl/office/uw-sharepoint-hubsite-instellen-e2daed64-658c-4462-aeaf-7d1a92eba098>.

7.3.4 Waardering op document-, dossier/zaak- of siteniveau

Veel overheidsorganisaties werken op dit moment met een DMS of zaakstelsel. Dit houdt in dat er respectievelijk op documentniveau informatie opgeslagen wordt of op zaak/dossierniveau. M365 biedt de mogelijkheid om op document-, zaak/dossier- of siteniveau te waarderen. De keuze voor het niveau waarop waardering plaatsvindt, heeft verschillende gevolgen voor uw informatiebeheer en latere archivering. De gemaakte keuzes dienen te worden vastgelegd. Let op dat wordt vastgelegd hoe en wanneer zaken/dossiers/projecten worden afgesloten. Het is aan te bevelen in M365 zichtbaar te maken welke bewaartermijnen aan welke documenten hangen, zodat dit voor alle medewerkers duidelijk is.

7.3.4.1 Waardering op documentniveau

Het waarderen op documentniveau heeft als voordeel dat u heel precies informatieobjecten kunt vernietigen of bewaren. Digitale informatieobjecten die onder de Selectielijsten van voor 2017 vallen, zijn ook op documenttypeniveau gewaardeerd (wanneer de M365-omgeving na 2017 is/wordt ingericht is de kans dat er documenten die onder deze Selectielijst vallen klein). Wanneer in de M365-omgeving informatie komt te staan die onder deze Selectielijsten vallen, is het van belang het systeem zo in te richten dat waardering en selectie op documentniveau wordt gefaciliteerd. Als u oudere informatie niet migreert moet u wel besluiten of u dit voor de toekomst zo wilt inrichten.

Tevens kan het gebeuren dat bepaalde documenten in een zaak langer bewaard moeten worden dan de rest van de zaak. Ook in dit geval is het handig om de optie te hebben deze stukken op documentniveau te kunnen waarderen. Waarderen op documentniveau levert echter ook een zeer lange Vernietigingslijst op. In Purview¹ wordt op itemniveau een Vernietigingslijst gegenereerd, maar dit kan met tools ook op een ander niveau geregeld worden.

7.3.4.2 Waardering op dossier/zaakniveau

De huidige Selectielijst is ingericht op basis van werkprocesgericht en zaakgericht werken. Dit maakt het makkelijk om per zaak of dossier de juiste bewaartermijn te koppelen, wanneer u M365 zaakgericht inricht. Het zorgt ervoor dat alle informatie uit een specifiek proces even lang bewaard blijft en tegelijk wordt vernietigd. Dit verkleint de kans op het onbedoeld achterblijven van documenten in de applicatie na de vernietiging. Zoals hierboven beschreven kan het echter nodig zijn om bepaalde documenten uit een zaak te halen en deze langer te bewaren, bijvoorbeeld bij uitzonderingen op de vernietiging voor stukken van voor de Selectielijst 2017. De inrichting van het systeem op dossier/zaakniveau biedt hier in eerste instantie niet de mogelijkheid toe, maar een combinatie van opties voor waarderen op documentniveau en op dossier/zaakniveau zou dit kunnen faciliteren.

¹ Microsoft Purview is een onderdeel van M365 waarmee de security en compliance wordt ingericht en beheerd.

7.3.4.3 Waardering siteniveau

Twee scenario's: Hele site bewaren vs. vernietigen op site

- Hele site bewaren consequenties:
 - o accepteren dat u te veel bewaart;
 - o zo inrichten dat er zo min mogelijk informatie met verschillende bewaartermijnen op kan komen.
- Vernietigen op site:
 - o via af te sluiten dossiers waar (handmatig?) een label aan gekoppeld wordt door een gebruiker;
 - o achteraf door DIV;
 - o met inzet van AI (op termijn).

Advies

Geadviseerd wordt uw keuze af te stemmen met de archiefdienst.

7.3.4.4 E-mail- en chatwaardering

E-mails en chats dienen ook opgenomen te worden in het bewaarbeleid van een organisatie. Dit kan via de Selectielijst (dus door e-mails en chats toe te voegen aan het inhoudelijk dossier) en eventueel aanvullend met de Capstone methode (alle e-mails in 1 selectie bij elkaar plaatsen). Belangrijk is om vast te leggen welke e-mails en chats bewaard blijven, voor hoelang en waar.

7.3.5 Waardering op basis van verzameldossier of alleen processen

Het kan voorkomen dat er zich een gebeurtenis voordoet, waaronder meerdere processen vallen. Al deze processen hebben hun eigen bewaartermijn. In sommige gevallen kan het dan handig zijn, om een verzameldossier te maken waar al deze processen onder vallen. Zo heeft u alle processen die bij deze gebeurtenis horen bij elkaar. Dit kan bijvoorbeeld op een kanaal of site. Een volgende stap is, om dit verzameldossier als geheel te waarderen en een bewaartermijn te geven. Dit heeft als voordeel dat alles met betrekking tot de gebeurtenis even lang wordt bewaard. Als nadeel heeft het dat in een verzameldossier van de langste bewaartermijn in het dossier uitgegaan dient te worden. Uitgaan van een kortere bewaartermijn leidt immers tot onrechtmatige vervroegde vernietiging. Bij het uitgaan van de langste bewaartermijn kunnen echter ook gegevens, vooral persoonsgegevens, langer bewaard worden dan conform AVG of Selectielijst is toegestaan. Wij bevelen aan uit te gaan van waardering op basis van processen en geen gebruik te maken van verzameldossiers. Maakt u, voor bijvoorbeeld stukken met korte bewaartermijnen, wel gebruik van verzameldossiers, stem dit dan altijd af met de archivaris of archiefinspecteur.

7.3.6 Technische inrichting waardering

Waarderen kan op verschillende manieren:

- Met algemene (sensitivity)labels²: hiermee geeft u vertrouwelijkheid aan en geen bewaartermijnen. Sensitivity labels kunnen gebruikt worden voor het vastleggen van beperkende bepalingen.
- Met retentielabels (gekoppeld aan een labelbeleid) onder Recordbeheer in Purview³
 - o Handmatig door de gebruiker aan documenten of evt. documentsets toe te kennen.
 - o Automatisch toegekend na aanmaak van het item, of na datum laatste wijziging of na een gebeurtenis (einde levensduur, einde contract, enz)

² <https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

³ <https://learn.microsoft.com/nl-nl/purview/purview>

- Op basis van door een beheerder/recordmanager ingestelde parameters (bijv. combinaties van metadatawaarden) die automatisch retentielabels toekennen als aan de parameters wordt voldaan.
- Op basis van ‘trainbare classificaties’: automatisch retentielabels toekennen op basis van herkende patronen nadat het systeem vele (honderden) voorbeelden heeft geleerd.

NB: automatisch toekennen en trainbare classificaties zijn alleen beschikbaar bij E5-licenties. De verschillen tussen de diverse licenties vindt u op de site [van Microsoft](#). Op de site van VNG⁴ kunt u informatie vinden over de juridische en inkoop voorwaarden die VNG met Microsoft heeft afgesproken.

- Met een bewaarbeleid onder *Levenscyclusbeheer van gegevens* in Purview.

In een labelbeleid kunnen retentielabels toegepast worden op diverse locaties in M365: 1 of meer Sharepointsites, 1 of meer M365-groepen, 1 of meer Exchange- e-mailadressen of 1 of meer OneDrive-accounts. Meer informatie over labels en retentie [vindt u hier](#).

Labelbeleid kan Statisch of Adaptief toegepast worden.

Voorbeeld Statisch toepassen: specifieke mailadressen of sitenamen benoemen.

Voorbeeld Adaptief toepassen: kiezen voor e-mailadressen waarbij (in de Azure Active Directory (AAD) *Title = burgemeester Or Title = wethouder*. Bij een wisseling van de wacht worden dan nieuwe collegeleden of een nieuwe burgemeester ook mee ‘opgepikt’. Een ander voorbeeld is dat u gebruik maakt van groepen die in de AAD goed worden bijgehouden. U moet hiervoor weten hoe de AAD is ingericht. Meer weten over de AAD? [Klik hier](#).

Wat u voor retentielabels maakt, hangt mede af van de inrichting die u kiest en welke metadata er beschikbaar zijn.

Voorbeeld: als u een label wilt toekennen op een dossier of site na afsluiten, dan moet u ergens ingericht hebben om wat voor dossiertype/zaaktype/werkproces het gaat en er moet een sluitingsdatum zijn. De sluitingsdatum kan ook met het (handmatig of op basis van bijv. x-tijd na laatste bewerking) zetten van het label toegekend worden.

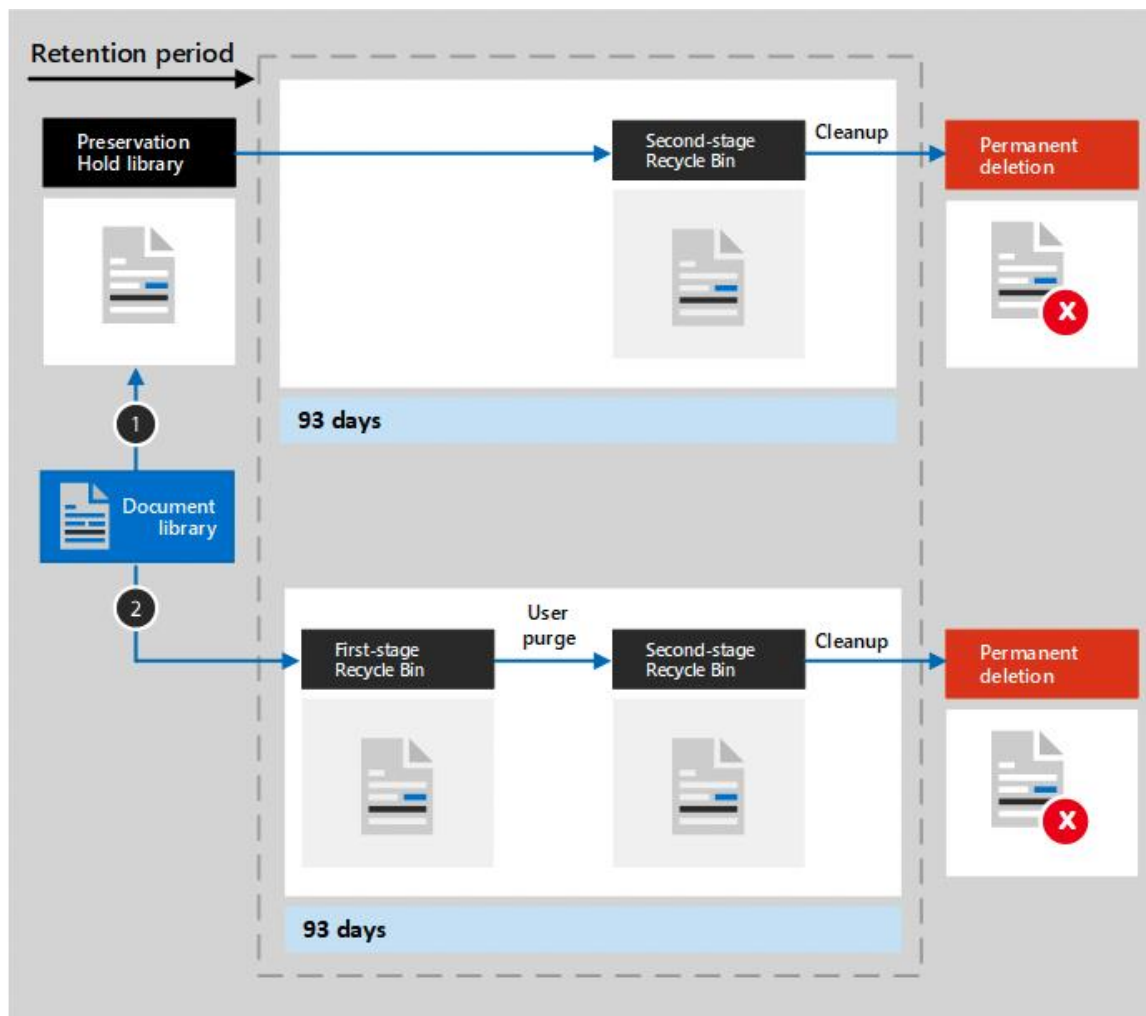
In sommige gevallen worden documenten zonder vernietigingsprocedure vernietigd. Denk aan kladjes of meerdere versies van concepten. Leg voor de organisatie vast welke documenten door gebruikers zelf vernietigd mogen worden en welke documenten via een vernietigingsprocedure worden vernietigd.

Na verloop van de ingestelde termijnen worden de items (ieder document of ander soort item) afhankelijk van de gekozen instelling direct vernietigd, of via een ‘verwijderingsbeoordeling’ in één of meerdere stappen door één of meerdere ‘revisoren’ beoordeeld. Let hierbij op dat directe vernietiging niet altijd mag en dat in veel gevallen een Vernietigingslijst moet worden opgemaakt. Er kan bepaald worden dat een document van vernietiging wordt uitgezonderd. Dit proces dient te worden ingericht.

Dat betekent dat u iets moet regelen om het verwijderen/vernietigen van documenten door gebruikers onmogelijk te maken. Dat kan op meerdere manieren:

⁴ <https://vng.nl/projecten/qt-microsoft>

- Dossiers/documenten met een retentielabel ook een 'record' maken (in te stellen bij uw labels in Purview).
- Alle dossiers/documenten (op geselecteerde locaties) een Preservation Hold meegeven. Een gebruiker kan dan nog wel verwijderen, maar de informatie blijft beschikbaar op de achtergrond.
 - Hier zitten nogal wat haken en ogen aan, want u moet daarna nog bedenken hoe/wie/wat er met die informatie in de Preservation Hold moet gebeuren. Bovendien kost het extra opslag.
 - Zet dit daarom heel bewust in, bijvoorbeeld alleen in bij processen waar de risico's hoog zijn. Hieronder ziet u de Preservation Hold Library in beeld.



7.4. Bepalen bewaartermijn en vernietigingsdatum Retentie (herwaarderen)

Hoe gaat u om met bewaartermijnen en de verschillende berekenwijze om deze te bepalen?

Bij het maken van retentielabels, kunt u bepalen wat er mee moet gebeuren als de retentieperiode voorbij is. Bij automatische vernietiging is er geen signaal waarna u kunt kiezen voor een nieuw label of een nieuwe termijn.

Bij de instelling van een 'verwijderingsbeoordeling' krijgt de beoordelaar (1 of meerdere beoordelaars) altijd nog de gelegenheid om het label aan te passen.

Tussentijds een label aanpassen, bijvoorbeeld omdat informatie onder een hotspot valt, kan ook, maar wel onder voorwaarden:

- Het bestand is geen record (anders moet het eerst de recordstatus ontnomen worden).
- U moet autorisatie hebben.
- Nieuwe labels moeten beschikbaar zijn.

Bij het instellen van uw labels bepaalt u dus mede wat er nog mogelijk is.

Keuzes en risico's

- Afwijken van zaaktype of selectielijst (denk aan langer bewaren i.v.m. bezwaar/beroep/hotspot) of vroegtijdige vernietiging persoonsgegevens uit een stuk (i.v.m. AVG).
- Het kunnen toevoegen van verschillende selectielijsten (stukken van voor 2017 vallen onder selectielijst 2012, stukken van voor 2020 vallen onder selectielijst 2017 etc.).
- Zorg ervoor dat de complete zaak, ongeacht opslaglocatie (let hierbij op verspreide opslag van verschillende zaakonderdelen), wordt vernietigd.

Als u meer wilt lezen [kunt u hier meer informatie vinden](#).

7.5. Classificeren

Classificatie van data is het labelen van informatie met een bepaalde waarde (denk aan persoonlijk, vertrouwelijk of openbaar) om zo te kunnen bepalen welk niveau van bescherming nodig is. Dataclassificatie helpt om na te denken over de beschikbaarheid, integriteit en vertrouwelijkheid van data. Groepen kunnen de beveiligingsgrenzen bepalen. Een groep is een set met termen die gemeenschappelijke beveiligingseisen delen. Daarnaast bestaat de mogelijkheid voor het beheer van termenopslag waarmee een taxonomie kan worden geïmporteerd en beheerd of een metadataschema, zoals TMLO of MDTO. Deze metadata kunnen op verschillende manieren worden toegepast.

Bron: <https://adoptify.nl/blogs/dataclassificatie-voor-gemeenten/>

8. Kwaliteit inrichting

De zorg voor kwaliteit houdt niet op bij een goede inrichting van een Team. Het vraagt om voortdurend monitoren, ondersteunen en sturen van gebruik en zorg voor het goed toegankelijk houden van de informatie. Hiervoor moeten zowel een geschikte organisatie als hulpmiddelen aanwezig zijn. Welke tools zijn hiervoor beschikbaar in M365 en hoe zorgt u dat u die goed kunt gebruiken?

Kwaliteit start bij de inrichting, maar vergt meer dan alleen een goede inrichting. Aan de voorkant dient, zoals eerder aangegeven, goed nagedacht te zijn over de benodigde metadata en de naamconventies voor titels/onderwerpen die nodig zijn voor duurzame toegankelijkheid (zie hoofdstuk 6). Met een goede strategie voor de inrichting wordt de kwaliteit van informatie niet volledig geborgd. De mens blijft van grote invloed op de kwaliteit van informatie. Er dient dus tevens gezorgd te worden voor goede training en adequate ondersteuning voor gebruikers.

8.1. Kwaliteitscontrole via Records Management (Disposition)

Daarmee zijn we er nog niet. Controle, als onderdeel van de alom bekende PDCA-cyclus, door gespecialiseerde vakmensen (DIV) blijft noodzakelijk om de kwaliteit op peil te houden. Voordat informatie, op basis van ingestelde vernietigingstermijnen definitief wordt verwijderd, krijgen reviewers de gelegenheid om de te vernietigen informatie te beoordelen. Hierbij wordt tevens de mogelijkheid geboden om informatie van vernietiging te ontzien. Wie deze vernietigingslijsten mag of kan reviewen kan door administrators worden ingesteld bij Records Management (Disposition). [Meer informatie vindt u hier](#). Reviewers zien alleen de items waarvoor ze een review-autorisatie hebben.

Hiermee wordt echter niet de kwaliteit m.b.t. metadata en de naamconventies afgedekt. Daarvoor zullen deels manuele controles dienen te worden uitgevoerd. Er zijn basaal twee methoden. Ten eerste, u maakt controle integraal onderdeel van het proces en zorgt ervoor dat een proces niet kan worden afgehandeld zonder dat er een controle is uitgevoerd. Dat is omslachtig en arbeidsintensief. De vraag is ook of alle informatie dezelfde aandacht dient te krijgen. Dient informatie met een bewaartermijn van slechts een jaar even zwaar of vaak gecontroleerd te worden als informatie die permanent wordt bewaard? Aangeraden wordt om controles risico-gebaseerd uit te voeren. Hoe hoger het risico des te meer er wordt gecontroleerd.

8.2. Kwaliteitscontrole via eDiscovery tooling

Een tweede methode is [om eDiscovery tooling](#), beschikbaar in Microsoft, in te zetten. eDiscovery biedt de mogelijkheid om informatie te identificeren, bewaren, verzamelen, beoordelen, analyseren en exporteren voor (interne) onderzoeken. Dit is een krachtige manier om informatie te traceren voor Woo-verzoeken, maar kan ook prima ingezet worden voor kwaliteitscontrole. Denk hierbij aan het inrichten van zoekfunctionaliteit voor controles. Voor de uitgebreide mogelijkheden op dit gebied is echter wel een E5 licentie nodig. Het is de moeite waard om te onderzoeken welke mogelijkheden eDiscovery verder kan bieden voor kwaliteitsinrichting en -beheer.

In het kader van de PDCA cyclus is van belang dat managers of procesverantwoordelijken inzicht krijgen in de kwaliteit van registratie en afhandeling van een proces, zodat zij kunnen sturen op verbetering van die kwaliteit indien noodzakelijk. Het reikt te ver voor deze handreiking, maar in dit verband zou ook eens gekeken kunnen worden naar de mogelijkheden van [PowerBI of PowerAutomate](#) op dit gebied.

8.3. Kwaliteitscontrole via Purview logs

Tot slot heeft Microsoft Purview ook audit logs beschikbaar. Deze logs maken het mogelijk om veranderingen in records te traceren. In de logs wordt o.a. bijgehouden wat er is veranderd, door wie, wanneer en vanaf welk apparaat. De logs zijn beschikbaar in de “audit search tool” in Microsoft Purview. De lijst geauditeerde activiteiten in de Microsoft omgeving is zeer lang en omvat alle belangrijke applicaties.

Houd er rekening mee dat audit logs in de Microsoft omgeving een beperkte bewaartermijn hebben. Er is een verschil tussen de verschillende licenties. In de standaard editie worden logs maximaal 90 dagen bewaard. Bij de E5 licentie kan het worden ingesteld tot maximaal 10 jaar.

^[1] <https://www.nationaalarchief.nl/archiveren/mdto/definitie-van-mdto-conform>.

^[2] Zie ook de aanbevelingen voor toepasbaarheid van het Zaakgericht werken voor onder andere projecten op GEMMA Online:

https://www.gemmaonline.nl/index.php/GEMMA_2_Katern_Zaakgericht_Werken#Toepasbaarheid_zaakgericht_werken.

9. Toegankelijkheid

Informatie heeft alleen waarde als het verantwoord gebruikt kan blijven worden. We moeten dus zorgen dat de informatie die in M365 wordt bewaard voldoet aan de eisen voor duurzame toegankelijkheid. Dit hoofdstuk beschrijft de twee kanten hiervan: het openstellen van informatie en het beveiligen van informatie en geeft tips hoe u dit binnen M365 kan regelen.

9.1. Vinden van informatie: Zoekfunctie

Wilt u meer weten? Kijk hier ^[1] <https://learn.microsoft.com/nl-nl/microsoft-365/solutions/collaboration-governance-first?view=o365-worldwide>

9.2. Openstellen van informatie

9.2.1 Beleid

Veel organisaties hebben een *open tenzij*-beleid. De AVG geeft aan wanneer informatie niet gedeeld mag worden. Welke regels er nog voor 'tenzij' gelden is aan iedere organisatie voor zich. Bij het openstellen van TEAMS-ruimtes of sites moet altijd bepaald worden welke informatie op de site gedeeld gaat worden en met wie de informatie gedeeld mag worden.

Een andere insteek van openstellen is het vinden van informatie voor bijvoorbeeld Woo-onderzoeken of interne onderzoeken. Dan wordt informatie gezocht die normaliter wellicht niet allemaal toegankelijk is voor één persoon. Bijvoorbeeld mails van bestuurders. Die informatie kan op verschillende manieren verkregen worden. Bijv. door het aanschrijven van medewerkers die mogelijk informatie hebben op het gebied van een specifieke Woo-vraag, door bepaalde medewerkers (permanent of op aanvraag) extra rechten te geven op verschillende systemen met informatie en/of met de M365-tooling.

Welke methode gekozen wordt, ligt idealiter vast in uw beleid. Evenals de controles die u wilt uitvoeren op het gebruik van deze krachtige tools.

Vindbaarheid van informatie hangt ook samen met de metadata die u toekent aan uw documenten, dossiers, kanalen of sites. Ook een goede naamgeving van alle onderdelen helpt om informatie snel terug te kunnen vinden.

Bedenk van tevoren welke informatie nodig is om stukken terug te kunnen vinden en bepaal daarmee welke metadata u nodig heeft. Uiteraard is het verstandig om daarbij aan te sluiten bij TMLO/MDTO-standaarden voor metadatering. Slechte metadatering betekent verminderde toegankelijkheid.

Verder is het nodig om na te denken over welke tools (apps) u medewerkers wilt geven die het werken makkelijker kunnen maken. Wilt u daar controle over, wilt u daar wel of niet trainingen voor geven, wilt u bepaalde apps alleen aan speciale gebruikers geven? Of wilt u apps gefaseerd beschikbaar stellen: eerst alleen de eenvoudige apps die voor iedereen goed bruikbaar zijn en later misschien ook andere apps?

9.2.2 Mogelijkheden Microsoft365

Open betekent bij M365 niet alleen dat informatie gevonden kan worden door iedereen die in de AAD^[1], maar dat iedereen ook lid kan worden en mee kan doen aan chatgesprekken en documenten kan bewerken. Dit is voor veel mensen een eng idee, ook al kunt u zien wie iets het laatst bewerkt

heeft en -via versiebeheer- ook wat iemand heeft gewijzigd. Het vergt dus aandacht in trainingen/adoptietrajecten.

Voor de autorisatiemogelijkheden voor het beveiligen van informatie verwijzen we naar [paragraaf 4.2](#).

Voor het beantwoorden van WOO-verzoeken heeft M365 een paar krachtige tools in Purview:

- Inhoud zoeken
- E-Discovery (Standard of Premium)

Met beide tools kan gezocht worden in alle informatie binnen bereik van M365, ongeacht bestaande autorisaties. Dus ook in mails, OneDrives en andere normaliter niet beschikbare informatie van alle medewerkers in de organisatie.

Met *Inhoud zoeken* kunt u zoeken in M365-gegevensbronnen en die exporteren naar een lokale computer.

E-Discovery werkt op de basis van *Inhoud zoeken*. U kunt hierin echter ook cases maken en *e-Discovery*-beheerders toewijzen aan specifieke cases. Niet iedereen kan dus bij alle cases. U kunt ook de gevonden resultaten (tijdelijk) behoeden voor verwijderen (*legal hold*). De premiumvariant biedt veel extra mogelijkheden voor werkstromen en analyses.

NB: met een E3-licentie kunt u bij *e-Discovery* alleen standaard zoekopdrachten gebruiken. Met een E3+ of E5-licentie kunt u zelf inhoud analyseren.

Belangrijk is om goed na te denken over wie (welke functies en/of personen) in de organisatie deze tooling mogen gebruiken onder welke voorwaarden. Afstemming met de OR is aan te raden.

Bij de inrichting van M365 kunt u de in het beleid benoemde verplichte dan wel gewenste metadata opnemen in kolommen. Bij het opnemen van kolommen kan er een achterliggende keuzelijst gehangen worden om uniformiteit in invullen af te dwingen. Daarmee legt u een basis voor eventuele dashboards of andere overzichten.

Bij een E3+ of een E5-licentie kunnen in Purview automatische (labeling)acties op basis van in kolommen opgenomen informatie gemaakt worden.

M365 heeft een groot aantal eigen apps en third party apps waar u gebruik van kunt maken. De apps kunt u toegankelijk maken voor iedereen, of bijv. alleen voor functioneel beheerders of alleen voor TEAMS-eigenaren. Uw licentie bepaalt mede welke apps er beschikbaar zijn.

9.2.3 Publiceren vanuit M365

9.2.3.1 Versiebeheer

Onder de Wet open overheid, de Wet hergebruik overheidsinformatie en de Wet op de elektronische publicaties zijn overheden verplicht om bepaalde categorieën informatie actief openbaar te maken. Dit gebeurt door middel van publicatie op het internet - stand van zaken juni 2023. Organisaties dienen de publicatie op het internet zelf te organiseren.

9.2.3.2 Wat gebeurt er bij start nieuwe Sharepoint omgeving of Teamsite

Bij de inrichting van SharePoint is het van belang een koppeling met PLOOI in te richten. Daarbij is het ook noodzakelijk om bepaalde vormen van anonimiseringsfunctionaliteiten van tevoren in te richten, zodat persoonsgegevens niet onnodig en disproportioneel worden verwerkt. Tevens dient rekening gehouden te worden met versiebeheer, zodat de juiste, niet geanonimiseerde versie van

een permanent te bewaren document overgebracht kan worden naar het e-depot en de geanonimiseerde versie gepubliceerd wordt.

Keuzes en risico's

- Bepaal welke informatie openbaar gemaakt moet worden.
- Richt uw proces zo in dat actief openbaar te maken informatie ook daadwerkelijk actief openbaar wordt gemaakt.
- Houd zicht op welke informatie in uw systeem onder de AVG valt en welke informatie wel en niet openbaar gepubliceerd mag worden onder de AVG.
- Zorg ervoor dat versiebeheer op orde is, zodat de juiste documenten gepubliceerd en bewaard worden. Houd rekening met het vernietigen van duplicaten en downloads (bijvoorbeeld op netwerkschijven en in overige tools).

Functionaliteiten

- Richt een functionaliteit voor publicatie in. Waarmee ook gekozen kan worden wat binnen een zaak gepubliceerd kan worden.
- Een anonimiseringsstool die het mogelijk maakt geanonimiseerde versies te maken. Dit is dan wel buiten M365 om.

Advies

Richt een proces in waarbij publicatie wordt ingericht en gefaciliteerd, zodat aan de Archiefwet- en regelgeving voldaan kan worden.

9.3. Beveiligen van informatie

9.3.1 Beleid

Voor het beveiligen van informatie die niet openbaar is, zijn er verschillende middelen.

- Beveiliging tegen kwade bedoelingen van buiten (informatiebeveiliging).
- Beveiliging om vertrouwelijke gegevens vertrouwelijk te houden (informatieveiligheid).

De BIO geeft met dataclassificatie handvatten om de informatie in te delen naar beveiligingsklassen en daar uw beveiliging op af te stemmen.

Daarnaast heeft u intern vaak een autorisatiebeleid, algemeen en toegespitst op specifieke applicaties. Door de andere inrichting en mogelijkheden van M365 moet het autorisatiebeleid wellicht aangepast worden.

Dit stuk gaat over *toegankelijkheid*. Om de toegankelijkheid van informatie te bepalen moet u weten welke informatie u heeft en wat u daar mee wilt; wat mag er met de informatie. Wat mag intern, wat mag extern en wie mag wat. Microsoft noemt de stappen:

- Ontdekken, bijvoorbeeld via patroondetectie.
- Classificeren, het labelen van informatie (sensitivitylabels of retentielabels).
- Beschermen, het bepalen wat met de gelabelde informatie gedaan mag/moet worden.
- Monitoren, rapporteren op afwijkingen.

Alvorens te starten met de ingebouwde mogelijkheden die bij elk van deze aspecten worden aangeboden moet een organisatie de volgende vragen in overweging nemen:

- Welke regelgeving en compliance factoren zijn van belang?
- Zijn mijn gegevens verspreid over apparaten, de cloud en on-premises servers?
- Zijn mijn gegevens geografisch verspreid?
- Zijn bepaalde medewerkers of groepen relevanter voor discovery?
- Ken ik de kenmerken van gevoelige of belangrijke gegevens?

Microsoft365 biedt mogelijkheden die er eerst niet waren, bijvoorbeeld:

- het onmogelijk maken van het via mail versturen van informatie met vertrouwelijke informatie (bijv. een lijst met BSN's) of werknemers alleen waarschuwen;
- toegang tot uw informatie afsluiten voor inlogpogingen vanuit bepaalde geografische locaties.

Wat u wilt op dit gebied: streng zijn of (nog) niet, moet vooraf vastgesteld worden en kan later worden bijgesteld op basis van ervaring. Via centrale instellingen in de tenant kan dit vrij eenvoudig geregeld worden.

9.3.2 Mogelijkheden van M365

Microsoft365 biedt verschillende niveaus van informatie: het item (document of anders), een map of documentset (dossier), kanalen, bibliotheken en Teams.

Toegang tot de items wordt verleend aan personen die opgenomen zijn in de Azure Active Directory (AAD), waar wordt vastgelegd wie ze zijn en welke rol ze hebben (bijv. interne medewerker of Gast-van buiten).

Aan een TEAMS-ruimte zitten gebruikers gekoppeld. Ieder TEAM heeft minimaal twee eigenaren die het beheer voeren en extra mogelijkheden hebben. Zij voegen o.a. leden toe aan een TEAM.

Een *Public*-TEAM is toegankelijk voor iedereen. Mensen die een document hebben gevonden van een public TEAM worden automatisch lid van dat TEAM en kunnen dan ook mee chatten of documenten bewerken. Alleen TEAMS waar u lid van bent ziet u in het overzicht in de linkerkolom.

Een *Private* TEAM is alleen toegankelijk voor leden van dat TEAM. Dat kunnen zowel interne medewerkers als externen zijn.

In een TEAMS-ruimte kan gewerkt worden met kanalen. Voor kanalen zijn er drie opties voor toegankelijkheid:

- Alle leden van het TEAM zijn lid van het kanaal (standaard bij kanaal Algemeen).
- Een kanaal is Private: alleen een deel van de leden van het TEAM zijn lid van het kanaal.
- Een kanaal is Shared: leden van dit kanaal kunnen lid zijn van het TEAM of leden van buiten het TEAM en zelfs leden van andere organisaties die M365 gebruiken. Belangrijk bij Shared Channels met externe partijen is om eerst te bepalen wie de archiefvormende organisatie is. Die richt het Shared Channel in.

Bij private kanalen en shared kanalen geldt dat deze niet zichtbaar zijn voor TEAMS-leden die geen lid van het betreffende kanaal zijn. Ook krijgen private en shared kanalen eigen achterliggende Sharepointpagina's en nemen ze (dus) niet een eventuele inrichting van de TEAMS-ruimte over.

Werkt u met externen, richt dan een proces in om periodiek te checken of deze nog toegang moeten hebben tot de locaties.

Het volgende niveau is het dossierniveau. Hier kunt u kiezen voor het gebruiken van mappen of van documentsets. Deze nemen de autorisatie van het kanaal over. U kunt een map of documentset nog

wel delen met extra personen buiten de kanaalleden en daarbij bepalen wat deze personen mogen (lezen, bewerken, delen). U deelt altijd een koppeling naar het dossier.

Een aparte autorisatie zetten op een dossier, zodat ook eigen kanaalleden er niet meer bij kunnen, is alleen mogelijk via een beheerder. Dat is niet fijn in het gebruik en levert veel beheer op, maar het beschermt ook tegen ongebreidelde ontoegankelijke stukken.

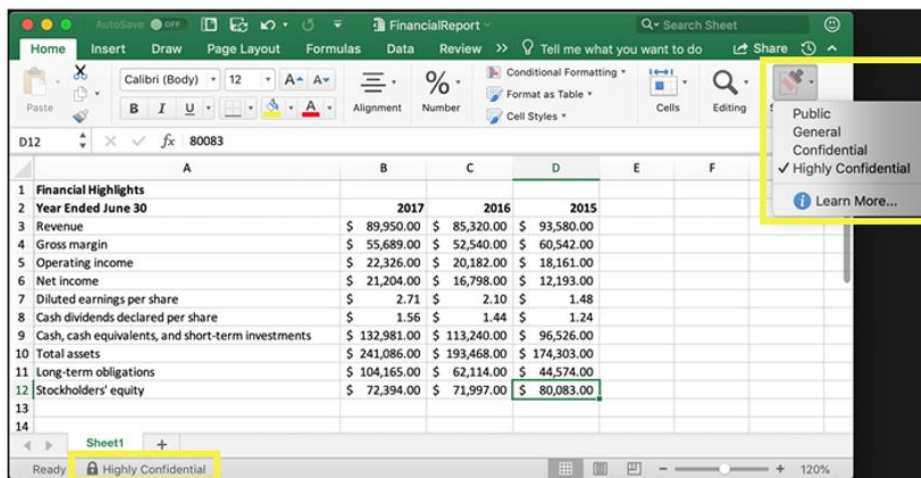
Voor het documentniveau geldt hetzelfde als voor het dossierniveau.

Wel kunt u aan documenten ook een sensitivity/vertrouwelijkheidslabel meegeven en voor de labels bepalen wat er wel of niet mee mag of moet gebeuren. Bijvoorbeeld wel of niet extern delen, encryptie toepassen of een watermerk toevoegen.

Een vertrouwelijkheidslabel kan handmatig toegekend worden door een gebruiker (rechtstreeks in Word) of automatisch op basis van inhoud, bij. BSN-nummers.



Figuur 1 knop in Word



Figuur 2 knop in Excel

Welke vertrouwelijkheidslabels er beschikbaar zijn voor een medewerker, is door een organisatie zelf te bepalen en in te richten in Purview.

Daarnaast kan informatie verder worden beschermd op Windows-devices middels Microsoft Intune Endpoint Manager, bijv. het blokkeren van het kopiëren of uploaden van een bestand. Wilt u meer weten [of MS Intune Endpoint Manager dan vindt u dat hier.](#)

Ook kan er met third-party apps gekoppeld worden, op dit moment (juni 2023) enkel voor Windows, Mac en Linux (mobiele devices volgen later).

9.3.3 Vindbaarheid

Informatie vinden in Microsoft365 kan relatief eenvoudig via de centrale zoekbalk. U kunt uw resultaten filteren op informatie in berichten (chats), over personen en in bestanden. Standaard krijgt u een overzicht van alles (berichten, personen, bestanden) gerelateerd aan uw zoekvraag, met een aantal per soort uitgelicht. Hoe specifieker u zoekt, hoe beter het resultaat.

U krijgt alleen die informatie te zien, waar u volgens uw autorisatie al toegang tot hebt.

U kunt ook meteen zien in welk TEAM en in welk kanaal iets gevonden is. U kunt niet meteen zien in welk dossier (map of documentset) een document zit. Wilt u dat wel, dan opent u een document en via de URL-balk kunt u dan zien in welk dossier een document zit.

U kunt niet zoeken op *dossiertitels*.

Via [Delve](#) krijgt u een ander soort overzicht van voor uw beschikbare informatie. In Delve ziet u verschillende inhoud uit heel M365. U ziet uw eigen documenten en documenten waaraan uw collega's werken. Dit zijn documenten die zijn opgeslagen in OneDrive voor werk of school of SharePoint in M365, of die met u zijn gedeeld als bijlagen in e-mailberichten. Onder *Start* informatie die wellicht voor u interessant is. Onder *Ik* uw profieltekst, documenten waar u recent aan heeft gewerkt, personen waar u veel mee samenwerkt en de documenten waar zij aan werken. U kunt ook *Favorieten* instellen en via die route informatie snel vinden.

Naast de zoekbalk en Delve kunt u natuurlijk altijd hiërarchisch zoeken: u weet op welke site u moet zijn, in welk kanaal en misschien ook in welk dossier. Om dit soort zoeken zo makkelijk mogelijk te maken is het aan te raden om aandacht te besteden (training, controle) aan juiste naamgeving van sites, kanalen, dossiers en documenten.

9.4. Toegankelijkheid op termijn

Microsoft365 is een product met een snelle ontwikkeling. Dingen die nu nog niet mogelijk zijn op het gebied van recordsmanagement zijn binnenkort of op termijn misschien wel mogelijk. Andersom kan ook: mogelijkheden kunnen verdwijnen of op een heel andere manier opgelost worden. Het record centre uit Sharepoint bijv. wordt niet meer ondersteund.

Het is daarom ook niet vreemd om bij langdurig te bewaren stukken te kiezen voor opslag in een gecertificeerd RMA of direct in een e-Depot.

Het Powerplatform van Microsoft biedt voor leveranciers mogelijkheden om tools te ontwikkelen om een koppeling te maken. Microsoft Power Platform is een reeks softwaretoepassingen voor business intelligence, app-ontwikkeling en app-connectiviteit. Microsoft heeft de Power Fx low-code programmeertaal ontwikkeld voor het uitdrukken van logica op het Power Platform. Het biedt ook integraties met GitHub en TEAMS.

Zo ver wij weten zijn er (waarschijnlijk) geen API's of werkende ZDMS-koppelingen

[\[1\]](#) Azure Active Directory

[\[1\]](#) DUTO-eisen

10. De functionaliteit van M365

Wat is nu eigenlijk M365, welke onderdelen zitten daarin en hoe verhouden ze zich met Teams. Waar staat de informatie van al die onderdelen en welke tooling is er om deze informatie ook duurzaam toegankelijk te beheren en tijdig te vernietigen?

Hoe werkt het en ook hoe richten we het in voor de functies die we nodig hebben?

10.1. Mogelijkheden voor workflows

Op basis van metadata kunnen er workflows worden ingericht. Bijvoorbeeld, iemand zet een document op status definitief. Een manager of DIV/IM-er krijgt een seintje om dit goed te keuren. Hiervoor is het nodig dat u rollen definieert in SharePoint.

10.2. Functionaliteit voor vernietigen: hoe doen we dat?

- In bulk kunnen vernietigen (zo weinig mogelijk handmatig werk).
- Het kunnen maken en uitdraaien van een vernietigingslijst.
- Voldoende metadata kunnen toevoegen die verplicht zijn voor op vernietigingslijst
- Verklaring van vernietiging.
- Geen back-up meer beschikbaar (vernietigd is ook echt vernietigd, niet alleen verwijderd).

10.3. Functionaliteit voor overbrengen

- Exportmogelijkheden: denk ook aan de mogelijkheid tot het inrichten van een API of uitwisselingsstandaard.
- Stel met uw archiefdienst de exportvereisten op en laat deze overeenstemmen met de importvereisten voor een e-depot.
- Bij migratie moet inzichtelijk worden gemaakt wat er is geëxporteerd voor de migratieverklaring.

We beseffen dat bovenstaande onderwerpen niet volledig uitgediept zijn. Dat geldt ook voor een aantal andere onderwerpen die wel op de planning stonden maar niet of niet volledig uitgediept zijn. Mocht u toevoegingen hebben, laat dit dan gerust weten via gripopinformatie@vng.nl.

11. Gebruikers (Adoptie en gebruik)

Voor de inrichting van MS365 is het nodig om een aantal zaken goed op orde te krijgen. Het werkt optimaal als er een aantal stappen genomen worden. Dan gaat het over het meenemen van een organisatie in het werken met TEAMS, het maken van afspraken over het werken met TEAMS, afspraken over het opslaan van documenten en de manier waarop het beheer ingericht wordt.

De focus van dit document ligt op inrichten van een optimale MS365omgeving voor de gebruikers van TEAMS (en SharePoint) is waarbij we de gemeentelijke organisatie op weg helpen om daarin keuzes te maken en stappen te zetten.

11.1. Kleine, middelgrote of grote gemeentelijke organisatie, maakt dat uit?

Voor het inrichten van de mogelijkheden voor de gebruikers maakt het eigenlijk niet uit of we naar een kleine, middelgrote of grote gemeente kijken.

Op het gebied van beheer is het daarbij van belang dat er iemand meekijkt in de 'achterkant' of er geen kanalen ontstaan met bijvoorbeeld maar één eigenaar; dat is onwenselijk in het kader van beschikbaarheid en continuïteit van dat specifieke kanaal.

11.2. Inrichten van rechten binnen de MS365 - E5 omgeving

Voor het toebedelen van rechten binnen de MS365 omgeving moeten er via het Microsoft Purview portaal rechten en compliancy instellingen gedaan worden. Daar worden de rechten van de gebruikers ingericht. Om die instellingen te kunnen doen heeft u beheerrechten voor de MS365 omgeving nodig. Zoek dus degene binnen ICT op die die rechten heeft en trek samen op om de rechten te bepalen voor uw organisatie. De CISO en mogelijk ook de Enterprise (informatie) architect hebben ook een belangrijke adviesrol. Stem de gemaakte keuzes ook af met de Concern Controller en leg de keuzes vast.

De afwegingen die daar door een gemeenten bij gemaakt moeten worden zijn bijvoorbeeld:

- Krijgt iedereen dezelfde rechten (en indien dat niet zo is wie beslist daarover?)?
- Kanalen aanmaken en verwijderen (kan iedereen dat?)?
- Enz.

11.3. Gebruikers binnen de M365 – E5 omgeving

Binnen de E5 licentie van M365 mag iedere gebruiker de MS365 officeapplicatie op maximaal 5 devices downloaden. Dat betekent dat een medewerker dat ook kan downloaden op zijn/haar eigen device; bijvoorbeeld een thuiswerkplek. Het grote voordeel is dat de documenten die dan aangemaakt worden meteen in de netwerkomgeving van de gemeente zelf gezet worden én dat ze niet meer beschikbaar zijn op het moment dat een account geblokkeerd wordt.

11.3.1 Alle verandering is moeilijk ...

De adaptatie; het leren werken met een applicatie zoals TEAMS (die zoveel mogelijkheden biedt) is voor sommige medewerkers beangstigend. De angst zit er dan vaak vooral in dat u iets weggooit dat niet gemoeten had, iets niet meer kan vinden en dat u handigheid moet krijgen met de manier van werken.

Het is nodig om uit te leggen dat u een document altijd kunt terughalen via de prullenbak van SharePoint (*na 90 dagen is het daaruit pas echt weg*) en dat u altijd documenten gemakkelijk kunt

vinden via de zoekbalk. Mocht u de functie prullenbak niet hebben dan heeft een beheerder een prullenbak die nog langer bewaard wordt waar u documenten uit kunt halen. Ook het werken met maar één versie is nieuw en moet u uitleggen aan gebruikers (*hoe kunnen gebruikers vorige versies vinden*).

11.3.2 Training en een Vragen en Tips kanaal

De adaptatie van TEAMS is vooral afhankelijk van de digitale vaardigheden van de medewerkers die binnen de gemeentelijke organisatie werken. Het is nodig om daar een beeld van te krijgen.

Verder moet u medewerkers training geven in het werken met Teams waarbij het aan te raden is om een beginners en een gevorderden variant aan te bieden.

U kunt ook (onder het hoofdkanaal) een subkanaal inrichten waar de vragen over TEAMS gesteld kunnen worden waarbij de beantwoording dan gedaan wordt door iemand die er handig(er) mee is.

Er kunnen daar ook tips uitgewisseld worden en iedereen kan meelesen en ziet dat anderen ook niet alles in een keer snappen. Dat help mee aan de adaptatie van dit onderdeel van MS365.

11.3.3 Beheer van documenten in verschillende MS365 producten

Binnen de M365 omgeving zijn er vele producten waarin gebruikers (automatisch) toegevoegd zijn wanneer ze een E5 account krijgen. Het is belangrijk om goede werkafspraken te maken over de manier waarop de bestanden in een MS365 applicatie zoals TEAMS en SharePoint worden opgeslagen. In de basis gelden die afspraken voor alle MS365 applicaties.

11.3.4 Maak werkafspraken voor samenwerken in TEAMS

Het is nodig om de medewerkers uit te leggen dat ze in TEAMS moeten zijn - om samen te werken.

Dezelfde mappenstructuur ontstaat dan ook in SharePoint.

Een voorbeeld van een set afspraken met betrekking tot TEAMS kan zijn:

1. Microsoft TEAMS gebruiken we om (digitaal) te **vergaderen, samen te werken en te communiceren**.
2. We maken er een gewoonte van om TEAMS **dagelijks te raadplegen** (ongelezen items zijn dikgedrukt). Net zoals we gewend zijn met onze e-mail.
3. Ieder Team heeft minimaal **twee Teameigenaren** die bovendien in dienst zijn bij de gemeente. Zij zijn zorgvuldig met het toelaten van gasten tot de omgeving.
4. **Kanalen** worden aangemaakt door de Teameigenaren. Om het overzicht te behouden maken de teameigenaren alleen kanalen aan die zijn bedoeld voor (hoofd)onderwerpen waar binnen het Team over gecommuniceerd moet worden.
5. De Teameigenaren maken in de kanalen een **overzichtelijke mappenstructuur** aan. Zo zorgen Teameigenaren voor een passende en heldere structuur in de documenten. Eigenaren maken met het Team afspraken over het aanbrenge van wijzigingen in de mappenstructuur.
6. Om in een document samen te werken wordt **één document** aangemaakt binnen de mappenstructuur waarin anderen kunnen meewerken. U mailt geen documenten meer naar anderen – alleen koppelingen;
7. **Posts** worden binnen een kanaal gebruikt om onderling te communiceren over het onderwerp van dat kanaal. Dit scheelt e-mailverkeer en zo houden we binnen onze Teams de communicatie overzichtelijk en veilig bij elkaar;

8. We gebruiken de **tag-functie** (door middel van het @) in posts bij belangrijke berichten waar we personen binnen het Team of het gehele Team op willen attenderen. Door de tag-functie te gebruiken krijgen zij een notificatie van het bericht;
9. Wanneer een project of programma afgelopen is, zijn de Teameigenaren verantwoordelijk om de mappen op te schonen en **alle relevante stukken op te slaan in het Zaaksysteem**;
10. Nadat alle relevante stukken zijn geborgd wordt het Team door de Teameigenaren **gearchiveerd**.

Het is nodig om over de bovenstaande werkwijze binnen de organisatie draagvlak te krijgen.

11.3.5 Gebruik van TEAMS is geen technisch feestje

U maakt een kanaal aan in TEAMS om samen te werken op een onderwerp.

Dat kan de afdeling zijn, het team, een sub-team of een Project of Programma.

11.3.5.1 Naamgevingsconventies volgen

U geeft dat kanaal een herkenbare naam die voldoet aan de ICT naamgevingsconventie die daarover afgesproken is – zo houden we het herkenbaar. TIP: heeft uw organisatie nog geen naamgevingsconventie spreek deze dan af.

U kunt er ook voor kiezen om Projecten laten beginnen met PRJ en Programma's met PGM.

11.3.5.2 Teameigenaren en lidmaatschap van een team

Een kanaal heeft altijd twee eigenaren die beheren wie er binnen dat kanaal toegang hebben.

Het is (technisch) mogelijk om iedereen automatisch aan het hoofdkanaal toe te voegen.

Het is niet mogelijk om automatisch gebruikers toe te voegen aan de diverse kanalen die ontstaan. Daarvoor is de teameigenaar dan weer verantwoordelijk. Mensen die al in het kanaal zitten kunnen wel leden voorstellen – dat verzoek gaat dan naar de teameigenaar die daarover beslist.

11.3.5.3 Beheer van het hoofdkanaal

Het is aan te raden om het veranderen van items in het hoofdkanaal tot een kleine groep te beperken. Het hoofdkanaal kent een aantal subkanalen die voor iedereen in de organisatie relevant zijn.

U kunt denken aan:

- Algemeen (die is standaard bij ieder kanaal)
- Intern Nieuws
- Storingen (IT)
- Vragen en tips over Teams

Het is technisch mogelijk om een koppeling te maken tussen een kanaal en (major) meldingen in het meldingenbeheersysteem (zoals bijvoorbeeld TOPdesk). Dan kunt u medewerkers actief informeren en te communiceren over een verstoring in de IT die gaande is en medewerkers kunnen dan via een link direct naar deze call in het meldingenbeheersysteem om aan te geven of en dat ze er ook last van hebben.

Bijlage 1. Voorbeeld van een gemeente Hilversum (CONCEPT)

Digitaal werken 2.0

We zijn al jaren op de PC aan het werk en maken veel documenten in voorbereiding tot bestuurlijke besluitvorming, besluitvorming voor inwoners, bedrijven en ketenpartners en adviezen voor de diverse partijen waarmee we werken en samenwerken. Daarbij is de rol van de afdelingen Publiekszaken, Leefomgeving en Sociaal Plein een iets andere dan die van Directie, Griffie, Interne Advisering en Interne Dienstverlening. De eerste drie maken ook veel documenten rechtstreeks in de vakapplicatie en die documenten worden daar meteen vastgelegd. De overige afdelingen werken vaak op een andere manier samen aan stukken. Dat kunnen we met Teams/SharePoint efficiënter, effectiever en veiliger. We gaan dus op een 2.0 manier samenwerken!

Om digitaal werken optimaal te laten werken moeten we afspraken maken en richtlijnen toepassen – die we in dit document beschrijven:

1. We stellen richtlijnen vast om ervoor te zorgen dat we de digitale informatiehuishouding op orde krijgen.
2. We maken afspraken voor digitale samenwerking zodat we veilig, efficiënt en effectief kunnen werken.

Eindbeeld

Het eindbeeld is dat de B: schijf op den duur verdwijnt en alle documenten - die door medewerkers gemaakt worden en die voorheen op de B: schijf opgeslagen werden – in de mappen in de Microsoft omgeving (Teams/SharePoint) komen.

We werken via Teams samen en beheren de documenten gemakkelijk via SharePoint.

We werken aan projecten (PRJ) of binnen programma's (PGM) en vanaf het begin van een project de relevante documenten in het zaakstelsel Case of een andere (archiefwaaardige/gekoppelde) vak applicatie opgeslagen.

Richtlijnen digitale informatiehuishouding (wat)

Richtlijnen geven houvast hoe we samen omgaan met informatie van de gemeente Hilversum.

Het doel van het werken met deze richtlijnen is een digitale informatiehuishouding waarin informatie van de gemeente Hilversum altijd en overal beschikbaar, actueel en snel vindbaar is.

- ✓ U bent zelf verantwoordelijk.
- ✓ U werkt 100% digitaal.
- ✓ U kunt altijd en overal bij jouw eigen data.
- ✓ We slaan documenten op één plek op en werken er samen in.
- ✓ Definitieve en relevante documenten slaat u op in het zaakstelsel of een andere (archiefwaaardige) vak applicatie.
- ✓ Documenten zijn open tenzij...
- ✓ We zijn compliant met de geldende wetgeving.

Afspraken digitaal samenwerken (hoe)

1. We helpen elkaar om handig(er) te worden in Teams/SharePoint.
2. Zaakstelsel **Case** blijft ons officiële archief.

3. U werkt samen in **Teams** aan documenten.
4. U gebruikt **SharePoint** om documenten te structureren.
5. U zorgt voor een heldere structuur in de documenten (mappenstructuur).
6. U maakt één document en laat de anderen daarin meewerken, u mailt geen documenten meer naar anderen - alleen nog koppelingen.
7. U **labelt** documenten en – waar nodig voegt u gradaties van **vertrouwelijkheid** van de documenten toe.
8. Wanneer een project of programma afgelopen is, is de teameigenaar verantwoordelijk om de mappen op te schonen en alle relevante stukken op te slaan in het zaaksysteem.
9. Ieder team heeft ten minste twee eigenaren die bovendien in dienst zijn bij de gemeenten; zij zijn zorgvuldig met het toelaten van gasten tot de omgeving.
10. Er is van iedere team/project/programma ook een **informatie SharePoint pagina** die door de teameigenaar bijgehouden en onderhouden wordt.

Goed samenwerken in Microsoft Teams; welke afspraken kunt u maken?

1. Microsoft Teams gebruiken we om (digitaal) te **vergaderen, samen te werken en te communiceren**.
2. We maken er een gewoonte van om Teams **dagelijks te raadplegen** (ongelezen items zijn dikgedrukt). Net zoals we gewend zijn met onze e-mail.
3. Ieder Team heeft minimaal **twee Teameigenaren** die bovendien in dienst zijn bij de gemeente. Zij zijn zorgvuldig met het toelaten van gasten tot de omgeving.
4. **Kanalen** worden aangemaakt door de Teameigenaren. Om het overzicht te behouden maken de teameigenaren alleen kanalen aan die zijn bedoeld voor (hoofd)onderwerpen waar binnen het Team over gecommuniceerd moet worden.
5. De Teameigenaren maken in de kanalen een **overzichtelijke mappenstructuur** aan. Zo zorgen Teameigenaren voor een passende en heldere structuur in de documenten. Eigenaren maken met het Team afspraken over het aanbrenge van wijzigingen in de mappenstructuur.
6. Om in een document samen te werken wordt **één document** aangemaakt binnen de mappenstructuur waarin anderen kunnen meewerken. U mailt geen documenten meer naar anderen – alleen koppelingen.
7. **Posts** worden binnen een kanaal gebruikt om onderling te communiceren over het onderwerp van dat kanaal. Dit scheelt e-mailverkeer en zo houden we binnen onze Teams de communicatie overzichtelijk en veilig bij elkaar.
8. We gebruiken de **tag-functie** (door middel van het @) in posts bij belangrijke berichten waar we personen binnen het Team of het gehele Team op willen attenderen. Door de tag-functie te gebruiken krijgen zij een notificatie van het bericht.
9. Wanneer een project of programma afgelopen is, zijn de Teameigenaren verantwoordelijk om de mappen op te schonen en **alle relevante stukken op te slaan in het zaaksysteem**.
10. Nadat alle relevante stukken zijn geborgd wordt het Team door de Teameigenaren **gearchiveerd**.



Deel een

Je werk productief doen

Je hebt binnen de omgeving van Microsoft Office 365 toegang tot programma's en tools die jouw werk ondersteunen.

Daarnaast heb je toegang tot applicaties via de browser. Daarmee kun je altijd en overal werken en vooral samenwerken.

Samenwerken

Op slaan en samenwerken

- Maak met je team afspraken over waar je aan bestanden **samenwerkt**.
- Je bent **zelf verantwoordelijk** voor het **éénmalig en digitaal opslaan** van bestanden die je maakt of verwerkte.
- Pas de richtlijn **'open tenzij'** toe wanneer je een openbare groep aanmaakt.
- Alle bestanden met een **historisch, juridisch of financieel** belang sla je op in **Case**.

Beschermd Communiceren

Je krijgt in je werk soms te maken met (persoons) gegevens die extra beschermd moeten worden.

- E-mail** is beschermd door encryptie op de mailservers en daarmee is alle inkomende en uitgaande mail versleuteld.
- Chatten** doe je via Teams.
- Videobellen** doe je via Teams*

*Soms moet je in Zoom meedoen; dan log je in met je eigen account buiten de Hilversum omgeving (Mware / Citrix)

Chatten over werk kan binnen kanalen of in de chatfunctie van Teams.

Het is niet nodig om samen achter één computer te gaan zitten of bestanden heen en weer te sturen. Iedereen kan dezelfde kopie van het document bewerken, zelfs in realtime.

In realtime samenwerken

Schrijf samen met anderen aan documenten en bekijk hun wijzigingen terwijl ze die maken.

Opslaan in de cloud

Door bestanden in de MS 365 omgeving op te slaan, heb je er overal toegang toe en kun je ze gemakkelijk delen met het team.

Delen

Nodig anderen via slechts één klik uit om de document te bewerken of te bekijken.

Ideeën vermelden of lezen

Houd automatisch wijzigingen bij en je deelt ideeën met behulp van opmerkingen. Iedereen kan bijdragen aan de conversatie en op de hoogte blijven van wijzigingen.

Deel twee



Deel drie



Bijlage 2. RASCI tabel Werken met TEAMS

Onderstaande tabel moet worden uitgewerkt als een RASCI tabel en verder worden aangevuld.

Rollen en verantwoordelijkheden bij het gebruik en beheer van TEAMS

Teamlid

- Slaat informatie op de juiste plaats en in de juiste structuur conform de afspraken binnen de organisatie op.
- Slaat informatie in TEAMS in de juiste structuur, met de juiste metadata en een heldere naamgeving op zodat anderen het gemakkelijk kunnen terugvinden en interpreteren.
- Zorgt dat bij behandeling in een ander (zaak- of proces-) systeem de benodigde informatie wordt meegegeven. Het vermelden van een gerelateerd zaaknummer in Teams helpt om beter integraal te beheren.

Teameigenaar

- vraagt een team aan;
- structureert de informatie m.b.v. kanalen en mappen;
- bewaakt dat teamleden informatie op de juiste plaats gestructureerd opslaan voorzien van metadata en een heldere naam;
- sluit een kanaal of team in Teams tijdig;
- past de teamleden aan bij wijzigingen in de Teamsamenstelling. Dit geldt ook voor het eigenaarschap;

Recordmanager/adviseur informatiebeheer

- richt het beheerregime in voor elk van de verschillende soorten informatie;
- beoordeelt een aanvraag voor een nieuw team o.b.v. archiefkaders;
- begeleidt medewerkers in het juiste gebruik van Teams met betrekking tot archiefbeheer;
- heeft rechten om in Teams te zoeken (afdeling, project, samenwerking);
- toetst of de informatie op de juiste plaats en in de juiste structuur met de juiste metadata is opgeslagen;
- bewaakt of informatie in een (ook afgesloten of verwijderd) team correct gearchiveerd is;
- zorgt voor tijdige vernietiging of overbrenging van informatie.

Functioneel beheerder

- beoordeelt een aanvraag voor een nieuw team o.b.v. I&A kaders;
- past de teamleden aan bij wijzigingen in de samenstelling van een afdeling (bij in-, door- en uitstroom van medewerkers). Dit kan geautomatiseerd worden ingericht. Een jaarlijkse controle op de juistheid van de autorisaties blijft noodzakelijk;
- is back-up voor het aanpassen van de teameigenaar en teamleden als teameigenaar in gebreke blijft;
- bewaakt de toegang voor gastgebruikers.

Archiefinspecteur

Bijlage 3. Uitgebreide inhoudsopgave

1. Aanleiding	5
1.1. Wat is Microsoft Teams?.....	5
1.2. Wat is SharePoint?	5
2. Toelichting op de inhoud van de hoofdstukken	7
3. Inleiding	8
4. Scenario's voor Teams	9
4.1. Korte beschrijving scenario's	9
4.2. Scenario 1: Samenwerken in Teams	10
4.2.1 Het informatielandschap.....	10
4.2.2 Welke informatie zit in welk systeem	11
4.2.3 Rollen, verantwoordelijkheden en bevoegdheden.....	11
4.2.4 Informatiebeheerprocessen.....	12
4.2.5 Archiveringseisen en benodigde functionaliteiten en componenten	13
4.3. Scenario 2: Archiveren in Teams	14
4.3.1 Het informatielandschap.....	14
4.3.2 Welke informatie zit in welk systeem	14
4.3.3 Rollen, verantwoordelijkheden en bevoegdheden.....	15
4.3.4 Informatiebeheerprocessen.....	16
4.3.5 Archiveringseisen[1] en benodigde functionaliteiten en componenten	16
4.4. Scenario 3: Zaakgericht werken in Teams	18
4.4.1 Het informatielandschap.....	18
4.4.2 Archiveringseisen en benodigde functionaliteiten en componenten	18
4.4.3 Advies scenario 3.....	19
4.5. Conclusie	19
5. Beheren van informatie in een team	21
5.1. Uitgangspunten	21
5.2. Processen voor Informatiebeheer	21
5.3. Inrichtingsfase	21
5.3.1 Aanvragen Team.....	22
5.3.2 Beoordeling van de aanvraag.....	22
5.3.3 Inrichten van het Team	22
5.3.4 Beschikbaar stellen van het Team.....	23
5.4. Gebruiksfase	23
5.4.1 Creatie van informatie.....	23
5.4.2 Wijzigen van informatie	23
5.4.3 Verantwoordelijkheden tijdens de gebruiksfase	23
5.5. Bewaarfase	24
5.5.1 Afsluiten Team.....	24
5.5.2 Waardering / kwaliteitscontrole	24
5.5.3 Toegankelijk houden van informatie (bewaren).....	24
5.5.4 Vernietiging	24
5.5.5 Overbrengen/exporteren.....	24
5.6. Governance, Organisatie en rollen	25
5.6.1 Overwegingen voor informatie-governance.....	25
5.7. Kwaliteitszorg.....	26
6. Inrichten van een team	27
6.1. Regelen van randvoorwaarden	27
6.2. Aandachtspunten en tips bij het aanmaken van een team	27
6.2.1 Rollen.....	27
6.2.2 Naamgeving.....	28

6.2.3	Toegang	28
6.2.4	Vertrouwelijkheid	28
6.2.5	Inrichten Retentie en vernietiging	29
6.2.5.1	Bepalen bewaartermijn en retentielabels	29
6.2.6	Apps	30
6.2.7	Sjablonen	30
6.2.8	Prullenbak	31
6.2.9	Metadata	31
6.2.10	En dan nog dit	32
7.	Bewaarbeleid	33
7.1.	Metadata-schema	33
7.2.	Waarderen	34
7.2.1	Uitgangspunten	34
7.2.2	Archiefwet- en regelgeving	34
7.2.3	Definitie dossier of zaak	34
7.2.4	Waardering op document-, dossier/zaak- of siteniveau	35
7.2.4.1	Waardering op documentniveau	35
7.2.4.2	Waardering op dossier/zaakniveau	35
7.2.4.3	Waardering siteniveau	36
7.2.4.4	E-mail- en chatwaardering	36
7.2.5	Waardering op basis van verzameldossier of alleen processen	36
7.2.6	Technische inrichting waardering	36
7.3.	Bepalen bewaartermijn en vernietigingsdatum Retentie (herwaarderen)	38
7.4.	Classificeren	39
7.5.	Inrichting TEAMS (zie ook Gebruikers)	38
7.5.1	Inrichting waardering	38
8.	Kwaliteit inrichting	40
9.	Toegankelijkheid	42
9.1.	Vinden van informatie: Zoekfunctie	42
9.2.	Openstellen van informatie	42
9.2.1	Beleid	42
9.2.2	Mogelijkheden Microsoft365	42
9.2.3	Publiceren	43
9.3.	Beveiligen van informatie	44
9.3.1	Beleid	44
9.3.2	Mogelijkheden van Microsoft 365	45
9.3.3	Vindbaarheid	47
9.4.	Toegankelijkheid op termijn	47
10.	De functionaliteit van Microsoft 365	48
10.1.	Welke informatie zit waar	47
10.2.	Mogelijkheden voor workflows	48
10.3.	Functionaliteit voor vernietigen: hoe doen we dat?	48
10.4.	Functionaliteit voor overbrengen	48
10.5.	Werken met retentielabels, do's en dont's	47
11.	Gebruikers (Adoptie en gebruik)	49
11.1.	Kleine, middelgrote of grote gemeentelijke organisatie, maakt dat uit?	49
11.2.	Inrichten van rechten binnen de MS365 - E5 omgeving	49
11.3.	Gebruikers binnen de M365 – E5 omgeving	49
11.4.	Hoe verhouden de diverse M365 producten zich tot elkaar?	48
11.5.	Adaptie en adaptatie	48
11.5.1	Leren werken met een MS365 applicatie	49
11.5.2	Alle verandering is moeilijk	49

11.5.3	Training en een Vragen en Tips kanaal	50
11.5.4	Beheer van documenten in verschillende MS365 producten.....	50
11.5.5	Maak werkafspraken voor samenwerken in TEAMS	50
11.5.6	Gebruik van Teams is geen technisch feestje	51
11.5.6.1	Naamgevingsconventies volgen	51
11.5.6.2	Teameigenaren en lidmaatschap van een team.....	51
11.5.6.3	Beheer van het hoofdkanaal.....	51
11.5.6.4	Welke processen in zaaksysteem	51
11.5.6.5	Intern gebruik vs samenwerking.....	51
11.6.	Kwaliteit	51
11.7.	Blijvend proces.....	51
11.8.	Rollen / personae	51
11.9.	Inrichting TEAMS	51
Bijlage 1.	Voorbeeld van een gemeente.....	52
Bijlage 2.	RASCI tabel Werken met Teams.....	56
11.9.1	Rollen en verantwoordelijkheden bij het gebruik en beheer van Teams.....	56
Bijlage 3.	Uitgebreide inhoudsopgave.....	58

Bijlage 4. Gemeente Noordwijk – Beleid en inrichting TEAMS

Bijlage 5. Gemeente Noordwijk – Directievoorstel instemmen beleid en inrichting TEAMS

Bijlage 6. Gemeente Noordwijk – Onderbouwing E5 licentie

Bijlage 7. Gemeente Noordwijk – Uitvoeringsdocument inrichting Teams

Bijlage 8. Gemeente Zwolle – Autorisatiematrix