Lokaal bestuur Aarschot

ICT-richtlijn

Opsteldatum: 22.08.2022 **Bevoegde dienst:** Interne Zaken **Datum huidige versie:** 04.12.2023

Revisiegeschiedenis

Versienummer	Datum	Medewerkers	Beschrijving
0.1	22.08.22	Aaron Bergen, Bene Celis	Eerste versie, aanzet
0.1.1	24.08.22	Michèle Hermans	Opmerkingen en goedkeuring
0.2	19.09.22	Aaron Bergen	Toevoeging 4.1.5 Draadloze netwerken
0.2.1	20.09.22	Aaron Bergen	Toevoeging 4.1.2 Opslag en versturen van informatie
0.3	28.12.22	Sanne Fredericxk, Corrine Reynders, Aaron Bergen	Aanpassingen aan de hand van opmerkingen van de personeelsdienst
0.4	15.02.23	Aaron Bergen	Toevoeging 4.1.1.3 wachtwoordbeleid, eenduidige benamingen voor ICT-dienst en ICT-richtlijn.
0.5	03.10.23	Aaron Bergen	Toevoegingen Jurplus, verwerken feedback management
0.6	04.12.23	Aaron Bergen, Bene Celis, Erika Van Essche, vakbonden	Aanpassingen aan de hand van feedback van de DPO en de vakbonden.

Inhoud

1 Inleiding

De stad Aarschot, OCMW Aarschot en AGB Aarschot *(hierna: het lokale bestuur)* stellen heel wat ICT-middelen ter beschikking voor de dagelijkse werking van de verschillende diensten. Het gebruik hiervan wordt sterk aangemoedigd als ondersteuning en optimalisering van de kernactiviteiten. Het gebruik van ICT-middelen is volledig ingebed in de dagelijkse werking van het lokale bestuur. Defecten, hindernissen of uitval zijn nefast voor de dagelijkse werking. Het lokale bestuur heeft wettelijke en morele verplichtingen om veiligheidsmaatregelen te nemen met betrekking tot deze ICT-middelen en de informatie die via deze ICT-middelen verloopt.

Het doel van dit document is om een richtlijn voor ethisch en veilig gebruik van de ter beschikking gestelde middelen te zijn. Daarmee wordt een kader gecreëerd waarbinnen medewerkers van het lokale bestuur kunnen werken.

Wanneer er iets niet duidelijk is, is het de verantwoordelijkheid van de gebruiker om uitleg te vragen aan de ICT-dienst.

2 Toepassingsgebied

2.1 Wat zijn ICT-middelen?

Het lokale bestuur beheert informatie- en communicatietechnologieën voor de uitoefening van de dagelijkse werking, veralgemeend onder de noemer 'ICT-middelen'. Deze technologieën kunnen worden opgesplitst in:

- **netwerkapparatuur (network hardware)**
  alle toestellen, kasten en bekabeling die nodig zijn om het netwerk te maken en te beheren;
- **systeemapparatuur (system hardware)**
  alle toestellen, kasten en bekabeling die nodig zijn voor het lokaal faciliteren van software, opslag en back-ups;
- **apparatuur op gebruikersniveau (client hardware)**
  alle toestellen die gebruikt worden door medewerkers, zoals: laptops/computers, randapparatuur (printers, USB-sticks, badgelezers, …), telefoons of gsm-toestellen (lijst is niet exhaustief);
- **informatie op de apparatuur (data)**
  alle data die verstuurd, opgeslagen, ontvangen of geïnstalleerd is op de hierboven opgesomde apparatuur, onafhankelijk van de bron, o.a.:
  - metadata van bestanden;
  - inhoud van bestanden;
  - login gegevens (gebruikersnamen en wachtwoorden);
  - e-mails;
  - gedownloade en geüploade gegevens;
  - software of geïnstalleerde programmatuur.

Wanneer in dit document wordt verwezen naar 'ICT-middelen' dan gaat het, tenzij anders gespecifieerd, over alle hierboven beschreven technologieën.

2.2 Op wie is deze richtlijn van toepassing?

Deze ICT-richtlijn is van toepassing op alle categorieën van gebruikers die toegang hebben tot de ICT-middelen van het lokale bestuur waaronder: personeelsleden, mandatarissen, externe medewerkers, consultants, stagiairs, vrijwilligers.

In dit document wordt een onderscheid gemaakt tussen drie groepen medewerkers:

- **Gebruikers:**
  Deze groep omvat iedereen die toegang heeft tot ICT-middelen.
  Toegang wordt hier gebruikt in de breedste zin van het woord. Zodra er mogelijkheid is om ICT-middelen aan te raken, te gebruiken of te beïnvloeden is er sprake van toegang, zelfs al is het gebruik van de middelen niet verbonden aan de job inhoud.
- **Leidinggevenden:**
  Deze groep omvat uitsluitend de diensthoofden, de departementshoofden, de leidinggevenden, de decretale graden.
- **ICT-dienst:**
  Deze groep omvat uitsluitend iedereen die werkt bij of voor de ICT-dienst.

3 Gebruik

3.1 Ingebruikname

Voor het gebruik van de middelen beschreven in het toepassingsgebied moet elke gebruiker een gebruiksovereenkomst[1] ondertekenen. Deze overeenkomst tussen de gebruiker en het lokale bestuur beschrijft de ontvangen middelen en hun staat op het moment van ingebruikname.

De middelen die door het lokale bestuur ter beschikking worden gesteld blijven eigendom van het lokale bestuur.

3.2 Teruggave

De verkregen middelen moeten onder volgende omstandigheden terug worden overgemaakt aan het lokale bestuur:

- bij het beëindigen van de werkrelatie en uiterlijk op de laatste werkdag maakt de gebruiker op eigen initiatief een afspraak met de ICT-dienst voor het inleveren van de verkregen middelen;
- op vraag van de algemeen directeur.

Op het moment van teruggave worden de verkregen middelen vergeleken met de beschreven staat in bijlage 1 van de gebruiksovereenkomst. Hierbij wordt rekening gehouden met normale sporen van gebruik. Van elke gebruiker verwachten we dat hij/zij zorgvuldig omgaat met de verkregen middelen en bereid is verantwoording af te leggen over het gebruik van deze bedrijfsmiddelen. Inbreuken kunnen leiden tot sancties zoals bepaald in de rechtspositieregeling of het arbeidsreglement.

1 Gebruiksovereenkomst: zie bijlage 1

3.3 Accountblokkering

De verkregen toegangsrechten worden standaard in de volgende gevallen stopgezet:

- bij het beëindigen werkrelatie;
- in geval van langdurige ziekte;
- bij vermoeden van problemen in verband met veiligheid of misbruik;
- bij langdurig niet inloggen of niet aanpassen van wachtwoord;
- en/of langdurige afwezigheid.

Uitzonderingen op deze blokkering kunnen worden verleend door de algemeen directeur.

4 Verantwoordelijkheden

Alle gebruikers hebben de verantwoordelijkheid om te werken in overeenstemming met de regels en principes van deze ICT-richtlijn. De risico's rond het beveiligen van de ICT-middelen kunnen alleen tot een minimum herleid worden wanneer iedereen zich houdt aan de richtlijn. De verantwoordelijkheid om de ICT-middelen veilig te houden is een zaak van elke gebruiker (gebruikers, leidinggevenden, ICT-dienst).

Alleen de ICT-dienst of aangestelde derden mogen ICT-middelen installeren, demonteren, verplaatsen of wijzigen. Er mag geen ander materiaal gebruikt worden dan de ICT-middelen die door de ICT-dienst en door erkende leveranciers ter beschikking werden gesteld.

Enkel de software die rechtmatig aangekocht werd, mag gebruikt worden. Het gebruik van deze software moet toegelaten zijn met het oog op het specifieke karakter van de opdrachten en goedgekeurd zijn door de ICT-dienst.

Aansluitingen op externe netwerken zoals het internet, die niet toegelaten zijn, of die geïnstalleerd noch geconfigureerd zijn door de ICT-dienst, zijn verboden.

4.1 Gebruikers

4.1.1 Veiligheid van de ICT-middelen

4.1.1.1 Bewustzijn

Verantwoord gebruik van ICT-middelen begint bij een bewustzijn van de verschillende soorten gevaren en van de afgesproken procedures.

Daarom is het belangrijk dat de gebruiker de:

- ICT-richtlijn en -procedures goed volgt;
- de gevaren inziet die het onverantwoord omspringen met data en login-gegevens met zich meebrengt;
- de kwetsbaarheden inziet die het delen van ICT-middelen met zich meebrengt;
- een kritische blik heeft op ontvangen communicatie of verkregen hardware van onbekende bronnen.

In het kader van dit bewustzijn kan de ICT-dienst beslissen om onaangekondigde campagnes te voeren waarbij gebruikers getest worden op kennis en alertheid met focus op veiligheid.

4.1.1.2 Cybercriminaliteit

Cybercriminaliteit is zeer winstgevend wat meteen de hoge frequentie van de aanvallen verklaart. De criminelen spelen op het scherpst van de snee en passen zich aan naargelang de beveiliging verandert. Een volledige bescherming tegen aanvallen kan nooit gegarandeerd worden en net daarom is het belangrijk om in te zetten op preventie en informeren. Twee van de meest voorkomende soorten aanvallen zijn:

Malware
Malware is de verzamelnaam voor alle kwaadaardige software zoals virussen, spyware, ransomware, enzovoort. De verspreiding van malware gebeurt via allerlei kanalen zoals e-mail, websites, instant messaging of door middel van fysieke toegang. Onder andere door het downloaden en openen van een bijlage, door het klikken op een link naar een besmette website of door het inpluggen van een onbekende usb-stick kunnen de ICT-middelen van het lokale bestuur besmet worden met deze malware.

Phishing
Phishing is het 'hengelen' naar (vertrouwelijke) informatie van de gebruiker of het lokale bestuur. Criminelen proberen door het nabootsen van vertrouwde websites, e-mails of telefoongesprekken deze informatie te ontvreemden van de gebruiker. Doorgaans gaat dit om login-informatie, bankgegevens of vertrouwelijke documenten.

Om aanvallen van cybercriminelen zo goed mogelijk te voorkomen is het belangrijk dat de gebruiker:

- aandachtig is bij het verwerken van e-mails, goed kijkt naar de afzender en zichzelf de vraag stelt: "Verwacht ik een e-mail of een bestand van deze persoon?";
- niet klikt op links van niet vertrouwde bronnen;
- bestanden van niet vertrouwde bronnen niet opent.

In bovenstaande gevallen en in geval van twijfel is het verplicht de ICT-dienst te verwittigen.

4.1.1.3 Gegevenslekken

Er wordt gesproken over een gegevenslek in situaties waarin persoonsgegevens dreigen ongeoorloofd te worden openbaar gemaakt, verloren te gaan, vernietigd of gewijzigd te worden.

Wat zijn persoonsgegevens?

- Een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon (de "betrokkene" genoemd in de AVG).
- Een persoon kan geïdentificeerd worden via de naam, een foto, een telefoonnummer, zelfs een telefoonnummer op het werk, een code, een bankrekeningnummer, een e-mailadres, een vingerafdruk, een IP-adres,...of het combineren van deze of andere gegevens.
- Het gaat niet alleen over gegevens die te maken hebben met de persoonlijke levenssfeer (privacy) van personen, aar ook over gegevens die te maken hebben met het professionele of openbare leven van een persoon.

Wanneer een gebruiker een gegevenslek vaststelt is het van kritisch belang een melding te maken van het incident via privacy@aarschot.be.

4.1.1.4 Richtlijnen rond wachtwoorden

Het wachtwoord is de eerste beveiliging van een account. Het is dus belangrijk dat er met de hoogste voorzichtigheid wordt omgesprongen met wachtwoorden:

- wachtwoorden zijn persoonlijk, deel ze nooit met anderen;
- zorg dat niemand toekijkt bij het ingeven van je wachtwoord;
- gebruik voor elke account die je aanmaakt (Windows, e-mail, applicaties, online diensten, …) een ander wachtwoord. Gebruik je professionele wachtwoorden niet voor je privé accounts;
- het opslaan van wachtwoorden is slechts toegestaan wanneer dit gebeurt in een versleutelde wachtwoordkluis die is goedgekeurd door de ICT-dienst, gebruik dus niet de functie “wachtwoord onthouden” in je browser;
- het opschrijven of afdrukken van wachtwoorden is niet toegestaan;
- iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder hun loginnaam en wachtwoord gebeurt.

Wachtwoorden van alle gebruikers verlopen automatisch na drie maanden. Na het verlopen kiest de gebruiker een nieuw wachtwoord zonder logische opvolging van het vorige wachtwoord en uniek in vergelijking met andere accounts.

4.1.1.4.1 Toepassingsgebied

De richtlijnen rond wachtwoorden worden afgedwongen op de volgende toepassingsgebieden:

- toegang tot de ICT-middelen (computer, mobiel toestel van het lokale bestuur, de ter beschikking gestelde software);
- toegang tot de Microsoft 365 omgeving.

Het bestuur of een hogere overheid kan er ook voor kiezen om deze richtlijnen af te dwingen op volgende toepassingen::

- alle externe toepassingen (gebruikersbeheer Vlaanderen, Social Security, RRNAdmin, …);
- alle interne toepassingen die gebruikt worden op de verschillende diensten (Alfa, Bravo, Mercurius, Echo, …).

Ook als dit (nog) niet verplicht gesteld is, blijft het ten sterkste aan te raden dit zelf toe te passen op:

- alle externe toepassingen (gebruikersbeheer Vlaanderen, Social Security, RRNAdmin, …);
- alle interne toepassingen die gebruikt worden op de verschillende diensten (Alfa, Bravo, Mercurius, Echo, …);
- alle persoonlijke accounts die niets met het bestuur te maken hebben, dit voor je algemene online veiligheid.

4.1.1.4.2 Kiezen van een wachtwoord

De sterkte van een wachtwoord wordt in de eerste plaats beïnvloed door de lengte, hoe langer een wachtwoord hoe beter. De ICT-dienst raadt aan om een wachtwoordzin te gebruiken in plaats van een moeilijk te onthouden combinatie van letters en tekens.

De volgende vereisten zijn van toepassing:

- een lengte van minimum 12 karakters;
- het gebruik van hoofdletters;
- het gebruik van kleine letters;
- het gebruik van cijfers;
- het gebruik van speciale tekens zoals: ! @ # % ( ];
- gebruik geen voor de hand liggende namen, woorden of getallen. Verwerk je naam, geboortedatum, gebruikersnaam of dienst niet in je wachtwoord.

Voorbeelden van sterke wachtwoorden:

- wEntelteef;57hoplakEE615
- 6504hond,Put-feesttaart!
- Erwaseensaldaareenvlindermetgrotebaard9846&$
- #a9*!F59Hyfe&5cn
- wv@!L$SUXH23!7Br

Voorbeelden van enorm zwakke wachtwoorden:

- 123456
- 123456789
- qwerty
- password
- 3200wachtwoord!
- Login-3200

4.1.1.4.3 Wijzigen van wachtwoorden

Het is verplicht en afgedwongen om het Microsoft-account wachtwoord minstens elke drie maanden te wijzigen. Daarnaast kan de ICT-dienst vragen om onmiddellijk je wachtwoord te wijzigen wanneer er bijvoorbeeld een inbraak of een afwijking van de afspraken wordt vastgesteld. Je kan steeds op eigen initiatief je wachtwoord wijzigen door na het aanmelden op je computer de toetsencombinatie CTRL+ALT+DEL te gebruiken en de optie “Wachtwoord wijzigen” te selecteren, en je bent verplicht dit te doen wanneer je het minste vermoeden hebt dat iemand je wachtwoord kent.

4.1.1.5 Multi Factor Authentication (MFA)

Multi Factor Authentication (MFA) is een beveiligingsmaatregel waarbij gebruikers hun identiteit moeten bevestigen bij het inloggen door middel van een prompt van een smartphone applicatie, of een hardware authenticatie toestel..

Elke gebruiker is verplicht gebruik te maken van MFA en zal zijn/haar identiteit minstens elke week moeten bevestigen via het MFA-systeem.

4.1.1.6 Inbraak

Wanneer een externe persoon of systeem ongeoorloofd toegang krijgt tot de systemen van het lokale bestuur dan spreken we over inbraak. Inbraak in de ICT-middelen kan bijvoorbeeld gebeuren door het verkrijgen van de logingegevens van een gebruiker of door zwakke punten in beveiliging van de systemen te misbruiken.

De gebruiker neemt verplicht minstens de volgende maatregelen om inbraak op de ICT-middelen te voorkomen:

- het vergrendelen van de systemen bij het verlaten van de ruimte (Windows-toets + L);
- het volgen van de afspraken rond wachtwoorden;
- de verkregen ICT-middelen niet door derden laten gebruiken.

4.1.1.7 Diefstal of verlies

Wanneer een malafide persoon permanente fysieke toegang heeft tot de systemen van het lokale bestuur zijn er veel meer mogelijkheden om de systemen aan te vallen. Het is dus van enorm belang om de ontvreemding van ICT-middelen van het lokale bestuur te voorkomen.

De gebruiker neemt verplicht minstens de volgende maatregelen om diefstal van de ICT-middelen te voorkomen:

- het nooit onbeheerd achterlaten van de toestellen in publieke ruimtes of op kantoor. Berg je laptop steeds op;
- het afsluiten van onbemande ruimtes wanneer er ICT-middelen achterblijven.

In geval van diefstal of verlies dient de gebruiker dit op het moment van vaststelling te melden aan de ICT-dienst. De gebruiker dient diefstal ook onmiddellijk aan te geven bij de politie en het bewijs van aangifte te bezorgen aan de ICT-dienst op het moment van ontvangst.

4.1.1.8 Beschadiging

In geval van beschadiging meldt de gebruiker de schade onmiddellijk na het feit of de vaststelling en ten laatste binnen de 48 uur aan de ICT-dienst en stelt een verklaring op over de omstandigheden van de beschadiging. Het schadebedrag zal ten laste van de medewerker teruggevorderd worden bij herhaling van schade, verlies of diefstal. Bij duidelijk aantoonbare nalatigheid zal het schadebedrag meteen teruggevorderd worden ten laste van de medewerker.

4.1.1.9 Gebruik voor privédoeleinden

De ICT-middelen van het lokale bestuur worden ter beschikking gesteld van de gebruikers om de professionele activiteiten uit te voeren. Gezien het gebruik van deze middelen echter zo alledaags is geworden, is incidenteel gebruik voor privédoeleinden toegestaan wanneer dit redelijk blijft, geen onwettelijk gebruik is en niet in strijd is met deze richtlijn.

Concreet is persoonlijk gebruik enkel toegestaan wanneer:

- dit zelden en van korte duur is;
- dit geen impact heeft op de plichten van de gebruiker;
- dit geen impact heeft op de uitvoering van je taken en de productiviteit van jezelf en die van je collega-medewerkers niet in het gedrang brengt;
- er geen extra kosten zijn voor het lokale bestuur;

- het netwerk niet overbelast wordt door onnodig internetverkeer;
- het gebruik niet in strijd is met de rechtspositieregeling/arbeidsreglement, deze of andere richtlijnen;
- het gebruik niet in strijd is met de GDPR- of andere relevante wetgevingen.

4.1.2 Opslag en versturen van informatie

4.1.2.1 Lokale opslag

De gebruiker is verantwoordelijk voor de juiste en meest veilige opslag van informatie. Dit wil zeggen dat werkgerelateerde bestanden moeten worden opgeslagen op netwerkschijven en in de juiste map. Alleen op die manier kan een back-up gegarandeerd worden.

4.1.2.2 Cloud opslag en versturen van informatie

Het online opslaan en versturen van informatie wordt uitsluitend toegestaan via diensten van Microsoft 365 zoals Teams, OneDrive of Sharepoint. Het gebruik van alternatieven is ten strengste verboden.

4.1.3 Digitale correspondentie

4.1.3.1 E-mail

Mailboxen op de domeinen van het lokale bestuur en op naam van de gebruiker worden als vertrouwelijk behandeld maar blijven eigendom van het lokale bestuur. Het gebruik van de officiële e-mailadressen van het lokale bestuur is enkel toegestaan voor professionele doeleinden voor zover:

- de uitgewisselde informatie ondubbelzinnig gelinkt is aan je taken;
- in de e-mail geen vertrouwelijke informatie wordt meegedeeld waartoe je geen bevoegdheid hebt;
- de geldende stijlregels worden nageleefd.

Bij een geplande afwezigheid moet je steeds je “out-of-office reply” vooraf inschakelen. Je voorziet daarbij een korte afwezigheidsboodschap waarin op een professionele manier de aanvang en het einde van je afwezigheidsperiode vermeld staat. Vermeld daarbij ook het e-mailadres en/of telefoonnummer van de collega(‘s) van de betrokken dienst die men kan contacteren tijdens jouw afwezigheid.

Bij een onvoorziene afwezigheid is je direct leidinggevende of elke andere door jou aangestelde vertrouwenspersoon ertoe gerechtigd om je mailbox te controleren op inkomende e-mails. Het doel hiervan is de lopende zaken en de continuïteit van de dienstverlening te kunnen garanderen.

Deze toegang is evenwel beperkt tot e-mails die noodzakelijk zijn om de continuïteit van de dienst te waarborgen.

Wanneer je tewerkstelling, mandaat, contract of aanstelling stopt, wordt er van gebruikers verwacht dat ze correspondenten laten weten dat ze de organisatie verlaten met vermelding van de contactgegevens van de dienst of collega’s. Diezelfde informatie dient eventueel in een

automatisch afwezigheidsbericht te worden opgenomen en moet ingeschakeld worden vóór vertrek met ingangsdatum na vertrek mits toestemming van het diensthoofd.

Na het vertrek zal de toegang tot de mailboxen voor de gebruiker worden stopgezet en de mailbox verwijderd of kan mits schriftelijke toestemming van de gebruiker toegang worden verleend aan het diensthoofd. Mits toestemming van de gebruiker én het diensthoofd kan ook toegang worden verleend aan een collega voor een maand. Hierna zal de individuele mailbox verwijderd worden. Mits akkoord van de gebruiker kan deze periode verlengd worden tot maximum 3 maanden.

Om continuïteit te garanderen is het de verantwoordelijkheid van de gebruikers en de dienst waar ze tewerkgesteld zijn om vóór het geplande vertrek door de ontvangen e-mails en bestanden te gaan om ze te verwijderen, op te slaan in een gedeelde map of door te sturen naar collega's.

4.1.3.2 Microsoft 365

Microsoft 365 accounts gekoppeld aan een Microsoft 365 licentie van het lokale bestuur en op naam van de gebruiker worden als vertrouwelijk behandeld maar blijven eigendom van het lokale bestuur. Het is niet toegelaten om Microsoft 365 accounts van het lokale bestuur te gebruiken voor commerciële doeleinden.

Zodra het arbeidscontract of de aanstelling van de gebruiker eindigt zal de toegang tot de Microsoft 365 account voor de gebruiker onmiddellijk worden stopgezet.

4.1.4 Draadloze netwerken

Het lokale bestuur biedt verschillende draadloze Wifi netwerken aan die gebruikt kunnen worden om te verbinden met het bedrijfsnetwerk of het internet. Voor de algemene veiligheid van de middelen is het belangrijk dat het juiste netwerk voor het juiste toestel wordt gebruikt.

Radius

- Rechtstreekse toegang tot het bedrijfsnetwerk en internet.
- Alleen toegelaten voor toestellen in beheer van de ICT-dienst.
- De gebruiker moet toelating vragen om hiermee te kunnen verbinden.

Mobiel

- Alleen toegang tot het internet.
- Alleen toegelaten voor mobiele toestellen van medewerkers.
- Niet toegelaten voor derden, deel het wachtwoord met niemand.

Hotspot (gasten-netwerk)

- Alleen toegang tot het internet
- Toegelaten voor externen

Het is niet toegelaten om data te versturen over netwerken die niet beveiligd zijn, zoals een Wifinetwerk zonder wachtwoord.

4.1.5 Meldplicht

Het is van groot belang om de ICT-dienst op de hoogte te houden van de status van de ICT-middelen. Wanneer er een aanval gebeurt op de systemen van het bestuur is tijd een belangrijk middel om erger te voorkomen, maar ook in geval van schade kan het nodig zijn om snel te handelen in het kader van de garantie. Als je zelf geen contact kan opnemen met de bevoegde dienst moet je de melding maken bij je diensthoofd die de verantwoordelijkheid heeft om de informatie daarna over te maken aan de ICT-dienst.

Het is verplicht om de ICT-dienst onmiddellijk op de hoogte te brengen bij:

- de minste argwaan over een ontvangen e-mail of bijlage;
- het kleinste vermoeden van actieve malware;
- het verliezen of ontvreemd zijn van een ICT-middel;
- de minste schade aan een ICT-middel;
- het vermoeden van een inbreuk op deze richtlijn;
- het besef van een gegevenslek;

4.1.5.1 Meldpunten

Meldingen aan de ICT-dienst dienen te gebeuren op de hieronder in prioritaire vermelde volgorde:

1. via het ICT support portaal;
2. telefonisch via 016 550 325 of 016 550 369 wanneer je niet aan het support portaal kan.

Meldingen in verband met gegevenslekken en inbraken op vlak van privacy dienen te gebeuren via privacy@aarschot.be.

4.2 Leidinggevenden

Alle hierboven beschreven artikels die van toepassing zijn op de gebruiker zijn ook van toepassing op de leidinggevenden. Daarnaast hebben de leidinggevenden de volgende extra verantwoordelijkheden:

4.2.1 Voorbeeldfunctie

De leidinggevende geeft het goede voorbeeld in het gebruik van de middelen en het naleven van deze richtlijn. Als leidinggevende heb je dus een voorbeeldfunctie. Daarnaast kijk je ook toe op het naleven van deze richtlijn door de medewerkers van je team.

4.2.2 Toezicht

Leidinggevenden zijn de eerste lijn in toezicht op de gebruikers. Ze zorgen dat deze richtlijn wordt nageleefd en helpen hun medewerkers om ze correct toe te passen. Het is dus belangrijk dat de problemen die gebruikers hebben, opgevolgd worden en indien nodig besproken worden met de ICT-dienst. Daarnaast is het van belang om inbreuken op deze richtlijn onmiddellijk op te volgen zodat de veiligheid van de systemen gewaarborgd blijft. Wanneer de leidinggevenden een inbreuk vaststellen, melden ze dit bij de ICT-dienst om soortgelijke inbreuken in de toekomst te voorkomen.

4.2.3 Toegangsbeheer

Elke toegangsrecht voor toepassingen en bestanden in gebruik of opgeslagen bij het lokale bestuur moet worden aangevraagd bij de ICT-dienst en worden gemotiveerd door de leidinggevende van de aanvrager.

4.3 ICT-dienst

De ICT-dienst heeft als doel de werking van het lokaal bestuur te ondersteunen en te faciliteren. Concreet wil dit zeggen dat de ICT-dienst naast het zorgen voor passende apparatuur ook instaat voor de beveiliging en de operationele werking van de middelen. De hierboven beschreven afspraken (4.1) vormen de basis voor het verzekeren van de dagelijkse werking.

4.3.1 Bewustmaking en opleidingen

Om de impact van de hierboven beschreven afspraken zo beperkt mogelijk te houden en het bewustzijn van de gebruikers te vergroten, zal de ICT-dienst in de mate van het mogelijke opleidingen voorzien en steekproeven organiseren.

5 Ongeoorloofd gebruik

Het lokaal bestuur laat het gebruik van de ICT-middelen niet toe (lijst is niet exhaustief):

- wanneer het in strijd is met de in hoofdstuk 4 beschreven verantwoordelijkheden;
- om informatie op te slaan of te verspreiden die:
    - het imago, de morele of de economische belangen van het lokale bestuur kan schaden;
    - beledigend, lasterlijk, aanstootgevend of discriminerend is;
    - schade kan toebrengen aan derden;
    - strijdig is met de openbare orde en openbare zeden;
    - gevaar voor verslaving vormt;
    - aanzet tot discriminatie wegens ras, etnische afkomst, geslacht, geloof, enz..
- om vertrouwelijke informatie door te geven aan personen die niet gerechtigd zijn om deze informatie te ontvangen;
- om software te installeren of te gebruiken waarvoor de ICT-dienst geen toestemming heeft verleend;
- om acties te ondernemen die de beveiliging van ICT-middelen in het gedrang kunnen brengen zoals bijvoorbeeld:
    - het omzeilen van systeem- netwerkbeveiliging;
    - het ontwerpen of installeren van malware;
    - ongeoorloofde toegang forceren;
    - het netwerk afluisteren.
- om eigen ICT-middelen aan te sluiten op hardware van het lokale bestuur zoals bijvoorbeeld:
    - smartphones en tablets;
    - laptops;
    - randapparatuur;

    - USB-sticks.
- om intern ontwikkelde programma's te commercialiseren en/of voor persoonlijke doeleinden te gebruiken;
- in het buitenland zonder voorafgaande toestemming van de leidinggevende en de ICT-dienst.

6 Aansprakelijkheid

Gebruikers zijn persoonlijk aansprakelijk voor alle handelingen die worden uitgevoerd met hun verkregen gebruikersaccount. De gebruiker kan te allen tijde om verantwoording worden gevraagd over het gebruik van de ICT-middelen.

7 Toezicht en controle

7.1 Principieel recht op controle

Binnen de wettelijke grenzen kan het lokale bestuur controle uitoefenen op gegevens die een gebruiker opslaat, verstuurt of ontvangt. Dit past binnen de opdracht van het lokale bestuur en haar doelstellingen.

7.2 Toepassingsgebied

De controle is van toepassing op:

- het gebruik van internet;
- het gebruik van e-mail;
- het gebruik van andere professionele communicatiemiddelen zoals Microsoft Teams;
- de informatie en bestanden die gebruikers doorsturen via of publiceren op internet;
- de informatie en bestanden die gebruikers opslaan.

7.3 Doel van de controle

Controle door de ICT-dienst is alleen mogelijk als een van de volgende vijf doelen worden nagestreefd:

1) het voorkomen en vaststellen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden.

Dat zijn feiten als:

- het kraken van computers, waaronder het op illegale manier kennis nemen van persoonsgegevens of vertrouwelijke medische bestanden;
- het raadplegen van sites die
    - zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;

- anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
- een gevaar voor verslaving vormen zoals goksites en pornografische sites;
- het privéleven van iemand aantasten.

2) het beschermen van bepaalde informatie. De algemene regel is 'openbaarheid van bestuur'. Er zijn echter uitzonderingen op die regel, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle door de werkgever is mogelijk als de te beschermen belangen van het lokale bestuur, zoals bepaald in de vigerende regelgeving rond openbaarheid van bestuur, worden geschaad. De werkgever kan ook controle doen op de praktijken die in strijd zijn met die belangen.

4) het te goeder trouw naleven van deze ICT-richtlijn en andere richtlijnen voor het gebruik van onlinetechnologieën.

5) het verzekeren van de continuïteit van de dienstverlening bij overlijden, onvoorziene afwezigheid of vertrek van een werknemer.

De gegevens die verzameld en verwerkt worden voor een controle met een van de vijf bovenstaande doelen, kunnen niet gebruikt worden voor een controle met andere doeleinden. Als een wettelijke bepaling dat toestaat of oplegt, kan de ICT-dienst de gegevens voor een ander doel gebruiken, inkijken en herleiden tot een bepaald personeelslid.

7.4 Methodologie

De controle wordt uitgevoerd door de ICT-dienst en zal uitsluitend gebeuren met goedkeuring van de algemeen directeur. De ICT-dienst heeft door hun dagelijkse functie de mogelijkheid om toe te zien op het gebruik van (een deel van) de ICT-middelen. Door deze autorisatie zijn ze gebonden aan strikte voorwaarden ten aanzien van de persoonlijke levenssfeer van de werknemers en worden alle acties discreet uitgevoerd. Daarbij moet het recht op een privéleven van de personeelsleden gerespecteerd worden. De controle moet getoetst worden aan:

- het finaliteitsbeginsel: een controle is alleen mogelijk voor het nastreven van gerechtvaardigde doelen;
- het transparantiebeginsel: er wordt open gecommuniceerd over de controles en de doelen en voorwaarden van de controles;
- het proportionaliteitsbeginsel: de controle en het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen:

- het recht van de werkgever op controle van werkmiddelen;
- het recht van de werknemer op zijn privéleven.

De ICT-dienst mag elke controle uitvoeren die inherent is aan het beheer van ICT-middelen, om de goede werking ervan te waarborgen, om overbelasting of veiligheidsproblemen te voorkomen of te verhelpen. Alle medewerkers moeten zich bewust zijn van het bestaan van deze controlemogelijkheid en van het feit dat alle communicatie die zij via het netwerk uitwisselen, hieraan onderworpen kan worden.

Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de systeem- en netwerkbeheerders worden ingekeken.

8 Procedure bij incidenten

Een incident is een actie of een feit die de normale werking van het informaticasysteem of het netwerk verstoort.

Voor de toepassing van deze richtlijn wordt een onderscheid gemaakt tussen twee soorten incidenten:

- technische incidenten;
- inbreuken op de gedragsregels.

8.1 Procedure bij technische incidenten

Bij het uitvoeren van hun beheerstaken wordt de ICT-dienst frequent geconfronteerd met technische incidenten. Gebruikers van de ICT-middelen waarvoor ze verantwoordelijk zijn, kunnen bijvoorbeeld het slachtoffer zijn van computervirussen of andere ongewenste fenomenen. Bij het oplossen van deze incidenten kan de ICT-dienst zelfstandig optreden en het netwerkgedrag van gebruikers op individueel niveau opvolgen zolang dit voor de oplossing van het incident noodzakelijk is.

Wanneer het voor de veiligheid en om de goede werking van het netwerk te waarborgen noodzakelijk is, kan de ICT-dienst (sub)netwerken en andere toegangen (zoals bv. e-mailadressen, directories, VPN, ...) onmiddellijk en zonder voorafgaandelijke waarschuwing afsluiten.

Wanneer noodzakelijk moet de medewerker op vraag van de systeem- en netwerkbeheerders de ICT-middelen onmiddellijk loskoppelen van de systemen van het lokale bestuur.

8.2 Procedure bij inbreuken op de gedragsregels

Bij inbreuken op de regels van deze richtlijn zijn, naargelang de ernst van de inbreuk, één of meer van de volgende procedurestappen van toepassing.

8.2.1 Meldingen en hun behandeling

Wie een inbreuk op de regels van deze richtlijn vaststelt, meldt dit bij een eerste waarneming aan de betrokken collega-gebruiker en wijst op de correcte manier van werken. Wanneer je herhaaldelijke inbreuken vaststelt, meld je dit aan de ICT-dienst. Meldingen kunnen onder meer afkomstig zijn van gebruikers, diensthoofden, mandatarissen of derden.

Een inbreuk kan ook gemeld worden aan de vertrouwenspersoon.

De ICT-dienst volgt de volgende procedure:

1. Er lijken geen regels van de ICT-richtlijn overtreden te zijn: De ICT-dienst behandelt zelf de melding op informele wijze en legt de afzender van de melding uit waarom geen verdere procedurestappen noodzakelijk zijn. Als de afzender van de melding niet instemt met de uitleg van de ICT-dienst, wordt de volgende procedurestap gevolgd.

2. Eén of meer regels van het ICT-richtlijn lijken (ernstig) overtreden te zijn: De ICT-dienst onderzoekt de gemelde inbreuk naar de effectieve feiten. Hierbij wordt een dossier over de feiten opgesteld.

Indien noodzakelijk neemt de ICT-dienst onmiddellijk (tijdelijke) voorzorgsmaatregelen om verdere onregelmatigheden te voorkomen.

De ICT-dienst bezorgt het dossier aan de algemeen directeur. Afhankelijk van de ernst van de inbreuken en van de schade berokkend aan het lokale bestuur wordt er door de algemeen directeur een vervolgprocedure opgestart. De algemeen directeur oordeelt, eventueel in overleg met het betrokken diensthoofd of anderen, over de te nemen vervolgstappen en/of tuchtmaatregelen in toepassing van de rechtspositieregeling en/of het arbeidsreglement en over eventuele andere maatregelen bijvoorbeeld op gerechtelijk vlak.

Mogelijke vervolgstappen kunnen zijn:

8.2.1.1 Waarschuwingsprocedure

De waarschuwingsprocedure heeft als doel de gebruiker te informeren over de gemelde of vastgestelde inbreuk en verantwoording te vragen over het gebruik van de ter beschikking gestelde ICT-middelen. De gebruiker wordt daarbij op de hoogte gebracht dat zijn/haar netwerkgedrag op individuele wijze gecontroleerd zal worden wanneer een nieuwe onregelmatigheid wordt vastgesteld.

De volgende regels worden hierbij in acht genomen:

- de voor de onregelmatigheid verantwoordelijk geachte gebruiker wordt uitgenodigd voor een gesprek met zijn/haar leidinggevende, een werknemer van de ICT-dienst en eventueel uitgebreid met een werknemer van de personeelsdienst en/of een lid van de leidinggevenden;
- dit gesprek heeft plaats voor iedere beslissing of evaluatie die de gebruiker individueel kan raken;
- de gebruiker krijgt de kans eventuele bezwaren met betrekking tot de voorgenomen beslissing of evaluatie uiteen te zetten. De gebruiker kan zich desgewenst door een vakbondsafgevaardigde laten bijstaan.

8.2.1.2 Maatregelen

Bij vaststelling van veiligheidsrisico's kunnen, naargelang het geval, volgende maatregelen genomen worden om de veiligheid en integriteit van de ICT-middelen te waarborgen:

- de toegangsrechten van de gebruiker kunnen gedurende het onderzoek geschorst of beperkt worden;
- ICT-middelen van de betreffende gebruiker kunnen worden geïnspecteerd en in beslag genomen.

8.2.1.3 Sancties

Sancties kunnen worden genomen in toepassing van de rechtspositieregeling en/ of het arbeidsreglement.

Mogelijke maatregelen en sancties die tegen werknemers kunnen worden genomen bij vaststelling van inbreuken op deze richtlijn en rekening houdend met de ernst van de inbreuken zijn:

- de gebruiker verwittigen van de inbreuk en opleiden om beter om te gaan met de verkregen ICT-middelen;
- ordemaatregelen door de algemeen directeur: de tijdelijke opheffing van een account of tijdelijke beperking van de toegang tot of het gebruik van (delen van) de ICT-middelen waarbij een evenwicht wordt gezocht tussen het belang van de dienst, de bescherming van de systemen en de rechten van de betrokkene;
- maatregelen en sancties zoals voorzien in de toepasselijke regelgeving en de interne reglementen.

8.2.1.4 Gerechtelijk onderzoeken

Iedereen die aan deze richtlijn onderworpen is, dient er zich bewust van te zijn dat het lokale bestuur maximaal zal meewerken aan gerechtelijke onderzoeken en betrokken instanties zal inlichten als de toestand daartoe aanzet.

Bijlage 1

Lokaal bestuur Aarschot

Gebruiksovereenkomst ICT-middelen

Gebruiker: .....

Opsteldatum:	28.12.2022	**Bevoegde dienst:**	Interne Zaken
Huidige versie:	0.3	**Auteurs:**	Aaron Bergen, Bene Celis

Revisiegeschiedenis

Versienummer	Datum	Medewerkers	Beschrijving
0.1	20.09.22	Aaron Bergen, Bene Celis	Eerste versie
0.2	28.12.22	Aaron Bergen	Klaar voor goedkeuring
1	05.10.23	Aaron Bergen, Christi Van Calster	Aanpassingen in verband met uitrol ICT-richtlijn

De stad Aarschot, OCMW Aarschot en AGB Aarschot, verder genoemd “het lokaal bestuur”

en .....

verder genoemd “de gebruiker”

KOMEN OVEREEN ALS VOLGT

Het lokaal bestuur stelt aan de gebruiker voor de uitoefening van diens opdracht volgende ICT-middelen ter beschikking in de staat zoals beschreven:

Laptop / Desktop	Merk	
	Type	
	ID	
	Staat	
Accessoires	Laptoptas	
	Muis	
	Keyboard	
	Monitor	
	Docking station	
	Headset	

Door de ondertekening van deze overeenkomst verklaart de gebruiker kennis te hebben van de ICT-richtlijn en deze na te leven.

Opgemaakt in Aarschot op 4.12.2023

De gebruiker

Het lokaal bestuur