Bijlage X Richtlijnen voor veilig en verantwoord gebruik van ICT-systemen en toepassingen in AZ Diest

Deze bijlage maakt integraal deel uit van het arbeidsreglement van AZ Diest en vervangt de gedetailleerde bepalingen in de artikelen 58 en 59 over het gebruik van computer- en communicatiesystemen. De artikelen 58 en 59 verwijzen beknopt naar deze bijlage als bindend beleidsdocument voor het gebruik van ICT-middelen.

(versie 2, 10/06/2026)

1. Doelstelling

Binnen AZ Diest wordt dagelijks gewerkt met informatie- en communicatietechnologieën (ICT). Deze richtlijnen geven alle gebruikers een leidraad om op een veilige, verantwoorde en ethische manier gebruik te maken van IT-systemen en toepassingen.

Het naleven van deze beleidsregels is essentieel om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen, om de algemene cyberveiligheid te versterken en om de privacy van patiënten, medewerkers en andere betrokkenen te beschermen.

Dit beleid ondersteunt de naleving van de Europese NIS2-richtlijn, de Belgische wet van 26 april 2024 inzake cyberbeveiliging van netwerk- en informatiesystemen, de Algemene Verordening Gegevensbescherming (AVG) en de CyberFundamentals (Essential-niveau) zoals uitgewerkt door het Centrum voor Cybersecurity België.

2. Toepassingsgebied

Deze richtlijnen zijn van toepassing op iedereen die toegang heeft tot de IT-infrastructuur, -systemen en -gegevens van AZ Diest, ongeacht de werkplek:

- werknemers van AZ Diest (contractueel en statutair);
- artsen en andere zorgverstrekkers die AZ Diest-infrastructuur gebruiken;
- externen (consultants, contractors, leveranciers, tijdelijke medewerkers);
- stagiairs en studenten
- vrijwilligers en alle andere personen die geautoriseerde toegang krijgen.

3. Kader en definities

Onder ICT-middelen worden onder meer verstaan: laptops, desktopcomputers, smartphones, tablets, randapparatuur, netwerkcomponenten, softwaretoepassingen, e-mail, internettoegang, cloudtoepassingen, AI-tools en alle andere digitale hulpmiddelen die door of namens AZ Diest ter beschikking worden gesteld.

AZ Diest maakt gebruik van de gedeelde IT-diensten van UZ Leuven (‘shared IT’) voor onder meer netwerkbeheer, infrastructuur, beveiliging, logging en incidentopvolging. De technische maatregelen en procedures van shared IT zijn bindend voor alle gebruikers van AZ Diest.

4. Accounts en toegangsbeheer

Toegang tot de systemen van AZ Diest gebeurt steeds via een persoonlijk gebruikersaccount. Het aanmaken, beheren en intrekken van accounts verloopt centraal via de bevoegde diensten van AZ Diest en UZ Leuven shared IT.

Wat doet AZ Diest / shared IT:

- aanmaken van persoonlijke accounts bij de start en tijdige deactivering bij beëindiging van de samenwerking;
- toekennen van rechten volgens het principe van “least privilege”: enkel toegang tot de toepassingen en gegevens die nodig zijn voor de functie;
- afdwingen van sterke authenticatie (bijvoorbeeld multifactor-authenticatie) voor kritieke toepassingen en externe toegang.

Wat je moet doen:

- gebruik uitsluitend je eigen account en wachtwoord;
- vraag bijkomende toegang enkel aan indien nodig voor je functie;
- meld onmiddellijk als je vermoedt dat je account of wachtwoord gecompromitteerd is.

Wat je niet mag doen:

- je account of wachtwoord delen met anderen;
- inloggen met de account van een collega, ook niet “kortstondig” of “uit praktische overwegingen”.

5. Fysieke toegang tot gebouwen en lokalen

AZ Diest is in belangrijke mate publiek toegankelijk, maar bepaalde gebouwen, afdelingen, gangen en lokalen zijn fysiek beveiligd. Toegang tot deze zones is enkel toegestaan via persoonsgebonden badges (of sleutels) en volgens de toegangsprofielen die door de organisatie zijn toegekend.

Wat je moet doen:

- gebruik enkel je eigen badge (sleutel) en laat die niet door anderen gebruiken;
- houd deuren naar beveiligde zones gesloten en zorg dat onbevoegden niet “meelopen”;
- meld verlies of diefstal van je badge onmiddellijk.

Wat je niet mag doen:

- je badge (sleutel) uitlenen of doorgeven;
- onbevoegden onbegeleid toegang verlenen tot beveiligde zones;
- deuren naar beveiligde zones opzettelijk openhouden (bijvoorbeeld met een voorwerp).

Wat indien je je badge thuis bent vergeten:

- aan het onthaal ‘Hoofdingang’ kun je een tijdelijke badge verkrijgen na registratie en in ruil voor je id-kaart of rijbewijs.

6. Gegevensbeheer en classificatie

AZ Diest hanteert vier categorieën van gegevens: gevoelig (categorie 1), vertrouwelijk (categorie 2), intern (categorie 3) en publiek (categorie 4). Deze classificatie geldt voor alle vormen van gegevensverwerking, niet enkel bij AI-gebruik.

Wat doet AZ Diest:

- voorzien van beleid en procedures inzake discretieplicht, gegevensclassificatie en beveiligingsniveaus;
- voorzien van centrale systemen (zoals EPD/KWS, fileservers en samenwerkingsplatformen) waarvoor automatische back-ups worden gemaakt;
- nemen van organisatorische en technische maatregelen voor bescherming van persoonsgegevens (AVG/GDPR).

Wat je moet doen:

- behandel gegevens volgens hun classificatie;
- bewaar belangrijke gegevens steeds in de voorziene centrale systemen;
- verwijder gegevens die niet langer nodig zijn of draag ze over volgens de geldende procedures;
- meld (vermoedelijke) datalekken onmiddellijk aan de DPO van AZ Diest (privacy@azdiest.be). Zie eveneens de intranetpagina: https://wiki.uz.kuleuven.ac.be/display/azd/Datalekken+melding

Wat je niet mag doen:

- AZ Diest-gegevens opslaan op niet-geautoriseerde cloudplatformen;
- AZ Diest-gegevens opslaan op persoonlijke apparatuur (pc, smartphone, USB, persoonlijke cloud);
- patiënt- of personeelsgegevens opsturen via onbeveiligde kanalen (zoals onbeveiligde e-mail) of delen met onbevoegden.

7. Wachtwoorden en authenticatie

Gebruikers moeten sterke, unieke wachtwoorden gebruiken en deze adequaat beschermen.

Wat doet AZ Diest / shared IT:

- opleggen van minimumvereisten voor wachtwoorden;
- beschikbaar stellen van een wachtwoordmanager;
- voorzien van een self-service wachtwoord-reset en ondersteuning via de IT-helpdesk;
- afdwingen van multifactor-authenticatie (MFA) waar noodzakelijk.

Wat je moet doen:

- wijzig je wachtwoord zodra je vermoedt dat iemand anders het kent;
- gebruik je AZ Diest-gebruikersnaam en wachtwoord nooit voor privétoepassingen;
- gebruik waar mogelijk de aangeboden wachtwoordmanager.

Wat je niet mag doen:

- je wachtwoord opschrijven op post-its, in notitieboekjes of onbeveiligde digitale notities;
- je wachtwoord delen met anderen of laten intypen door derden.

8. Hardware en software

Alle hardware en standaardsoftware worden door AZ Diest en UZ Leuven shared IT voorzien en geconfigureerd volgens de geldende beveiligingsrichtlijnen (patching, antivirus, configuratiebeleid).

Wat doet AZ Diest - IT-afdeling:

- Voorzien van alle hardware (laptops, computers, werkstations, printers, ...) die nodig zijn voor het uitvoeren van je taken;
- Configureren van al die hardware volgens de laatst goedgekeurde richtlijnen;
- Ondersteuning bieden in geval van problemen (via de IT-helpdesk);
- Vervangen en verwijderen van oude IT-hardware;
- Beschikbaar stellen van software via het Software Center. Deze software wordt technisch ondersteund door de IT-afdeling:
    - IT installeert een aantal standaard softwareapplicaties op iedere laptop/desktop.
    - Up-to-date houden van werkstations, inclusief standaard software.

Wat je moet doen:

- meld storingen of beveiligingswaarschuwingen aan de IT-helpdesk;
- voer tijdig updates uit wanneer daarom wordt gevraagd;
- lever ongebruikte hardware in bij de IT-dienst;

Specifieke afspraken voor gebruik van AZ Diest-applicaties (bv. mail, Teams) op je privé-apparaten (bv. eigen smartphone,thuis-pc ...):

- Een privé-apparaat gebruiken voor zakelijke doeleinden is toegestaan. Let op, dit is in principe beperkt tot de Outlook-app, Teams-app, KWS Companion-app en de planningstool gelinkt aan het AZ Diest-adres.
- Uitzonderingen zijn mogelijk voor specifieke functies/diensten, die goedgekeurd worden door IT.
- Besteed dan extra aandacht aan het beveiligen van je privé apparaat (bv. schermvergrendeling, pincode, vingerafdruk, ...).

Wat je niet mag doen:

- zelf niet-goedgekeurde software installeren;
- illegale of “gekraakte” software gebruiken op AZ Diest-apparatuur;
- privé-opslagmedia aansluiten op toestellen van AZ Diest zonder toestemming;
- toestellen van AZ Diest uitlenen aan derden (vrienden, familie, externe partijen).

9. Netwerkbeveiliging

Het netwerk van AZ Diest wordt beheerd in samenwerking met UZ Leuven (shared IT). Ongeautoriseerde apparatuur of wijzigingen kunnen de werking en veiligheid ernstig verstoren.

Wat je niet mag doen:

- netwerkbekabeling loskoppelen en niet-AZ Diest-toestellen aansluiten;
- eigen routers, access points of switches installeren;
- hackingactiviteiten uitvoeren of trachten beveiligingsmechanismen te omzeilen.

10. E-mail, internet en artificiële intelligentie (AI)

E-mail, internet en AI zijn krachtige hulpmiddelen. Onzorgvuldig gebruik kan echter leiden tot datalekken, reputatieschade en beveiligingsincidenten.

E-mail en internet:

- gebruik je AZ Diest e-mailadres voor professionele communicatie;
- open bijlagen en links enkel als je de afzender vertrouwt en de context logisch is;
- rapporteer verdachte berichten via de voorziene phishing-knop of aan de IT-helpdesk;
- stuur geen patiënt- of personeelsgegevens naar privé-e-mailadressen;
- gebruik beveiligde kanalen (bijvoorbeeld door AZ Diest of UZ Leuven goedgekeurde oplossingen) voor het delen van gevoelige informatie.

AI-gebruik:

Voor het gebruik van generatieve AI en andere AI-hulpmiddelen geldt aanvullend de procedure “Afspraken rond het gebruik van artificiële intelligentie (AI)” van AZ Diest. Deze procedure definieert toegelaten tools, datacategorieën en randvoorwaarden voor het gebruik van AI.

- gebruik geen publieke AI-tools (zoals algemene versies van ChatGPT, Gemini, enz.) voor gevoelige (categorie 1) of vertrouwelijke (categorie 2) gegevens;
- gebruik enkel door AZ Diest goedgekeurde AI-toepassingen (zoals MS Copilot 365) en volg de daarin opgenomen beperkingen;
- blijf altijd kritisch: je blijft zelf verantwoordelijk voor de inhoud en het gebruik van AI-output.

11. Social media

Medewerkers kunnen via sociale media het imago en de professionaliteit van AZ Diest beïnvloeden. Gebruik sociale media met respect voor discretieplicht, beroepsgeheim en de waarden van AZ Diest.

Wat je moet doen:

- gebruik een respectvolle en professionele toon;
- respecteer je discretieplicht en medisch beroepsgeheim;
- maak duidelijk dat je persoonlijke mening niet noodzakelijk de mening van AZ Diest is.

Wat je niet mag doen:

- vertrouwelijke of patiëntgebonden informatie delen via sociale media;
- interne problemen of conflicten via sociale media aankaarten in plaats van via interne kanalen.

12. Clean desk & screens

Een clean desk & screens-beleid voorkomt dat onbevoegden inzage krijgen in vertrouwelijke informatie.

Wat je moet doen:

- vergrendel je scherm wanneer je je werkpost verlaat;
- sluit toepassingen en documenten af die vertrouwelijke informatie bevatten als je ze niet gebruikt;
- berg papieren met gevoelige informatie op in een afgesloten kast of lade;
- laat geen patiëntlijsten, rapporten of andere gevoelige documenten zichtbaar achter.

13. Melding van beveiligingsincidenten

Incidenten met betrekking tot de beveiliging van IT-middelen, gegevens of gebouwen moeten **onmiddellijk worden gemeld**, rechtstreeks aan de IT-dienst of via de leidinggevende, volgens de interne procedures.

Mogelijke incidenten zijn onder meer:

- (dreigende) uitval of onderbreking van kritieke systemen;
- (vermoeden van) malware, hacking of ongeoorloofde toegang;
- verlies of diefstal van toestellen, badges (sleutels) of gegevensdragers;
- (vermoedelijke) datalekken in de zin van de AVG.

14. Toegang tot persoonlijke gegevens in noodsituaties

Toegang tot persoonlijke gegevens van een gebruiker (zoals mailboxen of persoonlijke netwerkfolders) door andere medewerkers kan enkel in uitzonderlijke gevallen en mits goedkeuring van de daartoe bevoegde directieleden, conform de interne procedure en met respect voor de toepasselijke wetgeving (AVG, CAO nr. 81).

15. Toezicht, logging en handhaving

AZ Diest en UZ Leuven (shared IT) zetten verschillende middelen in om de veiligheid en goede werking van de IT-omgeving te garanderen. Dit omvat onder meer logging van systeem- en netwerkgebeurtenissen, detectie van malware, monitoring van verdachte activiteiten en periodieke controles.

Deze controles gebeuren binnen de grenzen van de toepasselijke wetgeving (onder meer CAO nr. 81 en AVG) en zijn gericht op het voorkomen en detecteren van misbruik, het waarborgen van de continuïteit van de dienstverlening en het voldoen aan de verplichtingen uit de NIS2-wetgeving.

Loggegevens worden gedurende een gepaste termijn bewaard in overeenstemming met de risicoanalyse en de procedures van shared IT en kunnen geraadpleegd worden in het kader van beveiligingsonderzoeken of audits.

Bij inbreuken op deze richtlijnen zijn de tuchtmaatregelen zoals voorzien in het arbeidsreglement van toepassing. Voor personen die geen werknemer zijn van AZ Diest, kan AZ Diest de toegang tot haar systemen beperken of beëindigen en, indien nodig, de samenwerking stopzetten.

Toetsing op niet-toegelaten gebruik:

De onderstaande bepalingen zijn niet limitatief.

- **Verstorend gebruik:**

  het gebruik van de systemen dat een inmenging in het werk van anderen vormt, het ongeautoriseerd verwijderen of wijzigen van andermans bestanden, overdadig gebruik van de systemen of de voedingsbronnen van de systemen, ...

- **Onwettig gebruik:**

  het verkrijgen of onrechtmatig verkrijgen van toegang tot het internet door gebruik te maken van enig toegangscontrolemechanisme dat aan een andere gebruiker toegewezen werd, het beschikbaar stellen van het persoonlijke toegangscontrolemechanisme tot het internet aan personen die niet behoren tot de rechtmatige gebruikersgroep van AZ Diest, zich ongeautoriseerd toegang verschaffen of pogen te verschaffen tot enige computer, computernetwerken, gegevensbestanden, gegevens of elektronisch opgeslagen informatie, het downloaden van het internet en/of het doorsturen via e-mail van illegale software of software afkomstig van een onbetrouwbare bron enz.

- **Aanstootgevende of beledigende gegevens**:

  het verkrijgen, verzenden, opzoeken, weergeven, uitprinten, of anderszins verspreiden van gegevens die redelijkerwijze anderen beledigen, bedreigen of in verlegenheid brengen, of die seksueel expliciet, frauduleus of anderszins ongepast zijn in een professionele omgeving. Het versturen van uitspraken, taal, beelden of andere documenten die redelijkerwijze aanzien worden als beledigend of vernederend voor anderen op basis van

ras, nationaliteit, geslacht, seksuele geaardheid, leeftijd, handicap, religie of politieke overtuiging.

- **Schending van intellectuele eigendom**:

  de gebruikers dienen de bepalingen van de wetgeving inzake intellectuele eigendomsrechten na te leven.

- **Onomzichtig omspringen met gevoelige AZ Diest-gegevens:**

  gegevens kunnen 'openbaar', 'intern', 'vertrouwelijk' of 'strikt persoonlijk en vertrouwelijk' zijn. Bij het e-mailgebruik moet men bovendien rekening houden met het feit dat het e-mailbericht altijd ergens kan bewaard worden, ook na de verwijdering ervan door de gebruiker. De gebruiker dient dan ook de systemen slechts te gebruiken indien deze aangewezen zijn voor de bedoelde communicatie. Zo nodig dient de communicatie op de gepaste manier gelabeld ('vertrouwelijk'...) te worden.

Voor kennisname,

Diest, …… (datum)

Naam medewerker: …….

Handtekening: