

Richtlijn voor externe leveranciers en bouwactiviteiten met impact op het datacenter, de ICT- infrastructuur en ICT-gerelateerde apparatuur

Inhoudsopgave

Versiebeheer	2
1. Doel en toepassingsgebied	2
2. Toegang en toegangsbeheer (datacenter)	3
3. Voorbereiding van de werken	3
4. Gedrag en veiligheid op ICT-gevoelige locaties	3
5. Werken met impact op systemen, energievoorziening of netwerk	4
6. ICT-installaties tijdens bouwfases	4
6.1 Veilig plaatsen van bekabeling	4
7. Afhandeling en evaluatie	4
7.1 Schoonmaak na de werken	5
8. Overtredingen	5

Versiebeheer

Datum	Versie	Auteur	Opmerking
24/04/2025	1.0	Annelore Van Eeghem	Opmaak eerste versie
25/05/2025	2.0	Annelore Van Eeghem	Richtlijnen voor bouwactiviteiten toegevoegd. Richtlijn is niet enkel meer voor datacenter
02/06/2025	3.0	Annelore Van Eeghem	Onderdeel veilig plaatsen van bekabeling toegevoegd en aanpassingen op advies van Nina De Kerpel.
02/09/2025	4.0	Annelore Van Eeghem	Aanpassingen gedaan na overleg met vanuit technisch departement oa onderdeel schoonmaak

1. Doel en toepassingsgebied

Deze richtlijn is van toepassing op alle externe leveranciers die werkzaamheden uitvoeren binnen het ziekenhuis, ongeacht de locatie, en met mogelijke impact op:

- het datacenter,
- de ICT-infrastructuur (bv. bekabeling, netwerksystemen, stroomvoorziening, koeling, enz.),
- en ICT-gerelateerde apparatuur die zich in het ziekenhuis bevindt, zoals pc's, printers, telefoons, camera's, audiovisuele systemen, enz.

Het doel van deze richtlijn is om:

- de beschikbaarheid, integriteit en vertrouwelijkheid van alle ICT-middelen van het ziekenhuis te beschermen,

- risico's tijdens werken en bouwprojecten te beperken,
- en schade of storingen aan ICT-materiaal te voorkomen.

Alle leveranciers zijn verplicht om:

- ICT-apparatuur op hun werklocatie zorgvuldig te beschermen tegen stof, impact of verplaatsing,
- Vooraf af te stemmen met ICT bij risico op impact. Bij bouwwerken en werken aan de noodstroomvoorzieningen zal de leverancier afstemmen met de ATD adjunct of projectingenieur die op dat moment als centraal aanspreekpunt fungeert voor dit type werken, die zorgt dan intern voor de afstemmingen met ICT en de andere ondersteunende diensten.
- Geen nieuw ICT-materiaal te installeren op onbeveiligde of breed toegankelijke plaatsen tijdens de bouwfase, tenzij expliciet goedgekeurd.

2. Toegang en toegangsbeheer (datacenter)

- Toegang tot het datacenter is strikt beperkt tot geautoriseerd personeel.
- Leveranciers vragen minimum 24 uur op voorhand toegang aan via de dienst ICT of de technische dienst, tenzij in noodgevallen.
 - Bij niet-geplande technische activiteiten wordt ICT telefonisch geïnformeerd (03/760.20.20).
 - Technische dienst meldt dit aan ICT via een ticket in de ICT-helpdesk.
- Begeleiding door een medewerker van ICT of technische dienst is verplicht.

3. Voorbereiding van de werken

- Leveranciers bezorgen vooraf een werkplan met:
 - Doel van de interventie
 - Verwachte duur
 - Impact op ICT-infrastructuur of -apparatuur
 - Benodigde apparatuur
- Eventuele risico's voor servers, netwerken, koeling of werkplekapparatuur worden vooraf besproken met ICT.
- Werken in de buurt van ICT-apparatuur (bv. pc's in kantoren, printers in gangen, camera's aan plafonds) vereisen passende beschermingsmaatregelen zoals afdekken, spanningscontrole of tijdelijke afscherming.

4. Gedrag en veiligheid op ICT-gevoelige locaties

- Eten, drinken en roken zijn verboden in het datacenter.
- Er mag geen stof of verontreiniging ontstaan zonder voorafgaande toestemming en maatregelen.
- Persoonlijke beschermingsmiddelen zijn verplicht volgens de aard van de werken.
- Het is verboden om ICT-apparatuur aan te raken, te verplaatsen of los te koppelen zonder toestemming van de ICT-dienst.
- Kabels, aansluitpunten of netwerkapparatuur mogen niet losgemaakt, aangepast of tijdelijk verlegd worden tenzij goedgekeurd.

5. Werken met impact op systemen, energievoorziening of netwerk

- Werken met mogelijke impact op stroomvoorziening, koeling, netwerkverbindingen of ICT-apparatuur worden vooraf afgestemd met ICT.
- Noodmaatregelen of fallback-procedures worden op voorhand besproken.
- Testen van systemen mag alleen na expliciete goedkeuring van ICT.
- Indien tijdelijke ontkoppeling van ICT-apparatuur nodig is, moet dit steeds gemeld en begeleid worden door ICT.

6. ICT-installaties tijdens bouwfases

- Tijdens bouw- en renovatiefases is het niet toegestaan om ICT-apparatuur te installeren op onbeveiligde, publiek toegankelijke of onafgewerkte locaties. Dit omvat o.a.:
 - netwerkcomponenten (bv. switches, access points),
 - camera's, telefoons, badgelezers,
 - pc's, printers, audiovisuele displays.
- Installaties mogen enkel plaatsvinden na formele goedkeuring door ICT.
- Indien apparatuur toch tijdelijk of vroegtijdig aanwezig moet zijn, dienen beschermingsmaatregelen genomen te worden: te bekijken indien van toepassing: afscherming, afsluiting, camerabewaking, enz.
- De ICT-dienst en de dienst Projecten Bouw – technieken bepalen samen het meest opportune moment van installatie per projectfase. De bouwheer draagt pas de verantwoordelijkheid bij voorlopige oplevering van de bouwwerken, voorheen is de aannemer aansprakelijk. Planning wordt door beide partijen samen bepaald, technische diensten zijn SPOC voor coördinatie werken technieken.

6.1 Veilig plaatsen van bekabeling

- In de projectfase moet rekening gehouden worden met het veilig en afgeschermd aanleggen van alle nieuwe bekabeling (data en stroom).
- Bekabeling mag niet op een manier geplaatst worden die fysieke toegang door onbevoegden mogelijk maakt (bv. losliggende kabels, open kabelgoten in publieke zones, toegankelijke patchkasten in onafgewerkte ruimtes).
- De plaatsing van bekabeling dient vooraf afgestemd te worden met de ICT-dienst en waar nodig opgenomen te worden in het werkplan.
- Het is verboden om tijdens bouwwerken op eigen initiatief kabels te trekken of aan te sluiten op het netwerk zonder expliciete goedkeuring van ICT.
- Alle tijdelijke bekabeling moet beveiligd, afgeschermd en duidelijk gemarkeerd worden.
- Inspectie op correcte plaatsing van bekabeling maakt deel uit van de evaluatiefase en kan aanleiding geven tot correctieve maatregelen bij afwijkingen.

7. Afhandeling en evaluatie

- Na afloop wordt een korte rapportage bezorgd met:

- Uitgevoerde werken
 - Incidenten of afwijkingen
 - Openstaande restpunten of opvolging
- De werkomgeving moet in originele staat worden achtergelaten.
- ICT voert indien nodig inspecties uit en bezorgt feedback aan de leverancier of projectverantwoordelijke.

7.1 Schoonmaak na de werken

- Na afronding van de werken dient de volledige werkomgeving schoon en stofvrij te worden opgeleverd.
- Voor datacenters en technische ruimtes is een gespecialiseerde ESD-veilige schoonmaak vereist.
- Standaard schoonmaak is niet toegestaan in deze gevoelige omgevingen zonder voorafgaand overleg met de ICT-dienst.
- De leverancier is verantwoordelijk voor het tijdig inplannen en coördineren van deze schoonmaak met een partij die ervaring heeft met ESD-reiniging.
- De uitvoering van de schoonmaak wordt gecontroleerd door ICT of een aangestelde verantwoordelijke.
- Eventuele kosten verbonden aan het herstel van vervuilde of beschadigde ICT-ruimtes kunnen verhaald worden op de leverancier.

8. Overtredingen

- Overtredingen van deze richtlijn kunnen leiden tot toegangswegering of uitsluiting van verdere samenwerking.
- Ernstige inbreuken worden gemeld aan de ICT-verantwoordelijke en/of technische dienst-verantwoordelijke.
- Schade aan ICT-apparatuur veroorzaakt door nalatigheid kan aanleiding geven tot herstelacties of kostenverrekening.