

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
1. WLAN			
	1	Gebruik van WPA2 encryptie is verplicht. Systemen die worden aanschaf moeten ook WPA3 encryptie ondersteunen.	Netwerkbeheer
	2	Authenticatie op basis van WPA2-Enterprise wordt ondersteunt	Netwerkbeheer
	3	Authenticatie op basis van WPA2-PSK in combinatie met MAC authenticatie wordt ondersteunt	Netwerkbeheer
	4	Het systeem kan zowel op 2,4 als op 5Ghz functioneren binnen het radiospectrum	Netwerkbeheer
	5	Op de 2,4Ghz radio dienen de kanalen 1,6 en 11 te worden ondersteund Op de 5Ghz radio dienen de kanalen 36,40,44,48,100,104,108 en 112 te worden ondersteund	Netwerkbeheer
	6	Het team netwerkbeheer bepaald op welk SSID de apparatuur wordt aangesloten	Netwerkbeheer
	7	I.v.m. strikte security maatregelen levert u de verkeersstromen aan voor het functioneren van de dienst. Deze verkeersstromen worden vertaald naar configuratie van de WLAN firewall zodat communicatie mogelijk is. Als benodigde verkeersstromen niet zijn aangeleverd kan het betreffende apparaat nergens mee communiceren.	Netwerkbeheer
	8	Wanneer het systeem Quality of Service (QoS) nodig heeft zal hiervoor eerst de noodzaak bekend gemaakt worden bij het team netwerkbeheer. Het toestaan hiervan wordt bepaald het team netwerkbeheer	Netwerkbeheer
	9	U levert een lijst aan met de MAC adressen van alle te koppelen systemen voorafgaand aan het koppelen aan het WLAN	Netwerkbeheer
	10	Er vind altijd eerst een test plaats met 1 apparaat per type/soort zodat kan worden vastgesteld dat de werking overeenkomstig is met de eisen van het Erasmus MC alvorens de overige apparaten worden gekoppeld.	Netwerkbeheer
	11	Voor multimedia toepassingen dienen WMM-extenties ondersteunt te worden	Netwerkbeheer
2. Netwerk			
	1	U maakt alleen gebruik van de centrale netwerkkaparaatuur van het Erasmus MC. Levering van eigen netwerkkaparaatuur wordt niet toegestaan.	Netwerkbeheer
	2	Levering van server hardware dient altijd eerst besproken te worden met het team serverbeheer. Waar mogelijk dienen type en merk aan te sluiten bij de hardware standaarden van het Erasmus MC	Netwerkbeheer
	3	Bedrade systemen dienen netwerkauthenticatie (802.1x) te ondersteunen	Netwerkbeheer
	4	Clients ondersteunen het geautomatiseerd (SCEP/ACME) plaatsen van een authenticatie certificaat voor netwerk authenticatie 802.1x. Mocht dit niet worden ondersteund, dan wordt gebruik gemaakt van een vendor certificaat. Uitzondering is Mac Authentication Bypass (MAB) RFC3748	Netwerkbeheer
	5	Elk eindgebruikers apparaat mag slechts worden aangesloten op één netwerk aansluitpunt	Netwerkbeheer
	6	Het wordt niet toegestaan om switches aan te sluiten op netwerkpooorten van het Erasmus MC	
	7	Het te gebruiken netwerk aansluitpunt wordt door ICT Services aangewezen	Netwerkbeheer
	8	De interface van het systeem dient tenminste te voldoen aan IEEE 802.3, 1000Base-TX (1Gb p/s), auto-sensing	Netwerkbeheer
	9	Op alle switchpooorten staat Power over Ethernet ingeschakeld. Het aan te sluiten apparaat kan hier mee omgaan	Netwerkbeheer
	10	Voor de verbinding tussen eindgebruikers apparaat en aansluitpunt wordt één door ICT Services goedgekeurde aansluitkabel gebruikt, met een maximale lengte van 7 meter	Netwerkbeheer
	11	Er mag niet meer dan 1 IP-adres achter 1 MAC adres actief zijn	
4. Datacenter			
	1	Fysieke servers worden geplaatst in de datacenters van ICT Services.	Netwerkbeheer
	2	De datacenters zijn openbaar toegankelijk.	Netwerkbeheer
	3	Toegang tot een datacenter vind altijd plaats onder begeleiding van een Erasmus MC medewerker	Netwerkbeheer
	4	Toegang tot een datacenter dient tenminste 1 dag van tevoren aangevraagd te worden	Netwerkbeheer
	5	U geeft de verwachte benodigde bandbreedte op per component	Netwerkbeheer
	6	Geschikt voor warme-koude straten (eis)	Netwerkbeheer
	7	U geeft vooraf het aantal hoogte eenheden op per systeem	Netwerkbeheer
	8	U geeft de warmtelast op in kW	Netwerkbeheer
	9	U geeft het benodigde type voedingskabel op C13 of C19?	Netwerkbeheer
	10	Erasmus MC monitord alle hardware binnen een monitoringsapplicatie. Hardware dient aangemeld te worden voor monitoring	Netwerkbeheer

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
	11	U geeft op welke poorten en of services gemonitord moeten worden binnen de geleverde dienst.	Serverbeheer
	12	Ieder te plaatsen systeem in het datacenter is voorzien van een geldend supportcontract en dit contract wordt vernieuwd voordat deze is verlopen zolang de hardware binnen het datacenter is ingeschakeld.	Netwerkbeheer
	13	U geeft aan welke bestanden moeten worden meegenomen in de backup zodat in geval van volledige dataloss de dienst volledig kan worden hersteld	Serverbeheer
	14	Wie is contactpersoon (intern (=Erasmus MC, contactpersoon afdeling) en extern (=leverancier)) bij problemen met de server?	Serverbeheer
5. Servers			
	1	Laatste Microsoft Server OS wordt ondersteund	Serverbeheer
	2	Behoudens schriftelijke toestemming van ICT Services is het verboden om serverprogrammatuur voor de volgende infrastructurele diensten te activeren: 1. Domain Name System (DNS) 2. Dynamic Host Configuration Protocol (DHCP) en/of Boot Protocol (BOOTP) 3. Windows Internet Naming Service (WINS) 4. Lightweight Directory Access Protocol (LDAP) 5. Microsoft Active Directory Service (AD)	Serverbeheer
	3	Server systemen hebben tenminste 2 netwerkaansluitingen voor data en 1 netwerkaansluiting voor remote beheer (ILO, DRAC, IPMI, CIMC)	Serverbeheer
	4	Server systemen kunnen de twee data aansluitingen bundelen tot 1 logische data aansluiting via LACP/NIC bonding of active standby.	Serverbeheer
	5	Server systemen hebben tenminste twee voedingen A en B. Server kan operationeel functioneren op 1 voeding.	Serverbeheer
	6	Server systemen zijn voorzien van een 19" rack mounting kit	Serverbeheer
	7	Server systemen hebben een airflow van front naar back	Serverbeheer
	8	Servers worden voorzien van de bij het Erasmus MC in gebruik zijnde anti virus/spam software welke centraal door het Erasmus MC wordt beheert.	Serverbeheer
	9	Het systeem moet als een virtuele appliance op een Vmware omgeving kunnen draaien	Serverbeheer
	10	Middels een centrale management tool beheert door het serverbeheerteam van het Erasmus MC, worden servers op reguliere basis voorzien van patches.	Serverbeheer
6. Security			
	1	Het netwerk van het Erasmus MC is gesegmenteerd in diverse security segmenten. Het team security en netwerkbeheer bepalen in welk netwerksegment het systeem actief mag worden. U levert hiervoor een overzicht aan met benodigde verkeersstromen waaruit blijkt welke verkeersstromen nodig zijn om de dienst te laten functioneren. Hieruit dient ook te blijken welke verkeersstromen nodig zijn voor eventueel remote beheer.	Operationeel Security
	2	Ieder systeem is voorzien van Virus en Malware bescherming. U bespreekt met het team security hoe u deze bescherming per component wenst in te regelen. Afhankelijk van de geboden oplossing kan het Erasmus MC eisen dat u gebruik maakt van de centrale beveiligingssoftware beheert door het team Operationeel Security.	Operationeel Security
	3	Het is niet toegestaan om software te installeren waarmee andere op het Erasmus MC-netwerk aangesloten gebruikers-PC's kunnen worden benaderd, bestuurd en/of gemanipuleerd.	Operationeel Security
	4	Opdrachtnemer meldt beveiligingsincidenten, datalekken en kwetsbaarheden die impact hebben of kunnen hebben op de vertrouwelijkheid, integriteit of beschikbaarheid van de dienst onverwijld en uiterlijk binnen 24 uur na constatering volgens de met Erasmus MC overeengekomen meldprocedure.	Operationeel Security
	5	Opdrachtnemer beschikt over aantoonbare incident-response-, business-continuity- en disaster-recoveryprocedures. Deze procedures worden periodiek getest; bevindingen en verbetermaatregelen worden op verzoek gedeeld met Erasmus MC.	Operationeel Security
	6	Alle geleverde hardware, firmware, besturingssystemen, libraries en applicatiecomponenten bevinden zich gedurende de gebruikperiode binnen een ondersteunde lifecycle en ontvangen beveiligingsupdates.	Operationeel Security
	7	Opdrachtnemer voert aantoonbaar kwetsbaarhedenbeheer uit, inclusief periodieke scans, beoordeling van afhankelijkheden, risicogebaseerde hersteltermijnen en rapportage over openstaande kritieke en hoge kwetsbaarheden.	Operationeel Security

PVE ICT Services

Deelgebied	ID Eis	Verantwoordelijk
	8 Voor internetbereikbare of extern gehoste onderdelen wordt minimaal jaarlijks en na ingrijpende wijzigingen een onafhankelijke penetratietest uitgevoerd. Kritieke en hoge bevindingen worden binnen overeengekomen termijnen opgelost.	Operationeel Security
	9 Software wordt ontwikkeld en onderhouden volgens een Secure Software Development Lifecycle, inclusief secure coding, code review, dependency monitoring, secrets-scanning en beveiligingstesten.	Operationeel Security
	10 Beheer- en gebruikersrechten volgen least privilege en role-based access control. Beheeraccounts zijn persoonsgebonden, gebruiken MFA en worden periodiek beoordeeld.	Operationeel Security
	11 Security- en auditlogs zijn tijdgesynchroniseerd, beschermd tegen wijziging en exporteerbaar naar de door Erasmus MC aangewezen centrale monitoring- of SIEM-voorziening.	Operationeel Security
	12 Data van Erasmus MC, inclusief metadata, prompts en loggegevens, wordt niet gebruikt voor het trainen of verbeteren van AI-modellen zonder voorafgaande expliciete schriftelijke toestemming van Erasmus MC.	Operationeel Security
7. Documentatie		
	1 U levert een functioneel ontwerp aan	Algemeen
	2 U levert een technisch ontwerp aan	Algemeen
	3 U levert een visio of draw.io tekening aan waarin alle IT gerelateerde componenten zijn ingetekend waaruit blijkt wat de samenhang hiertussen is en hoe de dienst technisch in elkaar zit.	Algemeen
	4 U levert een sheet aan met de benodigde verkeersstromen per component van de dienst	Algemeen
	5 U levert een actueel componenten- en afhankelijkhedenoverzicht aan, inclusief gebruikte softwarecomponenten, versies, supportstatus en relevante externe diensten.	Algemeen
	6 U levert beheer-, herstel-, uitwijk-, update- en escalatieprocedures aan en actualiseert deze na relevante wijzigingen.	Algemeen
8. Remote beheer		
	1 Ten behoeve van toegang van buitenaf naar systemen binnen de muren van het Erasmus MC is het verplicht gebruik te maken van de centrale voorzieningen die door ICT Services worden aangeboden en beheerd	Operationeel Security
	2 Het op afstand overnemen van componenten binnen de infrastructuur van het Erasmus MC kan alleen via PAM. Sessies worden opgenomen om bij problemen de rootcause te achterhalen.	Operationeel Security
9. Licenties		
	1 U gebruikt alleen software waarvoor daadwerkelijk een licentieovereenkomst aanwezig is	Algemeen
10. Protocollen		
	1 Systemen maken alleen gebruik van het IP protocol voor toegang tot de logische netwerk-infrastructuur	Netwerkbeheer
	2 Systemen communiceren met elkaar op basis van DNS/FQDN naam. Communicatie op basis van statische IP-nummers is niet toegestaan.	Netwerkbeheer
	3 Multicast is mogelijk maar het team netwerkbeheer bepaald de te configureren adressen in de apparatuur. Als de apparatuur deze flexibiliteit niet ondersteund, is multicast alleen toegestaan in een gesloten netwerkdeel.	Netwerkbeheer
	4 Host naamgeving wordt vooraf bedacht en goedgekeurd door het netwerkteam van Erasmus MC	Netwerkbeheer
	5 Client systemen krijgen geen fixed ip-adres. DHCP geeft dynamische ip-adressen uit.	Netwerkbeheer
	6 Server systemen in de datacenters krijgen een fixed IP-Adres, uitgegeven door het server- of netwerkteam.	Netwerkbeheer
	7 Applicatiesoftware die actief gebruik maakt van IP- en/of Ethernet- broadcast (ARP) is niet toegestaan.	Netwerkbeheer
11. Databases		
	1 Het Erasmus MC is eigenaar van de data welke wordt opgeslagen in database systemen	Databasebeheer
	2 U levert het datamodel van de database aan. Bij updates van de dienst/applicatie levert u een nieuw datamodel aan als deze door de update wijzigt.	Databasebeheer
	3 Alleen een databasebeheerder van het Erasmus MC heeft admin rechten op de database. Installatie van een nieuwe database gebeurt altijd in samenspraak met een databasebeheerder van het Erasmus MC	Databasebeheer
	4 U levert aan op welke tabellen/velden indexen geplaatst dienen te worden om de performance te kunnen garanderen van de applicatie	Databasebeheer

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
	5	Het Erasmus MC hanteert een MS SQL tenzij beleid. U volgt de versies van MS SQL gebruikt door het Erasmus MC. Verder draagt u zorg voor het op tijd geschikt maken van de database zodat bij een update van het databaseplatform de database hiervoor geen belemmering is.	Databasebeheer
	6	U levert een duidelijk overzicht aan van de rechten die benodigd zijn om zowel de applicatie op functioneel vlak te laten opereren alsmede op administratieve vlak	Databasebeheer
	7	U levert een zo duidelijk mogelijk beeld op van de grootte van de database en de gemiddelde toekomstige groei	Databasebeheer
	8	De authenticatie dient in lijn met het Erasmus MC te lopen. dwz gebruik maken van windows authenticatie	Databasebeheer
	9	De database dient in een high available omgeving (Always on) te kunnen draaien	Databasebeheer
12. SAAS			
	1	Authenticatie van (SAAS) applicaties dient altijd via de directory services (on-premises via AD en online via Entra ID) van het Erasmus MC te verlopen. Geen uitzonderingen!	AD beheer
	2	Het Erasmus MC is voor 100% eigenaar van de data opgenomen in de SAAS dienst. Data kan in zijn geheel worden geëxporteerd door een bevoegd Erasmus MC SAAS beheerder	AD beheer
	3	Op verzoek dient de SAAS leverancier binnen 48 uur alle data gestructureerd te kunnen overhandigen aan het Erasmus MC	AD beheer
	4	De applicatie blijft goed presteren ongeacht de groei	AD beheer
	5	De leverancier voldoet aan relevante normen (bijv. ISO 27001, SOC 2, GDPR/AVG)	AD beheer
	6	De responsetijd bij incidenten is 30 min. na digitaal of telefonisch melden van het incident	AD beheer
	7	Oplostijd van een incident is binnen 4 uur	AD beheer
	8	De uptime van de SAAS dienst is 99,98%	AD beheer
	9	De SAAS dienst leverancier maakt eens per week een volledige backup van de data en per dag tenminste 4 incremental backups van de volledige dataset.	AD beheer
	10	Er wordt een test en acceptatie omgeving beschikbaar gesteld. Er kan eenvoudig een kopie gemaakt worden van de productiedata naar een acceptatie/test omgeving	AD beheer
	11	Nieuw uitgebrachte securitypatches van systemen die onderdeel uitmaken van de SAAS dienst worden uiterlijk binnen 48 uur in een vast afgesproken window uitgevoerd	AD beheer
	12	De SAAS leverancier staat audits toe van Erasmus MC medewerkers. Uitkomsten van audits dienen opgevolgd te worden.	AD beheer
	13	Data van en naar de SAAS dienst moet versleuteld zijn (in transit én at rest)	AD beheer
	14	Data wordt opgeslagen binnen de Europese Unie	AD beheer
	15	De SAAS leverancier stelt een portal beschikbaar waarop alle storingen zijn weergegeven van de afgenomen dienst. Deze is ook middels een API te benaderen zodat een storing ook in een centrale monitoringsapplicatie van het Erasmus MC kan worden opgenomen	AD beheer
	16	De Erasmus MC SAAS applicatie beheerder heeft altijd inzage in de logging en audit logging binnen de SAAS dienst. Deze is ook te exporteren in CSV formaat	AD beheer
	17	Alle data is ook middels een API benaderbaar. Zowel lezen als schrijven. De SAAS dienst zorgt zelf voor de integriteit van de data wanneer er gebruik wordt gemaakt van de API.	AD beheer
	18	De leverancier maakt alle ingeschakelde subverwerkers en onderleveranciers inzichtelijk en meldt wijzigingen vooraf volgens de contractueel overeengekomen termijn.	AD beheer
	19	De SaaS-dienst ondersteunt volledige gegevensportabiliteit en exit zonder verlies van gegevens. Export vindt plaats in een gangbaar, open, gedocumenteerd en machineleesbaar formaat, inclusief datamodel en relaties.	AD beheer
	20	API's beschikken over versiebeheer en actuele documentatie. Breaking changes worden vooraf aangekondigd met een overeengekomen overgangsperiode waarin de bestaande versie beschikbaar blijft.	AD beheer
	21	De leverancier meldt geplande wijzigingen die impact kunnen hebben op functionaliteit, integraties, beveiliging of beschikbaarheid vooraf en verstrekt release-informatie en terugvalmogelijkheden.	AD beheer
	22	Bij beëindiging van de dienstverlening worden gegevens na succesvolle overdracht aantoonbaar verwijderd, inclusief kopieën en back-ups, binnen de contractueel overeengekomen termijnen.	AD beheer
13. Desktop			
	1	Desktop MFF: Standaard-Compact formfactor (DM/MFF/Tiny) met Intel Core i3 (desktop, niet-mobiel), 16 GB DDR5, 512 GB NVMe SSD	Desktop Services

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
	2	Desktop SFF: Small Form Factor met Intel Core Ultra 7 of AMD Ryzen 7 Pro, 16 GB DDR5 DIMM, 1 TB NVMe SSD	Desktop Services
	3	Desktop MFF Extra: Compact formfactor (DM/MFF/Tiny) met Intel Core i5 (niet-mobiel) of AMD Ryzen Pro, 16 GB DDR5, 512 GB NVMe SSD	Desktop Services
	4	Hardware Algemeen:	Desktop Services
	5	Er wordt gebruik gemaakt van proven technology (hardware)	Desktop Services
	6	De desktop heeft een roadmap lifecycle van tenminste 12 maanden	Desktop Services
	7	5 jaar gegarandeerde Windows updates op configuratie	Desktop Services
	8	De garantie van 3 jaar Next Busines Day Onsite support inclusief Keep Your Hard Drive Warranty / Defective Media Retention (DMR)	Desktop Services
	9	Er worden test modellen beschikbaar gesteld t.b.v. het testen van o.a. BIOS-instellingen en image	Desktop Services
	10	Prijsvastheid van minimaal 3 maanden maanden na definitieve gunning -	Desktop Services
	11	Enkel producten uit het zakelijke segment mogen aangeboden worden	Desktop Services
	12	Producten worden CO2 neutraal geproduceerd (wens)	Desktop Services
	13	Chassis: MFF/DM/Tiny voor configuraties 1 en 3; SFF voor configuratie 2	Desktop Services
	14	Processor: uitsluitend desktop-variant (niet-mobiel); Intel T-serie toegestaan voor MFF Standaard	Desktop Services
	15	Geheugen: DDR5, bij voorkeur niet-gesoldeerd en uitbreidbaar 24 GB beschikbaar als besteloptie voor MFF; 32 GB aanbevolen voor SFF	Desktop Services
	16	Opslag: NVMe SSD vereist (geen SATA)	Desktop Services
	17	Besturingssysteem: Windows 11 Enterprise, bloatware-vrij, corporate image Zonder Microsoft Office — Windows 11 Pro niet toegestaan	Desktop Services
	18	Image stabiliteit op model en configuratie — midrange of hoger	Desktop Services
	19	Configuratie zonder toetsenbord en muis	Desktop Services
	20	Trusted Platform Module TPM 2.0	Desktop Services
	21	Secure Boot: Black Lotus ready, UEFI CA 2023 compliant; Microsoft Approved BIOS en Firmware (wens)	Desktop Services
	22	vPro / AMD Pro — standaard meeleveren waar beschikbaar in de configuratie (wens)	Desktop Services
	23	NPU: aanbevolen ≥10 TOPS; ≥40 TOPS (Copilot+) is optioneel	Desktop Services
	24	Wi-Fi 6E+ (802.11ax incl. 6 GHz-band), Bluetooth 5.3 of hoger	Desktop Services
	25	Interne speakers	Desktop Services
	26	Aansluitingen (minimaal): 6× USB-A (3.2 Gen 1+), 2× USB-C (3.2 Gen 2+), 2× DisplayPort + 1× HDMI, 1× RJ45 Gigabit, 1× headset-combojack Thunderbolt 4 / USB4 optioneel — geen VGA	Desktop Services
	27	Upgrade optie: meerprijs 5 jaar NBD onsite incl. Keep Your Hard Drive / DMR (basisgarantie 3 jaar NBD onsite is gedekt onder 1.4)	Desktop Services
	14. Laptop		
	1	Notebook 16": Intel Core Ultra 5/7 of AMD Ryzen 5/7 Pro, 32 GB DDR5/LPDDR5x, 1 TB NVMe SSD	Desktop Services
	2	Notebook 14": Intel Core Ultra 5 of AMD Ryzen 5 Pro, 16 GB DDR5/LPDDR5x (24 GB besteloptie), 512 GB NVMe SSD	Desktop Services
	3	Hardware Algemeen:	Desktop Services
	4	Er wordt gebruik gemaakt van proven technology (hardware)	Desktop Services
	5	De notebook heeft een roadmap lifecycle van tenminste 12 maanden	Desktop Services
	6	5 jaar gegarandeerde Windows updates op configuratie	Desktop Services
	7	De garantie van 3 jaar Next Busines Day Onsite support inclusief Keep Your Hard Drive Warranty / Defective Media Retention (DMR)	Desktop Services
	8	Er worden test modellen beschikbaar gesteld t.b.v. het testen van o.a. BIOS-instellingen en image	Desktop Services
	9	Prijsvastheid van minimaal 3 maanden maanden na definitieve gunning -	Desktop Services
	10	Enkel producten uit het zakelijke segment mogen aangeboden worden	Desktop Services
	11	Producten worden CO2 neutraal geproduceerd (Wens)	Desktop Services
	12	Notebook specificaties:	Desktop Services
	13	Processor: desktop Ultra-serie (niet-mobiel H-klasse); AMD Ryzen Pro gelijkwaardig 14": Core Ultra 5 of Ryzen 5 Pro — 16": Core Ultra 5/7 of Ryzen 5/7 Pro	Desktop Services

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
	14	Geheugen: DDR5 of LPDDR5x, bij voorkeur niet-gesoldeerd 14": min. 16 GB (24 GB besteloptie) — 16": min. 32 GB	Desktop Services
	15	Opslag: NVMe SSD vereist (geen SATA) 14": min. 512 GB — 16": min. 1 TB	Desktop Services
	16	Besturingssysteem: Windows 11 Enterprise, bloatware-vrij, corporate image via Dustin Zonder Microsoft Office — Windows 11 Pro niet toegestaan	Desktop Services
	17	Image stabiliteit op model en configuratie — midrange of hoger	Desktop Services
	18	Trusted Platform Module TPM 2.0	Desktop Services
	19	Secure Boot: Black Lotus ready, UEFI CA 2023 compliant; Microsoft Approved BIOS en Firmware	Desktop Services
	20	vPro / AMD Pro — standaard meeleveren waar beschikbaar in de configuratie (Wens)	Desktop Services
	21	NPU: aanbevolen ≥10 TOPS; ≥40 TOPS (Copilot+) is optioneel (wens)	Desktop Services
	22	Verlicht toetsenbord met touchpad	Desktop Services
	23	IR-webcam (RGB + IR) inclusief privacycover — vereist voor Windows Hello	Desktop Services
	24	Vingerafdruklezer geïntegreerd in behuizing of toetsenbord	Desktop Services
	25	Wi-Fi 6E+ (802.11ax incl. 6 GHz-band), Bluetooth 5.3 of hoger	Desktop Services
	26	Beeldscherm: 14" ±0,2" (configuratie 1) / 16" ±0,2" (configuratie 2); min. 250 cd/m ²	Desktop Services
	27	Gewicht (incl. accu, excl. adapter): max. 1,5 kg (14") / max. 2,0 kg (16") (wens)	Desktop Services
	28	Express Charge / snellaadondersteuning	Desktop Services
	29	Aansluitingen (minimaal): 2× USB-C (3.2 Gen 2+), 1× USB-A (3.2 Gen 1+), 1× HDMI of DisplayPort, 1× RJ45 (of dock met RJ45), 1× headset-combojaack Thunderbolt 4 / USB4 aanbevolen — geen VGA	Desktop Services
	30	NFC (contactloze aanmelding) (wens)	Desktop Services
	31	Upgrade optie: meerprijs 5 jaar NBD onsite incl. Keep Your Hard Drive / DMR (basisgarantie 3 jaar NBD onsite is gedekt onder 1.4) (wens)	Desktop Services
15. Monitoren			
	1	Configuratie 1: 24 inch Monitor (24.1) met beeldscherm verhouding 16:10	Desktop Services
	2	Configuratie 2: 24 inch Monitor (23.8) met beeldscherm verhouding 16:9	Desktop Services
	3	Configuratie 3: 24 inch Conference Monitor (23.8) met beeldscherm verhouding 16:9	Desktop Services
	4	Algemeen:	Desktop Services
	5	Er wordt gebruik gemaakt van proven technology (hardware)	Desktop Services
	6	De monitor heeft een roadmap lifecycle van tenminste 12 maanden	Desktop Services
	7	De garantie van 3 jaar Exchange service	Desktop Services
	8	Er worden demo modellen ter beschikking gesteld die exact gelijk zijn aan het aangeboden model	Desktop Services
	9	Prijsvastheid van minimaal 3 maanden maanden na definitieve gunning -	Desktop Services
	10	Producten worden CO2 neutraal geproduceerd (wens)	Desktop Services
	11	Monitor 1 & 2 specificaties:	Desktop Services
	12	Weergave positieaanpassingen : Hoogte,as (draaiend),draaibaar,tilt	Desktop Services
	13	Paneeltype IPS - Responstijd 8 ms of sneller	Desktop Services
	14	VESA-montageverbinding - 100 x 100 mm	Desktop Services
	15	Monitor inclusief statief/voet in 1 verpakking	Desktop Services
	16	Inclusief aansluitkabels : 1 x HDMI-kabel - 1.8 m - 1 x DisplayPort 1.2-kabel - 1.8 m 1 x USB-B naar USB-A-kabel - 1.8 m	Desktop Services
	17	Meerprijs voor 5 jaar Exchange service (wens)	Desktop Services
	18	Aansluitingen :	Desktop Services
	19	DisplayPort 1.2, HDMI, 3 x USB 3.2 Gen 1 downstream 1 x USB 3.2 Gen 1 upstream	Desktop Services
	20	Monitor 3 specificaties:	Desktop Services
	21	Weergave positieaanpassingen : Hoogte,as (draaiend),draaibaar,tilt	Desktop Services
	22	Paneeltype IPS - Responstijd 8 ms of sneller	Desktop Services
	23	VESA-montageverbinding - 100 x 100 mm	Desktop Services
	24	Monitor inclusief statief/voet	Desktop Services
	25	5,0 megapixel camera IR-camera	Desktop Services
	26	Meerprijs voor 5 jaar Exchange service (wens)	Desktop Services
	27	Luidsprekers - stereo 3 watt of meer	Desktop Services
	28	Inclusief aansluitkabels : 1 x DisplayPort 1.2-kabel - 1.8 m 1 x USB-B naar USB-C-kabel - 1.8 m - USB 3.2 Gen 1-upstreamkabel - 1.8 m	Desktop Services
	29	Aansluitingen :	Desktop Services

PVE ICT Services

Deelgebied	ID	Eis	Verantwoordelijk
	30	DisplayPort 1.2 DisplayPort 1.2-uitgang HDMI USB-C/DisplayPort 1.2 Alt Mode 3 x USB 3.2 Gen 1 downstream) Audio-uitgang (3,5mm jack) LAN (RJ-45)	Desktop Services
16. Cloud			
	1	Primaire Public Cloud Provider: Microsoft Azure is de primaire public cloud provider van Erasmus MC.	CCoE
	2	Infrastructure as Code & CI/CD: Alle productie en acceptatie cloud infrastructuur wordt middels Infrastructure as Code (IaC) vastgelegd en uitgerold volgens CI/CD pipelines. Voor productie workloads mag beheer en uitrol niet via GUI of portals gedaan worden.	CCoE
	3	IaC Repositories: Repositories met IaC zijn verplicht zodat er ook versiebeheer is.	CCoE
	4	Service Prioritering: SaaS > PaaS > IaaS. Waar mogelijk wordt SaaS gebruikt, anders PaaS diensten en in laatste geval IaaS diensten.	CCoE
	5	DTAP Omgevingen: Elke workload dient minimaal twee omgevingen (Development, Testing, Acceptance, Production) te hebben.	CCoE
	6	BIV Classificatie: Elke workload dient een BIV classificatie te hebben, bepaald door onze ISOs.	CCoE
	7	Exit Strategie: Elke workload in cloud heeft een (minimale) exit strategie beschreven.	CCoE
	8	Technisch Ontwerp & RACI: Elke workload met productiestatus dient een Technisch Ontwerp en een RACI matrix te hebben voordat deze in productie gaat.	CCoE
	9	Microsoft Cloud Adoption Framework: Erasmus MC volgt de best practices zoals beschreven in het Microsoft Cloud Adoption Framework; de Landing Zone is hierop ingericht.	CCoE
	10	Workload Lifecycle Management: Van IaC tot applicatiecode is update management en versiebeheer van belang, inclusief tijdig decommissioning van retired componenten.	CCoE
	11	Verantwoordelijkheden: De workload owner is verantwoordelijk voor het technisch en functioneel beheer van de applicatie. Het Cloud Center of Excellence (CCoE) is verantwoordelijk voor de gedeelde infrastructuur in de Landing Zone.	CCoE
	12	Kosten doorbelasting: alle kosten van de workload worden doorbelast naar een kostenplaats of project code. Kosten van gedeelde infrastructuur (zoals netwerk bandbreedte gebruik en firewalls) zullen naar rato worden doorbelast.	CCoE
	13	Alle cloudresources worden voorzien van de verplichte tags voor eigenaar, workload, omgeving, BIV-classificatie, kostenplaats of projectcode en lifecycle-status.	CCoE
	14	Secrets, certificaten en sleutels worden opgeslagen in een door Erasmus MC goedgekeurde secrets- of key-managementvoorziening en worden niet opgenomen in broncode, configuratiebestanden of pipeline-logs.	CCoE
	15	Cloudworkloads gebruiken centrale identity- en toegangsvoorzieningen, least privilege, MFA voor beheer en periodieke beoordeling van geprivilegieerde rechten.	CCoE
	16	Platform-, security- en auditlogging wordt aangesloten op centrale monitoring. Voor de workload zijn alarmering, opvolging, tijdsynchronisatie en bewaartermijnen vastgelegd.	CCoE
	17	Voor iedere productie-workload zijn hersteldoelen, back-upbeleid, herstelprocedure en periodieke hersteltest vastgelegd en afgestemd op de BIV-classificatie.	CCoE