Bijlage 11 - Technische en Beveiligingsspecificatie – Netwerkvereisten voor Repro diensten

Doel en toepassingsgebied

Deze specificatie beschrijft de technische en beveiligingsvereisten voor de aansluiting van printing diensten van de opdrachtnemer (hierna: *Repro*) op het netwerk van de VU.

De bepalingen zijn van toepassing op print en apparatuur (pc's/printer(s)/devices) die tijdens de uitvoering van de opdracht worden ingezet, ongeacht of deze tijdelijk of permanent worden geplaatst.

Netwerkarchitectuur en segmentatie

- De Repro sluit zijn print diensten en services uitsluitend aan op een door de VU toegewezen, gesegmenteerd netwerk (Repro VLAN).
- Dit Repro VLAN is volledig gescheiden van bedrijfs-, beheer- en gastnetwerken, zowel logisch als fysiek. (Ook onderling binnen dit VLAN gescheiden middels Software Defined Access (SDA) netwerk)
- Er is uitsluitend uitgaand netwerkverkeer toegestaan richting het Internet en/of Cloud diensten van de Repro. Inkomend verkeer wordt door de VU geblokkeerd.
- De Repro levert uiterlijk zeven (7) kalenderdagen voor ingebruikname een overzicht aan met:

    - Device-type en merk/model van de terminals;
    - MAC-adressen van alle apparaten;
    - Eventuele vereiste externe IP-adressen of Cloud en/of domeinnamen van de Repro.
    -

IP-adressering en netwerkbeheer

- Apparaten verkrijgen hun IP-adres via DHCP.
- MAC-adressen moeten van te voren worden aangeleverd ten bate van registratie.
- Indien vereist, kan de VU DHCP-reservaties instellen op basis van aangeleverde MAC-adressen.
- De bedrade netwerkinterfaces dienen te functioneren op basis van DHCP-adresconfiguratie en automatische snelheids- en duplexdetectie (auto-negotiation), met een maximale bandbreedte van 1 Gbps (Gigabits Ethernet).
- Statische IP-configuraties zijn uitsluitend toegestaan na voorafgaande schriftelijke goedkeuring van de VU. (Sterk afgeraden)

- De Repro dient eventuele netwerkverkeersproblemen te melden via de aangewezen ICT-servicedesk van de VU.

De VU is voornemens de bestaande MAC-gebaseerde netwerk-authenticatie te vervangen door een certificaat-gebaseerde authenticatieoplossing (802.1X/EAP-TLS).

De opdrachtnemer (Repro dienst) werkt actief mee aan deze wijziging door:

- het beschikbaar stellen van de gebruikte netwerkapparatuur (pinautomaat) voor test- en registratieactiviteiten;
- het verlenen van toegang voor het installeren of registreren van benodigde netwerkcertificaten;
- het afstemmen van een geschikt tijdsvenster waarin de wijziging kan worden uitgevoerd zonder verstoring van operationele processen.

De VU waarborgt dat de wijziging in overleg plaatsvindt en dat de continuïteit van de dienstverlening van de opdrachtnemer tijdens de overgangsfase behouden blijft.

Beveiliging en compliance

- Alle pinautomaten dienen aantoonbaar PCI-DSS compliant te zijn.
- Er mag geen opslag van kaart- of transactiegegevens plaatsvinden op pinautomaten, lokale terminals, of randapparatuur binnen het netwerk van de VU.
- Alle communicatie tussen pinautomaat en acquirer dient end-to-end versleuteld plaats te vinden via min TLS 1.2 of hoger.
- De Repro/Print apparatuur mag geen gebruik maken van draadloze communicatieprotocollen, waaronder (maar niet beperkt tot) Wi-Fi en Bluetooth. Alle netwerkverbindingen dienen uitsluitend bekabeld te worden gerealiseerd. (Het is uitdrukkelijk niet toegestaan dat repro leveranciers of onderaannemers eigen netwerkapparatuur, waaronder (maar niet beperkt tot) routers, switches, access points of vergelijkbare netwerkcomponenten, meenemen, aansluiten of in gebruik nemen binnen het campus netwerk.
- Apparaten moeten gebruikmaken van up-to-date firmware en beveiligingspatches op het moment van aansluiting.
- De VU behoudt zich het recht voor netwerkverkeer op het “Repro” VLAN te monitoren, isoleren of blokkeren in geval van afwijkend of verdacht gedrag, conform het interne beveiligingsbeleid.
- De Repro is verantwoordelijk voor het naleven en up to date houden van relevante privacy- en beveiligingswetgeving, waaronder de AVG, NIS2, en PCI-DSS.

Onderhoud, beheer en incidentafhandeling

- De Repro meldt beveiligingsincidenten of verbindingsstoringen **onverwijld** bij de VU.

- Tijdens evenementen of operationele periodes dient een contactpersoon van de Repro bereikbaar te zijn voor technische afstemming.
- Wijzigingen aan de netwerkconfiguratie of het toevoegen van extra apparatuur dienen vooraf te worden goedgekeurd door de opdrachtgever.

Samenvattende technische parameters

Parameter	Specificatie
Toegangstype	Bedraad (Ethernet) (Wi-Fi niet toegestaan)
Netwerksegment	Gescheiden VLANs (Repro VLAN/Pin VLAN)
IP-adressering	DHCP (gereserveerd)
Verkeer	Alleen uitgaand HTTPS (TCP 443)
Encryptie	TLS 1.2 of hoger
Protocol	IPv4, DNS vereist
Monitoring	In overleg
Compliance	