1 Inleiding en doel

Dit Programma van Eisen (PvE) legt de beveiligings-, informatiebeveiligings- en privacy-eisen vast waaraan multifunctionele printers (MFP's) en de bijbehorende beheeromgeving moeten voldoen bij aanschaf via lease voor KNAW en haar instituten. Een MFP is functioneel een netwerkcomputer met een besturingssysteem, interne opslag en meerdere netwerkdiensten. Het aanvalsoppervlak is daardoor groter dan bij een klassiek randapparaat, en het apparaat verwerkt structureel persoonsgegevens (adresboeken, scan-to-*, printlogs). De eisen in dit document waarborgen dat de MFP-fleet passend beveiligd is en aantoonbaar voldoet aan de AVG en aan het KNAW-informatiebeveiligingsbeleid.

Elke eis is voorzien van een verwijzing naar de relevante maatregel uit ISO/IEC 27001:2022 Annex A, zodat de eisen herleidbaar zijn naar het ISMS en bruikbaar in de leveranciersselectie en contractvorming.

2 Uitgangspunten en scope

De volgende uitgangspunten zijn kaderstellend en vertaald in de eisen verderop:

- Fleet-levering: meerdere MFP's, centraal te beheren als één beheerde vloot.
- Contractvorm: lease. De end-of-life-fase (retour van apparatuur met opslagmedia) is daardoor een expliciet en zwaarwegend beveiligingsaspect.
- Geen cloud: printbeheer en jobverwerking lopen via Papercut binnen het KNAW-netwerk. Externe cloud-printdiensten en vendor-portalen zijn niet toegestaan, tenzij separaat en aantoonbaar AVG-conform gecontracteerd.
- Federatieve context: de fleet bedient het centrale bureau en semi-autonome instituten; beheer en identiteiten sluiten aan op de bestaande KNAW-IAM (Entra ID).

3 Eisen

3.1 Apparaat-hardening en firmware

ID	Eis	ISO 27001:2022
HD-01	Standaard beheerderswachtwoorden zijn wijzigbaar en worden bij inrichting gewijzigd; per apparaat een sterk, uniek credential.	A.8.9, A.5.17
HD-02	Ongebruikte protocollen en diensten zijn uitschakelbaar (o.a. Telnet, FTP, SNMPv1/v2c, raw poort 9100, WSD, SMBv1, mDNS/Bonjour).	A.8.9, A.8.20
HD-03	Het apparaat ondersteunt secure/verified boot en uitsluitend digitaal gesigneerde firmware.	A.8.9, A.8.19
HD-04	De leverancier zegt tijdige security-updates toe en publiceert support- en end-of-life-datum van elk model.	A.8.8, A.5.20

3.2 Authenticatie, toegang en secure release (follow-me)

ID	Eis	ISO 27001:2022
AC-01	Gebruikersauthenticatie is verplicht vóór printen, kopiëren en scannen (badge/PIN en/of Entra ID).	A.8.5, A.8.3
AC-02	Secure release / follow-me: printjobs worden centraal vastgehouden en pas na authenticatie aan het apparaat vrijgegeven.	A.8.3, A.5.14
AC-03	Koppeling aan de KNAW-identiteitsvoorziening (Entra ID / LDAP); geen beheer op losse lokale accounts.	A.8.5, A.5.16
AC-04	Rolgebaseerd beheer met gescheiden, geprivilegieerd beheeraccount; geen gedeelde admin-credentials.	A.8.2
AC-05	Vastgehouden jobs worden na een instelbare bewaartermijn automatisch verwijderd indien niet vrijgegeven.	A.8.10, A.5.14

3.3 Netwerkbeveiliging

ID	Eis	ISO 27001:2022
NW-01	Het apparaat ondersteunt 802.1X poortauthenticatie en plaatsing in een apart printer-VLAN.	A.8.20, A.8.22
NW-02	Alle beheer- en printprotocollen zijn versleuteld (HTTPS-beheerinterface, IPPS); ondersteuning voor TLS 1.2 of hoger.	A.8.24, A.8.21
NW-03	Geen inkomende verbindingen vanuit internet; het apparaat is uitsluitend intern bereikbaar.	A.8.20, A.8.22

3.4 Gegevensbescherming en privacy (AVG)

ID	Eis	ISO 27001:2022
DP-01	De interne opslag (HDD/SSD) is versleuteld (AES-256).	A.8.24
DP-02	Jobdata wordt na verwerking direct en veilig gewist (image overwrite / secure erase).	A.8.10
DP-03	Adresboeken, scan-to-email-instellingen en logs zijn onderhevig aan dataminimalisatie en instelbare bewaartermijnen.	A.5.34, A.8.10
DP-04	Scan-to-* verloopt uitsluitend over versleutelde kanalen naar interne bestemmingen; geen doorzending naar externe partijen.	A.5.14, A.8.24
DP-05	Indien enige verwerkersrol bij de leverancier ontstaat: verwerkersovereenkomst, EU-hosting en toetsing op CLOUD Act-jurisdictie.	A.5.23, A.5.20

3.5 Lokale printserver (on-premise beheeromgeving)

ID	Eis	ISO 27001:2022
PS-01	De print-/releaseoplossing draait volledig on-premise binnen het KNAW-netwerk; geen afhankelijkheid van een externe cloud-tenant.	A.5.23, A.8.20
PS-02	De serversoftware ondersteunt gehardende Windows Server / Linux en integreert met Entra ID/AD voor authenticatie.	A.8.9, A.8.5
PS-03	Communicatie tussen printserver, apparaten en clients is end-to-end versleuteld.	A.8.24
PS-04	De printserver levert auditlogs en exporteert deze naar de KNAW-SIEM (Wazuh/Sentinel) via syslog.	A.8.15, A.8.16
PS-05	Rolgescheiden beheer op de printserver; wijzigingen zijn herleidbaar tot een persoon.	A.8.2, A.8.15

3.6 Logging en monitoring

ID	Eis	ISO 27001:2022
LM-01	Het apparaat en de printserver loggen gebruik (wie, wat, wanneer) en beheerhandelingen.	A.8.15
LM-02	Logs zijn exporteerbaar naar de KNAW-SIEM (Wazuh/Microsoft Sentinel) via syslog of gelijkwaardig.	A.8.16

3.7 Fysiek en end-of-life (lease-retour)

ID	Eis	ISO 27001:2022
EOL-01	Bij retour/vervanging garandeert de leverancier aantoonbare, onomkeerbare wissing of vernietiging van alle opslagmedia, met schriftelijk bewijs (certificaat van wissing/vernietiging).	A.7.14, A.7.10

3.8 Leverancier en supply chain

ID	Eis	ISO 27001:2022
SC-01	De leverancier wordt beoordeeld via de KNAW Vendor Risk Assessment (CIAp-methodiek) vóór gunning.	A.5.19, A.5.21
SC-02	Beveiligingseisen, meldplicht bij incidenten en verwerkersafspraken zijn contractueel vastgelegd.	A.5.20, A.5.19

ID	Eis	ISO 27001:2022
SC-03	De leverancier levert een gedocumenteerd firmware-/updatebeleid en incidenthistorie aan.	A.8.8, A.5.21
SC-04	Onderaannemers en hostingpartijen in de keten zijn inzichtelijk en beoordeeld.	A.5.21, A.5.23

4 Lease-specifieke contractuele eisen

Naast de technische eisen worden de volgende punten contractueel geborgd, omdat lease het beheer over de volledige levenscyclus deelt met de leverancier:

ID	Eis
LE-01	Aantoonbare data-sanitisatie bij elke apparaatwissel én bij einde lease (koppeling aan EOL-01), inclusief bewijsvoering per serienummer.
LE-02	Meldplicht bij beveiligingsincidenten binnen een vastgelegde termijn, afgestemd op de KNAW NIS2-/Cbw-verplichtingen.
LE-03	Onafhankelijke assurance (bijv. ISAE 3402 / SOC 2) is beschikbaar voor beheerde dienstcomponenten.
LE-04	Recht op audit of op aanlevering van assurance-rapportages gedurende de looptijd.
LE-05	Toezegging op firmware-ondersteuning voor de volledige leaseperiode; geen apparatuur die tijdens de looptijd end-of-life gaat zonder patchpad.

Bijlage A ISO/IEC 27001:2022 Annex A — verwijzingenoverzicht

Onderstaand overzicht koppelt de gebruikte Annex A-maatregelen aan de eisdomeinen in dit PvE.

Annex A	Maatregel	Toegepast in
A.5.9	Inventaris van informatie en andere geassocieerde activa	3.7 (asset-registratie MFP)
A.5.14	Informatieoverdracht	3.2 / 3.4 (scan-to-*, secure release)
A.5.16	Identiteitsbeheer	3.2 (IAM-koppeling)
A.5.17	Authenticatie-informatie	3.1 (credentials)
A.5.19–A.5.21	Leveranciersrelaties / eisen in overeenkomsten / ICT-toeleveringsketen	3.8 / 4 / 5
A.5.22	Monitoring van leveranciersdiensten	4 (assurance)
A.5.23	Informatiebeveiliging bij cloudgebruik	2 / 3.4 / 3.5 (geen cloud)
A.5.29	Informatiebeveiliging tijdens verstoring	3.5 (continuïteit printserver)
A.5.34	Privacy en bescherming van persoonsgegevens	3.4 (AVG)
A.7.8 / A.7.10 / A.7.14	Plaatsing en bescherming / opslagmedia / veilig verwijderen apparatuur	3.7 (fysiek, EOL)
A.8.2 / A.8.3 / A.8.5	Geprivilegieerde toegang / toegangsbeperking / veilige authenticatie	3.2 / 3.5
A.8.7	Bescherming tegen malware	3.1
A.8.8	Beheer van technische kwetsbaarheden	3.1 / 3.8
A.8.9	Configuratiebeheer (hardening)	3.1 / 3.5
A.8.10	Informatieverwijdering	3.2 / 3.4
A.8.13	Back-up van informatie	3.5
A.8.15 / A.8.16	Logging / monitoring	3.5 / 3.6
A.8.19	Installatie van software op operationele systemen	3.1 (firmware)
A.8.20 / A.8.21 / A.8.22	Netwerkbeveiliging / netwerkdiensten / segregatie	3.3 / 3.5
A.8.24	Gebruik van cryptografie	3.3 / 3.4 / 3.5

Toelichting: de nummering volgt ISO/IEC 27001:2022, Annex A. Maatregelomschrijvingen zijn verkort weergegeven.