Bijlage 17 – Notatie domeinen Netwerk & beheer

Notatie van domeinen voor leveranciers om aantoonbaar te voldoen aan het Normenkader IBP voor het Funderend Onderwijs.

Versie:	1.0
Perceel:	Basis
TLP:	**GREEN:** openbaar inzichtelijk, maar alleen te gebruiken binnen het kader van deelname aan de aanbesteding.

Inleiding

Schoolbesturen binnen het Funderend Onderwijs (FO) moeten uiterlijk eind 2027 voldoen aan alle 22 domeinen van het Normenkader Informatiebeveiliging en Privacy (IBP) FO. Dit normenkader omvat 15 domeinen voor informatiebeveiliging en 7 domeinen voor privacy.

voor Netwerk & beheer-dienstverlening is het van belang dat schoolbesturen inzicht krijgen in de normen waarop deze dienstverlening hen kan ondersteunen. Vanuit de behoefte van het funderend onderwijs onderzoekt SIVON hoe Netwerk & beheer kan bijdragen aan zowel een veiligere organisatie als het (gedeeltelijk) voldoen aan specifieke normen binnen het Normenkader IBP.

Deze notatie van domeinen biedt Netwerk & beheer leveranciers inzage in de domeinen waaraan zij middels de dienstverlening Netwerk & beheer kunnen bijdragen aan de naleving van onderliggende normen. Deze is nu als concept bedoeld om leveranciers een beeld te geven van de raakvlakken die SIVON ziet tussen de dienstverlening van Netwerk & beheer en het Normenkader IBP-FO. Gedurende de looptijd van de raamovereenkomsten zal SIVON deze notatie van domeinen specificeren naar een selfassessment op norm-niveau waarbij de leverancier kan toelichten hoe het schoolbestuur wordt ondersteund om geheel of gedeeltelijk aan de norm te voldoen. Het resultaat is een conclusie waarin zichtbaar wordt of naleving volledig, gedeeltelijk of niet haalbaar is met behulp van de betreffende dienstverlening.

Legenda	
Blauw	Leverancier kan invulling geven aan de normen notatie t.b.v. de dienstverlening die hij direct aanbiedt aan scholen.
Roze	Kan leverancier indirect aan bijdrage maar de normen notatie kan leverancier hier niet voor invullen.
Oranje	Domein is niet van toepassing voor leverancier en/of schoolbestuur

Domeinen notatie Normenkader IBP – Netwerk & beheer

Schoolbestuur – zelf in te regelen	Leverancier – (in)directe bijdrage van dienst aan scholen	Leverancier – intern op orde
Onderdeel: Informatiebeveiliging		
(IB) Domein 1: Bestuur		
IBP-beleid en roadmap vaststellen, rollen/mandaten, risicobereidheid en toezicht.	Adviseert en levert aantoonbaarheid (rapportages/meetwaarden) die bestuur helpt bij sturing en verantwoording (SLA/KPI's).	ISMS/beleid en governance volgens ISO 27001 of gelijkwaardig; naleving IBP-FO contractueel geborgd.
(IB) Domein 2: Organisatie		
Rollen (IBP, FG, proceseigenaren), bevoegdheden, bewustwording/gedrag, meldproces datalekken.	Levert heldere RASCI/overlegstructuur en operationele rapportages vanuit beheer/monitoring.	Rollen en rechten op de juiste wijze documenteert en geïmplementeerd in het kader van de dienstverlening aan klanten.
(IB) Domein 3: Risicomanagement		
Periodieke risicoanalyse en prioriteiten op onderwijsprocessen.	Levert input (capacity/performance & security-rapportages) om risico's op netwerkgebied te beoordelen.	Eigen risicomanagement, inclusief processen, op de dienstverlening. Aantoonbaar gedocumenteerd met BIV afwegingen per onderdeel.
(IB) Domein 4: Personeelsbeheer		
VOG/proces voor screening, onboarding inc. toegang tot systemen/apps voor (nieuwe) medewerkers, gedragscode, awareness.	Ondersteunt met leesrechten/portals en eenvoudige procedures voor meldingen en changes.	Personeelsscreening/VOG waar gevraagd, geheimhouding en security-awareness.
(IB) Domein 5: Configuratiemanagement		
Device management en inrichting hiervan in een CMDB. Indien uitbesteed procedure voor device- management afstemmen met leverancier.	CMDB/asset-registratie, baselines en change-logging;	Eigen CMDB/versiebeheer en gecontroleerde uitrolprocessen.
(IB) Domein 6: Incidentmanagement		
Interne melding/registratie voor zowel IB als P, coördinatie met Security Officer, FG/AP incl. evaluaties.	Monitoring binnen supportvenster, incidentdetectie en melding, inclusief incidentrapportages.	Eigen incident- en problemmanagement.
(IB) Domein 7: Changemanagement		

Besluitvorming over changes met onderwijsimpact; onderhoudsvensters afstemmen.	Formeel wijzigingsproces, test/acceptatie, terugvalplan; onderhoud buiten lestijden en tijdig aangekondigd.	Eigen change-proces met segregatie van omgevingen en kwaliteitsborging.
(IB) Domein 8: Softwareontwikkeling		
(Meestal beperkt bij PO/VO) eisen stellen aan leveranciers/saas; security & privacy by design.	Niet van toepassing.	Eigen systeemontwikkelingtoetsing i.v.t.
(IB) Domein 9: Datamanagement		
Data-eigenaren, data, systeem en document classificatie, bewaartermijnen, back-upbeleid.	Actueel overzicht van netwerkcomponenten (o.a. MAC-adressen) in portaal / CMDB en rapportages over capaciteit en gebruik.	Eigen documentatie/ bewaartijden; veilige opslag en gecontroleerde toegang tot klantgegevens. Classificatie van data, documenten en systemen.
(IB) Domein 10: Identity- en Accessmanagement		
Autorisatiematrix/rollen voor eigen apps; goedkeuringen; IST/SOLL-controles.	Standaard dienstverlening: Basis toegangsbeheer per gebruikersgroep met 2FA voor beheeraccounts. Aanvullende dienstverlening: Directory-koppeling met rolgebaseerde rechten, traceerbaarheid en IST/SOLL-rapportages.	IAM intern: rolgebaseerde toegang, superuser-beheer en noodprocedure.
(IB) Domein 11: Securitymanagement		
Beveiligingsbeleid en -eisen richting leverancier; toezicht op naleving. Op orde hebben van een securitybaseline. Indien uitbesteedt opstellen, refereren en verwijzen naar proces met leverancier. Onderdeel van NaaS.	(Netwerk)segmentatie (VLAN), monitoring, patching & CVSS-termijnen; beschikbaarheid en onderhoudseisen.	Eigen patch/threat- & vuln-management, logging en hardening conform norm. Aantoonbaar maken van security-maatregelen van NaaS oplossing richting aangesloten schoolbesturen.
(IB) Domein 12: Fysieke beveiliging		
Toegang server/patchruimtes, sleutelbeheer, bezoekers/uitgifte.	Fysieke toegangscontrole ligt bij school.	Fysieke beveiliging eigen locaties/datacenters/magazijnen.
(IB) Domein 13: IT-operatie		
Regie op eerstelijns ondersteuning; afspraken met ketenpartijen.	2e/3e-lijns support, pro-actieve monitoring, duidelijke escalatiepaden en KPI's (SLA).	Operationele capaciteit, serviceproces en tooling op volwassen niveau.

(IB) Domein 14: Bedrijfscontinuïteitsmanagement		
BC/onderwijscontinuïteit; kritieke processen en fallback-maatregelen.	Continuïteit van netwerkdiensten (SLA, onderhoudsvensters, herstel), configuratie-back-ups.	Eigen BC-plannen voor dienstverlening aan scholen.
(IB) Domein 15: Ketenbeheer		
Contract- & leveranciersmanagement (SIVON, infra-/cloud-/app-leveranciers).	Aanleveren SLR's op verzoek SIVON.	Beheer onderaannemers (toestemming/controle) ivt, audits.
Onderdeel: Privacy		
(P) Domein 1: Beleid		
Privacybeleid opstellen en vaststellen; verantwoordelijkheden (FG, bestuur, proceseigenaren) en doelen voor gegevensbescherming vastleggen.	Geeft inzicht in aard, omvang en locatie van netwerkverkeer en logdata; ondersteunt bij afspraken over dataverwerking, opslag en toegang	Heeft eigen privacybeleid en verwerkingsregister conform AVG; borgt naleving via DPIA's en jaarlijkse evaluatie.
(P) Domein 2: Processen		
Procedures voor verwerking van persoonsgegevens, meldingen van datalekken, en DPIA's waar nodig.	Levert beschrijving van verwerkingen binnen Netwerk & Beheer (beheer, monitoring, authenticatie); levert input voor verwerkingsregister of DPIA; geeft bewaartermijnen van logdata.	Interne processen voor incidentafhandeling, datalekken en DPIA's aantoonbaar ingericht; logt alle privacy-incidenten.
(P) Domein 3: Organisatorische inbedding		
Functionaris Gegevensbescherming (FG) aangewezen; verantwoordelijkheden belegd in organisatie en beleid geborgd.	Verwerkt persoonsgegevens uitsluitend binnen overeengekomen doeleinden; gebruikt subverwerkers alleen met toestemming van SIVON/opdrachtgever	Privacy Officer en Security Officer zijn formeel belegd; verantwoordelijkheden vastgelegd in governance-structuur incl. privacyoverleggen i.h.k.v. NaaS dienstverlening.
(P) Domein 4: Rechten van betrokkenen		
Procedures inrichten voor inzage-, correctie-, verwijderings- en bezwaarverzoeken.	Biedt traceerbare logs en toegangsrapportages; verwijdert gebruikers- en loggegevens bij beëindiging van de dienstverlening conform exitprocedure.	Waarborgt dat medewerkers en systemen verzoeken van betrokkenen correct en tijdig afhandelen; naleving vastgelegd in interne procedure.
(P) Domein 5: Verantwoording		
Verwerkingsregister bijhouden; kunnen aantonen dat verwerking rechtmatig en zorgvuldig gebeurt.	Borgt AVG-rollen in verwerkersovereenkomst, levert overzicht subverwerkers, voorwaarden voor	Houdt intern een volledig verwerkingsregister bij; rapporteert wijzigingen in subverwerkers vooraf.

	gegevensverstrekking en informatie over doorgifte buiten EER (met waarborgen).	
(P) Domein 6: Beveiliging		
Technische en organisatorische maatregelen treffen voor persoonsgegevens, in lijn met informatiebeveiligingsbeleid.	Implementeert beveiligingsmaatregelen in ontwerp van netwerkdiensten: encryptie, 2FA voor beheeraccounts, logging van wijzigingen, scheiding van netwerken en opslag uitsluitend binnen EU	Voldoet aan eigen security- en privacybeleid (ISO 27001 / NEN 7510); voert jaarlijkse interne audit en pentest uit.
(P) Domein 7: Verantwoording		
Interne audits uitvoeren; toezien op naleving van privacybeleid en bijsturen waar nodig.	Ondersteunt audits door technische informatie, configuratierapportages en bewijslast voor naleving van verwerkersverplichtingen. Deelt relevante resultaten uit pentests of externe controles met schoolbesturen of SIVON.	Voert periodiek audits en managementreviews uit; resultaten vastgelegd en gedeeld met opdrachtgevers indien relevant.