Checklist Normenkader IBP

Naam invuller: _____

Bewijsvoering	**Afdeling**
☐ Visie & Strategie [vastgesteld] – 1.1	CvB, PO
☐ IBP-beleid [goedgekeurd] -1.2	CvB, PO
☐ Jaarlijkse aandacht voor IBP - 1.2	CvB, PO
☐ Onboardingproces – 1.2	HR
☐ Procurementproces; IBP-beleid onderdeel van inkoop eisen - 1.2	Inkoop
☐ Informatiebeveiligingsplan (Planning/Roadmap) [goedgekeurd] - 1.3	CISO
☐ Jaarrapportage planning/roadmap - 1.3	CISO
☐ Functiebeschrijving; informatiemanagement en architectuur in functiepakket benoemd – 1.4	HR
☐ Referentie Architectuur = FORA [vastgesteld] - 1.4	ICT
☐ EIAM [goedgekeurd] – 1.4	ICT
☐ Auditplan beleid – 1.5	CvB, PO
☐ Auditplan uitvoering [goedgekeurd] – 1.5	CvB, PO
☐ Auditcommisie; wie zijn lid van het team – 1.5	CvB, PO
☐ Checklists – 1.5	CvB, PO
☐ Auditrapport – 1.5	CvB, PO
☐ Actieplan n.a.v. auditrapport – 1.5	PO, CISO
☐ Rollen, verantwoordelijkheden (aansprakelijkheid) en governancestructuur – 2.1	CvB, PO
☐ Intentieverklaring – 2.1	CvB, PO
☐ Autorisatiematrix beleid – 2.2	CvB, PO
☐ Toezicht bij afwijking van richtlijn logische toegangsbeveiliging – 2.2	CvB, PO
☐ Autorisatiematrix [vastgesteld] – 2.2	CvB, PO
☐ Informatierisicomanagementbeleid – 3.1	CvB, PO, CISO
☐ Informatierisicomanagementproces [goedgekeurd] – 3.1	CvB, PO, CISO
☐ Bedrijfsdoelstellingen – 3.2	CvB
☐ Risicomanagementproces – 3.2	PO, CISO
☐ Risicoanalyses – 3.2	PO, CISO
☐ Risico overleg – 3.2	PO, CISO
☐ Beleid behandeling en beperking van risico's – 3.3	PO, CISO
☐ Risico-actieplan [goedgekeurd] – 3.3	PO, CISO

☐ IT-Personeelsbeheerbeleid – 4.1	HR
☐ Wervingsproces IT-personeel [goedgekeurd] – 4.1	HR
☐ Opleidingsplan (IT-)personeel [goedgekeurd] – 4.2	HR
☐ IT-personeelsrisicobeleid – 4.3	HR
☐ IT-personeelsplan [vastgesteld] – 4.3	HR
☐ Personeel wijzigingsproces; i.g.v. uitdienst/wijziging functie (kennisoverdracht, rechten en verantwoordelijkheden) [goedgekeurd] – 4.4	HR
☐ HR-checklist; ter controle wijzigingsproces voor vertrek of wijziging – 4.4	HR
☐ IT-applicatie gebruikersondersteuningsproces [goedgekeurd] – 4.5	ICT
☐ Proces beheerdocumentatie [goedgekeurd] – 4.5	ICT
☐ Security-awareness-programma richting medewerkers en leerlingen – 4.6	HR
☐ Beleid Configuratiemanagement – 5.1	ICT
☐ Procedure Configuratiemanagement [vastgesteld] – 5.1	ICT
☐ Licentiebeheerproces – 5.1	ICT
☐ Fysieke bedrijfsmiddelen beleid – 5.1	ICT
☐ Ingericht CMDB – 5.2	ICT
☐ Procedure CMDB, m.a.w. in alle processen die een wijziging van de CMDB tot gevolg hebben dienen in deze stap opgenomen te worden – 5.2	ICT
☐ Incidentmanagementbeleid [vastgesteld] – 6.1	CISO
☐ Incidentmanagementproces – 6.1, 6.2	CISO
☐ Register van beveiligingsincidenten & datalekken - 6.1, 6.2, 6.3	CISO, PO
☐ Rapportage beveiligingsincidenten & datalekken – 6.1, 6.2, 6.3	CISO, PO, FG
☐ Problem managementbeleid [vastgesteld] – 6.4	ICT
☐ Register van problems (meenemen in register 6.1) – 6.1	ICT
☐ Rapportage problems (meenemen in rapport 6.1) – 6.1	ICT
☐ Procedure voor Change management [vastgesteld] - 7.1, 7.2, 7.3, 7.4, 7.5, 7.6	ICT
☐ Overzicht testomgeving – 7.4	ICT
☐ Testplan administratie – 7.5	ICT
☐ Acceptatiecriteria administratie – 7.6	ICT
☐ Procesimplementatie Secure Software Development – 8.1	ICT
☐ Opleidingsplan – veilige software ontwikkeling – 8.1	ICT
☐ Beleid aanschaf nieuwe/ontwikkeling software derden – 8.1, 8.2, 8.3	ICT
☐ Proces aanschaf nieuwe/ontwikkeling software derden – 8.1, 8.2, 8.3	ICT
☐ Data-eigenaarschap en classificatie is onderdeel van IBP-beleid (zie norm 1.2) – 9.1, 9.2	HR
☐ Beveiligingseisen voor datamanagement beleid – 9.3	HR
☐ Beleid voor opslag en retentie – 9.4	HR

☐ Proces voor inrichting van opslag en retentie – 9.4	HR, Onderwijs
☐ Bewaartermijnen en vervolgacties – 9.4	HR, Onderwijs
☐ Data uitwisselingsbeleid – 9.5	HR, Onderwijs
☐ Data verwijderingsbeleid voor hardware 9.6	HR
☐ Proces voor verwijdering van data per scenario (o.a. hergebruik, verkoop, vernietiging) – 9.6	HR
☐ Beleidsdocument IAM, onderdeel van IBP-beleid – 10.1	ICT
☐ Autorisatiematrix voor bedrijfskritische applicaties, onderdeel van IBP-beleid – 10.1	ICT
☐ Audit & controleplan - Proces toegangsrechtencontrole – 10.1	ICT
☐ Proces voor centrale gebruikersregistratie – 10.1	ICT
☐ Proces toekennen/wijzigen van toegangsrechten – 10.2	ICT
☐Proces in-/uitdiensttreding – 10.2	HR
☐ Proces toegangsrechtencontrole superusers (audit & controleplan, zie ook 10.1) – 10.3	ICT
☐ Proces Noodtoegang, onderdeel van proces toegangsrechten (=10.1 IAM beleid) – 10.4	ICT
☐ Register gebruik van noodprocedure – 10.4	ICT
☐ Evaluatie gebruik noodprocedure – 10.4	ICT
☐ Overzicht bedrijfskritische applicaties [vastgesteld] – 10.1	ICT/CISO
☐ Security baselines [goedgekeurd] – 11.1	CISO
☐ Proces security baseline controle - 11.1	CISO
☐ Security baseline register - 11.1	CISO
☐ Rapport security baseline - 11.1	CISO
☐ Beleid voor gebruikersauthenticatie, onderdeel van IBP beleid (norm 1.2) – 11.2	ICT/CISO
☐ Proces aanvragen, toekennen, toewijzen en intrekken van toegang – 11.2	ICT
☐ Centrale database voor user ID's en toegangsrechten – 11.2	ICT
☐ Proces toegangsrechten controle – 11.2	ICT
☐ 2FA/MFA beleid, inclusief eventuele risicoanalyse en maatregelen bij afwijking van de standaard, onderdeel van IBP beleid (norm 1.2) – 11.2	ICT/CISO
☐ Beleid voor Mobiele Apparaten en Tele(thuis)werken, onderdeel van IBP beleid (norm 1.2) – 11.3	ICT/CISO
☐ Keuze voor MDM/MAM en Anti-virus/malware applicatie – 11.3	ICT/CISO
☐ Gedragscode ICT voor medewerkers – 11.3	HR
☐ Gedragscode ICT voor leerlingen – 11.3	Onderwijs
☐ Beleid voor Logging, onderdeel van het IBP-beleid (norm 1.2) – 11.4	ICT/CISO

☐ Logging proces – 11.4	ICT/CISO
☐ Audit & Controleplan [vastgesteld] – 11.5	ICT/CISO
☐ Beleid voor Patchmanagement [vastgelegd] – 11.6	ICT
☐ Proces (controle)patchmanagement – 11.6	ICT
☐ Beleid voor Threat en Vulnerability Management - 11.7	CISO
☐ Proces voor Threat en Vulnerability Management [vastgelegd] – 11.7	CISO
☐ Beleid voor beschikbaarheid en bescherming van de IT-infrastructuur – 11.8	ICT/CISO
☐ Proces voor beschikbaarheid en bescherming van de IT-infrastructuur [vastgesteld] – 11.8	ICT/CISO
☐ Beleid onderhoud IT-infrastructuur – 11.9	ICT
☐ Proces onderhoud IT-infrastructuur – 11.9	ICT
☐ Beleid voor Cryptographic Key Management – 11.10	ICT/CISO
☐ Proces voor Cryptographic Key Management [vastgesteld] 11.10	ICT/CISO
☐ Beleid voor Netwerkbeveiliging – 11.11	ICT/CISO
☐ Netwerkbeveiliging – 11.11	ICT/CISO
☐ Beleid voor beheersing Malware – 11.12	ICT/CISO
☐ Beheersing Malware – 11.12	ICT/CISO
☐ Bewustwording rondom anti-malwaremaatregelen (norm 4.6) – 11.12	ICT/CISO
☐ Beleid bescherming van beveiligingstechnologie – 11.13	ICT/CISO
☐ Proces bescherming van beveiligingstechnologie – 11.13	ICT/CISO
☐ Beleid voor fysieke beveiliging – 12.1	Facilitair
☐ Risicoanalyse fysieke beveiliging - 12.1	Facilitair
☐ Beleid voor cameratoezicht – 12.1	Facilitair
☐ Rapport nog niet doorgevoerde fysieke beveiligingsmaatregelen – 12.1	Facilitair
☐ Fysieke beveiliging aan basis van ontwerp bij verbouwing/verhuizing – 12.1	Facilitair
☐ Vaststelling IT-kritieke ruimtes / beveiligingsobjecten – 12.2	Facilitair
☐ Vaststelling maatregelen – 12.2	Facilitair
☐ Fysieke toegang autorisatiematrix [vastgelegd] – 12.2	Facilitair
☐ Proces registratie en up-to-date houden toegekende fysieke toegangsrechten – 12.2	Facilitair
☐ Registratie toegang tot IT-kritieke ruimte – 12.2	Facilitair
☐ Beleid IT-operatie (bevat OP.01, OP.02 en OP.03) – 13.1	ICT
☐ Overzicht van Job Scheduling – 13.1	ICT
☐ Beleid voor back-up en herstel van systemen, applicaties, data en documentatie [vastgesteld] - 13.2	ICT/CISO
☐ Proces voor back-up en herstel van systemen, applicaties, data en documentatie – 13.2	ICT/CISO
☐ Dataherstel opgenomen in BCP (norm 14.1) – 13.2	ICT/CISO
☐ Beleid Capacity & Performance management – 13.3	ICT

☐ Proces Capacity & Performance management – 13.3	ICT
☐ Bedrijfscontinuïteitsmanagement beleid – 14.1	CvB, PO
☐ Bedrijfs- & IT-continuïteitsplan [vastgesteld] – 14.1	CvB, PO
☐ Bedrijfscontinuïteitsplan test – 14.2	CvB, PO
☐ Rapportage bedrijfscontinuïteitsplan test 14.2	CvB, PO
☐ Proces off-site back-up opslag [vastgesteld/goedgekeurd] -14.3	ICT
☐ Proces voor datareplicatie – 14.4	ICT
☐ Crisismanagementplan - 14.5	CvB, PO
☐ Proces voor Crisisoefening – 14.5	CvB, PO
☐ Beleid ketenbeheer – 15.1	Inkoop
☐ Proces voor inkoop van IT services – 15.1	Inkoop
☐ Standaard SLA [goedgekeurd] – 15.1	Inkoop
☐ Proces Leveranciersmanagement - sub Service Level Management [goedgekeurd] – 15.2	Inkoop
☐ Rapportage SLA beoordeling – 15.2	Inkoop
☐ Proces Leveranciersmanagement - sub leveranciersrisicomanagement [goedgekeurd] – 15.3	Inkoop
☐ Leveranciersmanagement risicoanalyse – 15.3	Inkoop
☐Proces Leveranciersmanagement - sub Toetsing van Interne Beheersmaatregelen [goedgekeurd] -15.4	Inkoop