SPEYK

CHECKLIST DOCUMENTATIE NORMENKADER

4-3-2024
Behandeld door Olaf Ritman
Gecontroleerd door Jak Mentjot
Versienummer 1.0

ISO 27001

Microsoft Solutions Partner

INLEIDING

Het normenkader IBP (Informatiebeveiliging en Privacy) voor het Funderend Onderwijs wordt in 2027 verplicht. Dit kader biedt richtlijnen voor het veilig inrichten van het geheel aan voorzieningen die van invloed zijn op de verwerking van (gevoelige) informatie.

Als onderlegger voor de implementatie van de verschillende normen wordt verwacht dat beleid, processen, procedures, werkinstructies en plannen worden vastgelegd in documentatie en dat deze worden goedgekeurd door het bevoegd gezag en gecommuniceerd naar alle betrokkenen.

OVER DEZE CHECKLIST

Dit document bevat een samenvatting van alle in het normenkader verwachte documenten, incl. een referentie naar de norm waar het document betrekking op heeft.

Onderstaand overzicht beoogt niet de enige juiste manier te zijn, maar geeft een richtlijn zoals deze door SPEYK wordt gebruikt bij de implementatie van het normenkader bij haar klanten. Het dient als checklist om gericht alle documentatie op orde te krijgen.

CHECKLIST DOCUMENTATIE NORMENKADER

Document

Informatiebeveiligingsbeleid (1.2), incl.:
- Strategie en visie op informatiebeveiligingsbeleid (1.1)
- Roadmap + jaarlijkse planning (1.3)
- Eigenaarschap & Functiescheiding (2.1, 2.2)
- Datamanagement (9.1)
  o Classificatie (9.2)
  o Beveiligingseisen (9.3)
  o Inrichting opslag en retentie (9.4)
  o Uitwisseling gevoelige gegevens (9.5)
  o Verwijderen van data (9.6)
- Security baselines (11.1), incl. beleid op:
  o Authenticatie (11.2)
  o Mobile devices en telewerken (11.3)
  o Logging (11.4)
  o Testen (11.5)
  o Patchmanagement (11.6)
  o Threat en Vulnerability management (11.7)
  o Bescherming en onderhoud infrastructuur (proces) (11.8, 11.9)
  o Cryptografie (11.10)
  o Netwerkbeveiliging (11.11)
  o Malware-aanvallen (11.12)
  o Beveiligingstechnologie (inbreuk beperken, wachtwoordbeleid) (11.13)
- Fysieke beveiliging + procedures (12.1, 12.2)

Enterprise Information Architecture Model (1.4)
Auditplan (1.5)
Risicomanagementbeleid en procedure (3.1)

Document
HR-beleid (4.1), incl.: - Wervingsproces (4.1) - Screening (4.1) - Trainging & scholing (4.2) - In-, door- en uitstroom (4.3, 4.4) - Proces voor kennisdeling (4.5) - Security awareness programma (in lijn met informatiebeveiligingsbeleid) (4.6)

IT Service Management beleid
- Configuration Management (5.1, 5.2), incl.:
  o Procedures en werkinstructies
- Incident Management (6.1, 6.2), incl.:
  o Procedures en werkinstructies
  o Escalatieprocedure (6.3)
- Problem Management (6.4)
- Change Management (7.1), incl.:
  o Procedures en werkinstructies (incl. Impactanalyse en inrichting CAB) (7.2)
  o Procedure voor noodwijziging (7.3)
  o Beleid op Testomgeving (7.4)
  o Beleid op overzetten naar Productie (7.5)
- Operation Management
  o Runbook voor job scheduling (13.1)
  o Backup en restore procedures (13.2)
  o Capaciteit en performance monitoring (13.3)
- Service Level Management (15.2), incl.:
  o Leveranciersrisicomanagement (15.3)
  o Proces voor interne beheersing bij leveranciers (15.4)

Beleid op softwareontwikkeling en -implementatie (8.1), incl.: - Toegang tot productieomgeving door ontwikkelaars (8.2) - Beleid op dataconversie (8.3)
Beleid op toegangsrechten (10.1, 10.5), incl.: - Toestemmingsprocedure (10.2) - Procedure voor super users (10.3) - Noodprocedure (10.4)
Business Continuity & Disaster Recovery, incl.: - Impactanalyse, RTO, RPO (14.1) - Testplannen (14.2) - Backup beheer (off-site) (14.3) - Replicatie (14.4) - Crisismanagement (14.5)