5. Informatiebeveiliging en betrouwbaar

Gegenereerd op 23 november 2026

Bron: https://frontend-production-toets-hn7.rig.prd1.gn2.quattro.rijksapps.nl/normen/05-betrouwbaar/

Versie: v1.0.1

Het verantwoordelijke overheidsorgaan beheert de door hen opgemaakte of ontvangen documenten op zodanige wijze dat de inhoud van documenten betrouwbaar, volledig en beveiligd zijn en documenten geen 'aanmerkelijke' digitale achteruitgang of informatieverlies ondervinden gedurende hun bewaartermijn, óók wanneer incidenten zich voordoen. Daarnaast mogen documenten niet ongecontroleerd gewijzigd worden en moeten deze volledig zijn.

Bron: Archiefbesluit, artikel 2.1, eerste lid, sub e en f; Archiefbesluit, artikel 2.1, tweede lid. Bekijk bron

Toelichting

Om documenten duurzaam toegankelijk te maken en te houden moeten deze betrouwbaar (opent in een nieuw venster) zijn. De Inspectie beoordeelt informatiebeveiliging in het kader van duurzame toegankelijkheid primair vanuit de verantwoordelijkheid en inspanningsverplichting van het overheidsorgaan.[1] Daarbij kijkt de Inspectie of verantwoordelijke overheidsorganen passende maatregelen nemen op het gebied van informatiebeveiliging die zijn afgestemd op de risico's, het gebruik en de levensduur van de documenten en of zij erop zijn gericht om de authenticiteit, volledigheid en beschikbaarheid van documenten te borgen. De Inspectie richt zich niet op de technische kant van informatiebeveiliging.[2]

Een passende maatregel is het voldoen aan de actuele Baseline Informatiebeveiliging Overheid (BIO).[3] Organisaties kunnen aanvullende of alternatieve maatregelen treffen, mits zij aantoonbaar een vergelijkbaar beschermingsniveau realiseren, passend bij de risico's en het gebruik van de documenten.

Het risico van onvoldoende beveiliging is dat documenten kunnen worden gestolen, beschadigd of vernietigd. Daardoor bestaat het risico dat de duurzame toegankelijkheid wordt aangetast.[4]

Voorschriften

Voorschrift 5.1

De oorspronkelijke inhoud van documenten is betrouwbaar, volledig en beveiligd.[5]

Criterium

- Het verantwoordelijke overheidsorgaan heeft op een aantoonbare en toetsbare manier vastgesteld dat passende maatregelen zijn getroffen conform de BIO[6] of een vergelijkbaar normenkader, waarmee de beveiliging en betrouwbaarheid van documenten die onder de Archiefwet vallen wordt geborgd.

Indicatoren

- In periodieke interne of externe audits, risicoanalyses of beleidsdocumenten zijn beveiligingsmaatregelen opgenomen.[7]
- Bij het opstellen en uitvoeren van beleid vindt samenwerking plaats tussen relevante disciplines, zoals informatiebeveiliging, privacy, gegevensbeheer en ICT.[8]
- Er is beleid voor het regelmatig uitvoeren van back-ups.
- Er is vastgelegd met welke frequentie back-ups worden gemaakt, wie daarvoor verantwoordelijk is en hoe hierop wordt gecontroleerd.
- Er is vastgelegd hoe back-ups worden bewaard, geraadpleegd en vernietigd in relatie tot geldende bewaartermijnen en archiefwetgeving.

Voorschrift 5.2

Documenten zijn beschermd tegen ongeautoriseerde wijzigingen en verlies.[9]

Criterium

- Er is toegangsbeheer voor de aanwezige documenten.

Indicator

- Er is vastgelegd welke functionarissen wijzigingen mogen doorvoeren bij de aanwezige documenten.

Voorschrift 5.3

Beveiligingsmaatregelen zijn passend[10] en afgestemd op de risico's.[11]

Criterium

- Er is een risicomanagementsysteem gebruikt voor de passende beveiligingsmaatregelen.

Indicatoren

Bij dit voorschrift zijn geen indicatoren.

Voorschrift 5.4

Het verantwoordelijke overheidsorgaan kan de betrouwbaarheid en authenticiteit van een document gedurende de levensduur aantonen.[12]

Criteria

- Met metadata kan worden aangetoond dat documenten volledig zijn.[13]
- Met metadata kan worden aangetoond wanneer documenten zijn opgemaakt of ontvangen.[14]
- Gegevens, zoals persoonsgegevens, zijn niet ongeoorloofd uit documenten gewist.[15]

Indicatoren

- In de metadata is de integriteitscheck vastgelegd bij digitale documenten die langer dan tien jaar worden bewaard.[16]
- Er wordt gebruikgemaakt van een hashfunctie[17] voor de controleerbaarheid van de integriteit van digitale documenten.
- Er is een audittrail waarin veranderingen in documenten en metadata worden vastgelegd.

Reikwijdte

Alle documenten moeten betrouwbaar, volledig en beveiligd zijn. Dit geldt ook voor documenten die op elk moment mogen worden vernietigd.

Bronnen

1. Archiefbesluit, nota van toelichting, p. 12. Bekijk bron (opent in een nieuw venster)
2. Voorbeelden van onderwerpen waar de Inspectie zich niet op richt zijn: firewalls, versleuteling (encryptie), antivirussoftware, multifactorauthenticatie (MFA), of het patchen van kwetsbaarheden. Archiefbesluit, nota van toelichting p. 11-12. Bekijk bron (opent in een

nieuw venster)

3. Archiefbesluit, nota van toelichting, p. 12. Bekijk bron (opent in een nieuw venster)

4. Archiefbesluit, nota van toelichting, p. 11. Bekijk bron (opent in een nieuw venster)

5. Archiefbesluit, artikel 2.1, sub e; Archiefbesluit, artikel 2.1, tweede lid. Bekijk bron (opent in een nieuw venster)

6. Archiefbesluit, nota van toelichting, Algemeen deel, inleiding, onder “veilig”, p. 11. Bekijk bron (opent in een nieuw venster)

7. De Inspectie voert daarbij geen diepgaande technische toets van informatiebeveiliging uit, maar stemt, waar relevant, haar beoordeling af met de RDI.

8. Archiefwet 2026, Memorie van Toelichting, Kamerstukken II 2021/22, 35968, nr. 3, Algemeen deel, onder 4.3 “Beheerstrategie”. Bekijk bron (opent in een nieuw venster)

9. Archiefwet, Memorie van Toelichting, Kamerstukken II 2021/22, 35968, nr. 3, Algemeen deel, onder 3.5 “Archiveren by Design”. Bekijk bron (opent in een nieuw venster)

10. Archiefbesluit, artikel 2.1, tweede lid. Bekijk bron (opent in een nieuw venster)

11. Archiefbesluit, Nota van toelichting, Algemeen deel, 1 Inleiding, onder “veilig”; BIO, Hoofdstuk 8, p. 11. Bekijk bron (opent in een nieuw venster)

12. Archiefregeling, artikel 2.10; Archiefbesluit, artikel 2.1 eerste lid, onder e. *(Bron beschikbaar na publicatie van de Archiefregeling.)* Bekijk bron (opent in een nieuw venster)

13. Archiefregeling, artikel 2.5, tweede lid. *(Bron beschikbaar na publicatie van de Archiefregeling.)*

14. Archiefregeling, artikel 2.5, tweede lid, sub f. *(Bron beschikbaar na publicatie van de Archiefregeling.)*

15. Archiefbesluit, artikel 2.1, eerste lid, onderdeel e; Archiefbesluit, nota van toelichting, p.18 van document. Met ongeoorloofd wordt bedoeld anders dan op grond van een verplichting uit andere wetgeving. Deze verplichting mag echter niet in strijd zijn met de uitvoering van de Archiefwet. Bekijk bron (opent in een nieuw venster)

16. Archiefregeling, artikel 2.8, onderdeel b. *(Bron beschikbaar na publicatie van de Archiefregeling.)*

17. DUTO-modeleis R15 t.b.v. functie Validatie, NEN-ISO 16175-1:2020, R.1.1.4 Bekijk bron (opent in een nieuw venster)

Dit is versie v1.0.1 van het toetsingskader. Bekijk voor de actuele versie https://frontend-production-toets-hn7.rig.prd1.gn2.quattro.rijksapps.nl/. Aan dit document kunnen geen rechten worden ontleend.