



**CoreTrustSeal Trustworthy Digital Repositories
Requirements 2023-2025**

Extended Guidance

Nederlandse vertaling

**DANS, voor de Wegwijzer Certificering (een
Netwerk Digitaal Erfgoed voorziening)**

V01.01

Inhoud

Inleiding	2
CoreTrustSeal Resources	2
Achtergrond en algemene richtlijnen	3
Complianceniiveaus	3
Links naar ondersteunend bewijs en ontbrekende informatie/bewijzen	4
Interne informatie, gevoelige informatie en vertrouwelijkheid	5
Engelstalige en niet-Engelstalige documentatie	5
Geldigheid en verlenging van certificering	5
Structuur en omvang van de aanvraag	6
Requirements	6
R0. Background Information & Context	6
Organisatorische infrastructuur	11
Mission & Scope (R01)	11
Rights Management (R02)	12
Continuity of Service (R03)	13
Legal & Ethical (R04)	14
Governance & Resources (R05)	16
Expertise & Guidance (R06)	17
Beheer van digitale objecten	18
Provenance and authenticity (R07)	18
Deposit & Appraisal (R08)	19
Preservation plan (R09)	20
Quality Assurance (R10)	21
Workflows (R11)	23
Discovery and Identification (R12)	24
Reuse (R13)	25
Informatietechnologie en beveiliging	26
Storage & Integrity (R14)	26
Technical Infrastructure (R15)	27
Security (R16)	28
Opmerkingen/feedback	30
Feedback aanvrager	30

Inleiding

De CoreTrustSeal Standards and Certification Board¹, bestaande uit leden van de CoreTrustSeal Community of Reviewers², is verantwoordelijk voor de periodieke herziening van de CoreTrustSeal Trustworthy Repository Requirements, het proces van peer review en de uiteindelijke certificering. De Board streeft ook naar bijdragen aan en afstemming op andere organisaties, normen en praktijken in de databeheercyclus.

Een aanvrager van het CoreTrustSeal moet diensten voor preservering op lange termijn (duurzame preservering) aanbieden. Voor sommige onderdelen van de collectie kan een lager niveau van dienstverlening gelden, maar dit moet in de tekst duidelijk worden gemaakt. Na toewijzing van de aanvraag controleert elke reviewer kort:

- de omschrijving van de Designated Community om te zien of deze voldoende duidelijk is;
- het preserveringsplan om na te gaan of er sprake is van actieve preservering;
- de verwerking en waardering om vast te stellen dat digitale objecten actieve preservering ondergaan;
- het hergebruik om te verifiëren dat de uitkomsten van de curatie overeenkomen met de behoeften van de Designated Community.

Als niet duidelijk is of de aanvrager actieve preservering aanbiedt, als niet duidelijk is welke andere niveaus van curatie worden aangeboden of als niet duidelijk is dat aan de behoeften van de omschreven Designated Community wordt voldaan door de informatie over hergebruik, komt de aanvrager niet in aanmerking of heeft die onvoldoende informatie verstrekt voor een review.

In dat geval wordt de aanvraag teruggestuurd naar de aanvrager met een toelichting op de onderdelen die revisie behoeven. Deze revisie kan impliceren dat ook andere wijzigingen in de aanvraag nodig zijn, hetgeen ter beoordeling van de aanvrager is.

Ter beoordeling aangeboden aanvragen zijn voor zowel de reviewers als de CoreTrustSeal Board vertrouwelijk, maar succesvolle aanvragen worden openbaar gemaakt. Aanvragers dienen daarom al deze partijen in aanmerking te nemen.

Succesvolle aanvragers kunnen medewerkers voordragen als lid van de Community of Reviewers. De leden van deze peer-review pool komen in aanmerking voor het lidmaatschap van de Board.

In aanvulling op de volledige tekst van de CoreTrustSeal Requirements, die gedurende de periode 2023-2025 ongewijzigd blijft, bevat dit document de **Extended Guidance** voor CoreTrustSeal-reviewers en -aanvragers. De tekst van de Extended Guidance ('Uitgebreide toelichting') wordt in blauw en omkaderd gepresenteerd. Deze tekst kan in de periode 2023-2025 worden gewijzigd.

CoreTrustSeal Resources

¹ <https://www.coretrustseal.org/about/standards-and-certification-board/>

² <https://www.coretrustseal.org/about/assembly-of-reviewers>

<https://www.coretrustseal.org/apply/>

<https://www.coretrustseal.org/why-certification/frequently-asked-questions/>

CoreTrustSeal Requirements v01.00 2023-2025 (<https://doi.org/10.5281/zenodo.7051011>)

De volledige normatieve CoreTrustSeal Requirements en Guidance. Ongewijzigd gedurende de periode 2023-2025.

CoreTrustSeal Extended Guidance v01.00 2023-2025 (<https://doi.org/10.5281/zenodo.7051095>)

De volledige tekst van de CoreTrustSeal Requirements met Extended Guidance inclusief commentaar en discussiemateriaal. Kan periodiek worden gewijzigd gedurende de periode 2023-2025.

Nederlandse vertaling: <https://doi.org/10.5281/zenodo.7323026>

CoreTrustSeal Glossary v01.00 2023-2025 (<https://doi.org/10.5281/zenodo.7051124>)

Definities van de belangrijkste begrippen die worden gebruikt in de CoreTrustSeal Requirements.

Nederlandse vertaling: <https://doi.org/10.5281/zenodo.7322994>

Een aantal begrippen en termen die in CoreTrustSeal worden gebruikt, zijn gebaseerd op het OAIS Reference Model³. Aanvragers wordt aangeraden zich vertrouwd te maken met deze standaard.

Achtergrond en algemene richtlijnen

De *CoreTrustSeal Requirements* zijn een beschrijving van de kenmerken van betrouwbare archieven voor digitale data en metadata. Elke Requirement gaat vergezeld van Guidance-tekst waarin de antwoorden worden beschreven, alsmede de onderbouwing die aanvragers moeten verstrekken om een objectieve beoordeling mogelijk te maken. Aanvragers moeten antwoord geven op alle Requirements.

Compliancenniveaus

De aanvrager moet voor elk van de Requirements een compliancenniveau opgeven:

- In Progress: het digitale archief is in de implementatiefase.
- Implemented: de Requirement is door het digitale archief volledig geïmplementeerd.

Compliancenniveaus zijn een indicatie van de voortgang volgens de aanvrager zelf, maar de reviewers beoordelen de compliance aan de hand van de antwoorden én de onderbouwing. Een reviewer kan een compliancenniveau verlagen tot 'In progress' en dit toelichten in de feedback aan de aanvrager. Alle Requirements die worden beoordeeld als 'In progress'

³ Consultative Committee for Space Data Systems (juni 2012). Reference Model for an Open Archival Information System (OAIS). Recommended Practice, issue 2, CCSDS 650.0-M-2. NASA. <https://public.ccsds.org/pubs/650x0m2.pdf>

moeten vergezeld gaan van een verklaring waarin de aanvrager de activiteiten en het tijdpad uiteenzet om de status ‘Implemented’ te bereiken. Een reviewer zal nooit een zelfverklaard ‘In progress’ opwaarderen tot ‘Implemented’. Certificering kan worden toegekend als enkele Requirements ‘In progress’ zijn. Wanneer het CoreTrustSeal daarna wordt verlengd, verwachten de reviewers een voortgang van ‘In progress’ naar ‘Implemented’ te zien, of een heldere uitleg waarom dat niet mogelijk is.

Tijdens de verlengingsprocedure kan een aanvrager een zelfverklaard compliancieniveau verlagen van ‘Implemented’ naar ‘In progress’, bijvoorbeeld als een belangrijke upgrade wordt uitgevoerd die tijdelijk effect heeft op de dienstverlening. Deze mate van transparantie is zeer wenselijk en hoeft, mits voldoende toegelicht, geen belemmering te zijn voor verlenging van de certificering.

Er geldt geen formeel maximum voor het aantal compliancieniveaus ‘In progress’ waarbij een aanvraag wordt afgewezen. Dat zal altijd afhangen van het digitale archief in kwestie en de planning die voor de implementatie wordt voorzien. Reviewers zullen met name alert zijn als een digitaal archief zijn Continuity of Service (R03) of Preservation plan (R09) als ‘In progress’ bestempelt.

Links naar ondersteunend bewijs en ontbrekende informatie/bewijzen

De door aanvragers gekozen antwoorden moeten worden ondersteund met links naar online, openbaar beschikbaar bewijs. Definitieve versies van succesvolle aanvragen zijn openbare documenten. Deze mate van transparantie is van belang omdat het certificeringsproces geen locatiebezoek van een auditor omvat. Links moeten worden geverifieerd direct voor het indienen van de aanvraag.

De lezers van de aanvragen (de reviewers en uiteindelijk het grote publiek) moeten de antwoorden kunnen begrijpen zonder het gelinkte bewijs uitvoerig te hoeven raadplegen. Wanneer langere documenten als onderbouwing worden gepresenteerd, of als dezelfde onderbouwing wordt gebruikt bij meer dan één Requirement, moet de aanvrager verwijzen naar de specifieke relevante gedeelten en die informatie in het antwoord citeren of samenvatten.

Het CoreTrustSeal-certificeringsproces hangt af van de antwoorden en de onderbouwing van de aanvrager. De kwaliteit van het openbare ondersteunende bewijs zal naar verwachting in de loop der tijd toenemen.

Aanvragen kunnen niet worden beoordeeld als er informatie ontbreekt of als deze ontoereikend of onduidelijk is.

Voorafgaande bekendheid van de reviewer met een digitaal archief mag geen rol spelen bij het beoordelen van de aanvragen. De definitieve openbare uitspraak over de onderbouwing moet ook begrijpelijk zijn voor andere digitale archieven.

Een reviewer wordt niet geacht op de website van de aanvrager naar onderbouwing te zoeken. Aanvragers moeten specifieke referenties verstrekken, inclusief citaten of samenvattingen van de relevante informatie. De aanvraag wordt met een toelichting

teruggestuurd als de verstrekte informatie voor de reviewer ontoereikend is om een besluit te nemen en een compliancenniveau vast te stellen.

Voor informatie die door een andere partij dan de aanvrager wordt geleverd moet de relatie met die partij worden beschreven, zie de sectie *Cooperation and outsourcing to third parties, partners and host organisations*. (*Samenwerking met en uitbesteding aan derden, partners en host-organisaties*).

Interne informatie, gevoelige informatie en vertrouwelijkheid

Er hoeft geen gevoelige informatie te worden bekendgemaakt om het CoreTrustSeal te verwerven. Bewijs dat niet openbaar mag worden gemaakt, kan vertrouwelijk worden gedeeld tijdens het certificeringsproces.

Voor CoreTrustSeal-certificering is het niet vereist om ondersteunend bewijs te openbaren dat vertrouwelijk of commercieel gevoelig is dan wel een veiligheidsrisico oplevert. Aanvragers beschikken mogelijk over interne bedrijfsgegevens die *zowel* gevoelige informatie *als* voor het CoreTrustSeal relevant bewijs bevatten. Dergelijk bewijs kan vertrouwelijk worden ingediend bij de reviewers⁴ terwijl de documenten worden genoemd en beschreven in de aanvraag. Na verloop van tijd moeten de aanvragers het relevante bewijs scheiden van de vertrouwelijk materialen en erop toezien dat een openbare versie beschikbaar wordt gesteld voor de volgende review.

Als documentatie nog niet bestaat, in voorbereiding is of momenteel alleen voor intern gebruik bestemd is, moet in de aanvraag een datum van openbaarmaking worden vermeld. Certificering kan worden toegekend op basis van deze toezeggingen. Aanvragers worden geacht de openbare documentatie te verstrekken wanneer zij hun certificering verlengen.

Engelstalige en niet-Engelstalige documentatie

Alle antwoorden moeten in het Engels worden gegeven. Als links naar niet-Engelstalige onderbouwing worden gegeven, moet in het antwoord een samenvatting in het Engels worden opgenomen. Deze samenvatting kan kort zijn voor bepaalde soorten documenten (zoals een verwijzing naar een lijst met voorkeursformaten), maar moet voor andere (bijv. een preserveringsbeleid) uitvoeriger zijn.

Volledige Engelse vertalingen van gelinkte onderbouwingen zijn niet vereist.

Geldigheid en verlenging van certificering

CoreTrustSeal-certificering is drie jaar geldig vanaf de datum van certificering. Een organisatie met goed gedocumenteerde en beheerde bedrijfsprocessen moet met minimale aanpassingen verlenging kunnen aanvragen. Meer ingrijpende aanpassingen kunnen nodig zijn als:

- de organisatie, haar datacollectie, haar technische infrastructuur of haar Designated Community aanmerkelijk is veranderd;
- de CoreTrustSeal Requirements zijn gewijzigd op een wijze die impact heeft op de aanvrager.

⁴ Neem contact op met het CoreTrustSeal-secretariaat via info@coretrustseal.org

De CoreTrustSeal Requirements worden elke drie jaar tegen het licht gehouden en zo nodig herzien. Dit heeft geen gevolgen voor succesvolle aanvragers totdat zij verlenging aanvragen.

Structuur en omvang van de aanvraag

Het is onmogelijk om elk denkbaar scenario voor digitale archieven in de Guidance of Extended Guidance te behandelen. Bovendien zijn bepaalde richtlijnen of vragen niet overal van toepassing. De antwoorden van aanvragers moeten betrekking hebben op de zaken die in de Guidance aan de orde worden gesteld en moeten zijn gebaseerd op hun lokale context. De uiteindelijke beoordeling van een Requirement hangt af van de volledigheid en kwaliteit van het antwoord. Reviewers verwachten heldere, open verklaringen en onderbouwingen die specifiek zijn voor de aanvrager. Uiteraard zal de lengte van de antwoorden variëren, maar de aanvraag als geheel dient een geconcentreerde beschrijving van het ondersteunende bewijs te zijn.

Aanvragers hoeven niet één op één op elke vraag antwoord te geven. Zij dienen uitgeschreven antwoorden op elke Requirement te geven, met daarin relevante elementen van de Guidance en Extended Guidance.

Reviewers begrijpen dat de organisatiestructuren, missies, omvang en digitale collecties van aanvragers sterk uiteenlopen. Zelfs in de Extended Guidance kan niet elk type onderwerp en onderbouwing worden behandeld dat voor de aanvraag relevant zou kunnen zijn. Er kan enige aanvullende tekst nodig zijn om de relevantie van de verstrekte onderbouwing toe te lichten, met name als deze niet in het Engels beschikbaar is. Er is geen minimale of maximale lengte voor antwoorden vastgesteld, maar zelfs de meest complexe verklaringen zijn gewoonlijk niet langer dan 500-800 woorden. Verklaringen over het bewijs moeten worden gestaafd met openbare links naar de documentatie die de aanvrager gebruikt voor het beheer van de organisatie en de digitale objecten. Het is dit openbare bewijs dat de beste garantie voor naleving van de Requirements biedt.

In de CoreTrustSeal Requirements wordt gestreefd naar minimale herhaling en overlapping, maar sommige aanvragers kunnen dezelfde onderbouwing verstrekken voor meer dan één Requirement. Aanvragers hoeven geen lange stukken tekst te herhalen in hun antwoorden op verschillende Requirements. Indien onderbouwingen geldig zijn op meer dan één Requirement, kan worden volstaan met een beknopte uitspraak over de relevante informatie en een verwijzing naar de Requirement waar nadere details worden gegeven.

Requirements

R0. Background Information & Context

In dit deel wordt de informatie gegeven die reviewers nodig hebben om de antwoorden van de aanvrager volledig te kunnen beoordelen. Het is voor de aanvraag als geheel van groot belang dat de juiste opties worden geselecteerd en dat voldoende gedetailleerde antwoorden worden gegeven.

(1) *Re3data Identifier*⁵.

⁵ <https://www.re3data.org/>

Antwoord

- (2) **Repository type.** Selecteer een type digitaal archief:
- **Generalist repository (Generiek digitaal archief)**
 - **Specialist repository (Gespecialiseerd digitaal archief)**
 - o Gespecialiseerde digitale archieven worden verzocht hun domein(en) en/of discipline(s) te vermelden.

Antwoord

Zoals in de begrippenlijst wordt beschreven, is een gespecialiseerd digitaal archief een domein- of onderwerpspecifiek digitaal archief dat is gespecialiseerd op een specifiek onderzoeksterrein of datatype en dat een Designated Community ondersteunt. Een generiek digitaal archief is niet gespecialiseerd op een domein, discipline, onderzoeksterrein of datatype en ondersteunt een Designated Community.

- (3) **Overview.** Geef een kort overzicht van de belangrijkste kenmerken van het digitale archief, die typerend zijn voor het geselecteerde type archief. Hierin moet informatie staan over de scope en omvang van de datacollecties, -typen en -formaten. Ook andere contextuele informatie kan worden vermeld.

In het overzicht moet contextuele informatie worden opgenomen die niet elders in de Requirements wordt behandeld.

Antwoord

- (4) **Designated Community.** Een heldere omschrijving van de Designated Community (gedefinieerde doelgroep) toont aan dat de aanvrager inzicht heeft in de scope, basiskennis en methodologieën (inclusief voorkeurssoftware/-formaten) van de gebruikersgroepen waarop de curatie- en conserveringsmaatregelen primair gericht zijn. De omschrijving moet zo specifiek zijn dat reviewers kunnen vaststellen of die doelgroep wordt bediend in de antwoorden op andere Requirements.

Zoals uit de definitie blijkt (zie de begrippenlijst), kan een digitaal archief een Designated Community hebben die bestaat uit verschillende 'subgroepen', bijvoorbeeld voor verschillende collecties. Als dit het geval is, moet de aanvrager een definitie en een voldoende gedetailleerde omschrijving geven van elk van deze subdoelgroepen. Hierbij moet worden opgemerkt dat de Designated Community kleiner kan zijn dan de totale groep gebruikers van de data, metadata en diensten van het digitale archief. De digitale collecties van een natuurhistorisch museum kunnen een brede groep belangstellenden aanspreken, waaronder het grote publiek. Toch kan het museum de Designated Community

nauwer omschrijven, bijvoorbeeld als biologen en antropologen die onderzoek doen naar natuurhistorische onderwerpen.

Een digitaal archief moet inzicht hebben in de samenstelling, vaardigheden, basiskennis en behoeften van de Designated Community, en in de verandering daarin in de loop der tijd. Dit geldt ook voor typische scenario's en doelstellingen van hergebruik, die heel generiek kunnen zijn ("Read online publications on a computer to learn more about the history of X") of juist heel specifiek ("Run statistical analyses using SPSS"). Uit de gehele aanvraag moet een duidelijk begrip blijken van de curatie- en conserveringsactiviteiten (aanvullende context, voorkeursformaten, enz.) die het meest geschikt zijn voor de Designated Community (inclusief eventuele subdoelgroepen). Ook moet duidelijk zijn hoe de aanvrager veranderingen in de behoeften van de Designated Community bewaakt en verwerkt.

Een digitaal archief met een zeer specifieke, nauw gedefinieerde doelgroep zou eenvoudig de verwachte basiskennis kunnen beschrijven (bijvoorbeeld de mate van inzicht in genetica of het expertiseniveau op het gebied van statistische software). Daarentegen betekent een brede gedefinieerde doelgroep (die uit meerdere gebruikersgroepen bestaat) dat het digitale archief voldoende inzicht moet hebben in hun basiskennis en uiteenlopende contextuele informatie moet geven om ervoor te zorgen dat iedereen in de Designated Community de data begrijpt. In verband met de omschrijving van de basiskennis van de Designated Community dienen aanvragers uitdrukkelijk stilzwijgende aannames te vermelden, zoals (vreemde)talenkennis, ervaring met specifieke besturingssystemen of internetbrowsers, gebruik van bepaalde software, enzovoort.

Antwoord

(5) Levels of Curation. (Niveau van preserving.)

Select all relevant types from: (Kies alle relevante types:)

- A. Content distributed as deposited (Content wordt beschikbaar gesteld zoals deze is gedeponneerd)
- B. Basic curation - e.g. brief checking, addition of basic metadata or documentation (Basispreserving, met onder andere eenvoudige controles, toevoeging elementaire metadata of documentatie)
- C. Enhanced curation - e.g. conversion to new formats during ingest, enhancement of documentation and metadata (Uitgebreide preserving, zoals het migreren naar nieuwe bestandsformaten en het verbeteren van documentatie)
- D. Data-level curation - as in C above, but with additional editing of deposited data (Beheer op informatieniveau: zoals C hierboven, maar met aanvullende verrijking en correctie van gedeponeerde data)

Antwoord

Toelichting

Een digitaal archief moet aantonen dat het de duurzame toegankelijkheid en bruikbaarheid van data kan waarborgen wanneer de behoeften van de Designated Community veranderen. De kans dat dit op curatieniveau A en B mogelijk is, is minder waarschijnlijk, omdat zonder normalisering van de aangeleverde bestandsformaten naar een standaard preserveringsformaat bij toekomstige formaatmigraties de nodige problemen zouden kunnen ontstaan als gevolg van de heterogeniteit van de collectie. Maar ook een gebrek aan rijke metadata en documentatie kan een risico vormen voor duurzame bruikbaarheid van de data.

Een digitaal archief kan verschillende curatieniveaus bieden voor verschillende digitale objecten en het is belangrijk dat dit duidelijk is voor de depotgevers, de gebruikers en de CoreTrustSeal Reviewers.

Er kan meer dan één optie (A, B, C of D) voor het niveau (of de reikwijdte) van de curatie worden geselecteerd, afhankelijk van het type data en de bij deponering overeengekomen preserveringsvoorwaarden. Geef voor elk geselecteerd niveau enige beknopte informatie over hoe het zal worden gerealiseerd, bijvoorbeeld met automatische controles van metadata, intellectuele controle en bewerking van documentatie, identificatie van bestandsformaten, omzetting naar preserveringsformaten, enz.

Wanneer een digitaal archief curatie op meerdere niveaus uitvoert, moet nadere informatie worden toegevoegd over de verdeling van de verschillende niveaus over de data in de collectie. In dit geval moeten aanvragers in hun antwoorden op de Requirements alle relevante verschillen in workflows of gebruikte maatregelen toelichten voor elk geselecteerd curatieniveau.

Voor alle curatieniveaus gelden de volgende uitgangspunten: (1) de oorspronkelijke gedeponeerde data worden ongewijzigd bewaard en bewerkingen worden uitsluitend uitgevoerd op kopieën van die originele data, (2) metadata waarmee de Designated Community de data zelfstandig kan begrijpen en gebruiken (d.w.z. zonder de oorspronkelijke samensteller te raadplegen) zijn bij deponering aanwezig of door het digitale archief toegevoegd, en (3) er zijn permanente maatregelen getroffen voor actieve preservering van het grootste deel van de collectie(s).

Annotaties en bewerkingen moeten in overeenstemming zijn met de licentievoorwaarden die met de depotgever van de data zijn overeengekomen en duidelijk tot de capaciteiten van de curatoren behoren. Derhalve wordt van het digitale archief verwacht dat het aantoont dat dergelijke annotaties en bewerkingen altijd worden uitgevoerd en gedocumenteerd door gekwalificeerde experts en dat de integriteit van alle oorspronkelijke data gehandhaafd blijft.

Hoe hoger het preserveringsniveau (A-D), hoe groter de verwachtingen van de reviewers ten aanzien van het niveau van formele herkomst, integriteit en versiebeheer (wijzigingslogs e.d.).

**(6) Cooperation and outsourcing to third parties, partners and host organisations.
(Samenwerking met en uitbesteding aan derden, partners en host-organisaties)**

Antwoord

Toelichting

Als de aanvrager geheel verantwoordelijk is voor alle beslissingen en zelf alle relevante maatregelen treft om te voldoen aan elk van de 16 Requirements, kan dit gedeelte worden overgeslagen. Als de aanvrager voor een of meer Requirements bij beslissingen of maatregelen wordt geassisteerd door een andere organisatie, moeten die organisatie, de rol die zij speelt en haar relatie met de aanvrager hier worden vermeld.

Digitale archieven kunnen verschillende organisatiestructuren hebben. Het is van belang dat de certificering betrekking heeft op een helder gedefinieerde organisatie. De structuur van de aanvragende organisatie wordt behandeld onder Governance & Resources (R05).

Als een functie van het digitale archief en/of ondersteunend bewijs voor het CoreTrustSeal niet onder directe controle van de aanvrager staat, moet de relevante host-organisatie, partner of andere derde partij hier vermeld worden. Beschrijf de functie of de geleverde dienst van deze organisatie, de aard van de relatie of overeenkomst (contract, Service Level Agreement, Memorandum of Understanding, enz.) en vermeld of zij relevante certificeringen heeft. Passende kwalificaties en certificeringen, waaronder het CoreTrustSeal, zijn gewenst maar niet verplicht. Uitleg over de soorten overeenkomsten die zijn gesloten, of een toelichting waarom die niet mogelijk zijn, bevordert de transparantie. Van aanvragers wordt niet verwacht dat zij commerciële of andere gevoelige details van hun relaties bekendmaken (zie Internal Information, Sensitive Information & Confidentiality).

Dergelijke relaties kunnen de volgende vormen aannemen (maar zijn daartoe niet beperkt): samenwerking of federatie met andere digitale archieven, diensten die worden verleend door een instelling waarvan de aanvrager onderdeel is, opslagruimte die wordt verstrekt door anderen in het kader van multi-copy redundancy of organisaties die verantwoordelijkheid kunnen nemen voor data, metadata en diensten ten behoeve van de continuïteit of opvolging.

De genoemde organisaties moeten duidelijk worden vermeld onder elke relevante Requirement.

Omdat bij uitbestede functies gewoonlijk sprake zal zijn van een mate van gedeelde verantwoordelijkheid, moet de aanvrager afdoende bewijs leveren voor Requirements die niet worden uitbesteed en voor de onderdelen van de datacyclus waarover zij de controle hebben.

Hoewel zeer uiteenlopende diensten en functies kunnen worden uitbesteed, moet een CoreTrustSeal-aanvrager zelf de verantwoordelijkheid houden voor planning en uitvoering van de conserveringsmaatregelen die worden genomen om data en metadata op lange termijn bruikbaar te houden voor de Designated Community.

Dit kan een complex gebied zijn om te beschrijven en definiëren, maar dergelijke details zijn cruciaal om een alomvattend beoordelingsproces mogelijk te maken.

Als er sprake is van meer dan één betrokken partner, kan het nuttig zijn om een contextdiagram (bijv. het OAIS-functiemodel) te gebruiken om de volledige schaal van het uitbestedingsproces te tonen. Het is aanvaardbaar om meerdere partners te hebben (bijv. een

voor opslag, een voor het onderhouden van toegankelijkheid), mits alle relaties inzichtelijk worden gemaakt. Reviewers zullen om herformulering van het antwoord verzoeken als in onderbouwingen elders in de aanvraag wordt verwezen naar entiteiten die hier niet zijn vermeld.

(7) *Applicants renewing their CoreTrustSeal certification: summary of significant changes since last application. (Aanvragers van verlenging van hun CoreTrustSeal-certificering: samenvatting van belangrijke wijzigingen sinds de vorige aanvraag.)* CoreTrustSeal-certificering brengt de verwachting van permanente verbetering in de loop der tijd met zich mee. Digitale archieven die hercertificering aanvragen, moeten beknopt belangrijke wijzigingen van de afgelopen drie jaar vermelden, bijvoorbeeld in technische systemen, de Designated Community of de financiering. Hiertoe behoren ook maatregelen die zijn genomen om van ‘In progress’ naar ‘Implemented’ Requirements te geraken.

Antwoord

Organisatorische infrastructuur

Mission & Scope (R01)

R01. The repository has an explicit mission to provide access to and preserve digital objects. (Een expliciete missie van het digitale archief is het toegankelijk maken en behouden van data binnen een specifiek domein.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Digitale archieven zijn de beheerders van digitale objecten en zijn verantwoordelijk voor het bewaren van materialen in een daarvoor geschikte omgeving gedurende een vastgestelde termijn. Voor depotgevers en gebruikers moet duidelijk zijn dat het behouden en toegankelijk houden van de data een expliciete taak van het digitale archief is.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de missie om de toegang tot digitale objecten actief te behouden en te blijven aanbieden;
- de mate van goedkeuring die de missie heeft ontvangen.

Onderbouwing voor deze Requirement is bijvoorbeeld een goedgekeurde openbare missieverklaring, taken die door financiers zijn opgedragen of een beleidsstuk dat door een bestuursorgaan is ondertekend.

Als preservatie niet wordt genoemd in de missie van het digitale archief of andere relevante

openbare documenten die als onderbouwing worden verstrekt, kan het compliancenniveau niet hoger zijn dan “In Progress: the repository is in the implementation phase” (In uitvoering: het digitale archief bevindt zich in de implementatiefase).

Rights Management (R02)

R02. The repository maintains all applicable rights and monitors compliance. (Het digitale archief beschikt over alle toepasselijke rechten en bewaakt de naleving ervan.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Het digitale archief beheert, en informeert relevante stakeholders over, alle rechten (toestemmingen, verboden, plichten) met betrekking tot de deponering, de opslag, de preservering, het ontsluiten en het gebruik van data en metadata.

Deze Requirement betreft het systeem, de methoden en de artefacten (bijv. licenties, overeenkomsten, algemene voorwaarden en bijbehorende beleidsregels en procedures) voor het rechtenbeheer.

Het digitale archief moet alle noodzakelijke rechten van de depotgever verwerven, en aantonen dat het over voldoende controle-instrumenten beschikt om erop toe te zien dat die worden toegepast en bewaakt.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- het algemene beleid inzake rechtenbeheer voor gedeponeerde bestanden, data en metadata;
- de rechten om digitale objecten te kopiëren, om te zetten en op te slaan ten behoeve van preservering, en om er toegang toe te verlenen;
- gebruiksvoorwaarden (intellectueel eigendom, distributie, gebruiksdoel, bescherming van gevoelige informatie, enz.);
- depot- en toegangsovereenkomsten of -licenties;
- het beheer van metadata voor mensen (bijv. licentiedocumenten/-bestanden) of machines;
- bewaking van de compliance bij deponering, tijdens curatie/preservering en bij toegang en hergebruik, met een beschrijving van omstandigheden waaronder compliancebewaking niet mogelijk is;
- maatregelen die worden getroffen in geval van niet-naleving.

Aan data en metadata, inclusief ‘open data’, zijn gewoonlijk rechten verbonden, ook als er geen ondertekende licentie of formele overeenkomst bestaat. Deze kunnen betrekking hebben op verplichtingen zoals de citatie en toeschrijving van gebruikte data en metadata, of de verplichting om secundaire analyse openlijk toe te staan. Als alle data en metadata beschikbaar worden gesteld zonder enige toegangsbeperking of gebruiksvoorwaarde, moet dit expliciet worden vermeld in het antwoord.

Onderhandelingen over en overdracht van rechten moet worden behandeld onder Deposit &

Appraisal (R08). Ethische gedragscodes, privacymaatregelen en regels die van invloed zijn op het rechtenbeheer moeten worden beschreven onder Legal & Ethical (R04).

Bepalingen over de toegang tot en het gebruik van data kunnen in algemene voorwaarden worden vastgelegd of per depotgever of dataset worden uitgesplitst. Voorbeelden van veelgebruikte licentie-opties zijn die van Creative Commons (<https://creativecommons.org/>), zoals ‘CC 0 Waiver’ en ‘public domain data’.

Met name voor gevoelige data kunnen in licenties specifieke bepalingen worden opgenomen over gebruiksbepalingen, gebruiksomgevingen (zoals speciale ruimtes en beveiligde toegang op afstand) en soorten gebruikers (zoals gekwalificeerde onderzoekers en gebruikers met een speciale opleiding). Meer recentelijk zijn de Local Contexts Traditional Knowledge en BioCultural Notices and Labels ontstaan als middel waarmee inheemse volkeren aanpasbare verklaringen van herkomst, protocollen en vergunningen voor onderzoek naar objecten kunnen toewijzen.⁶

Schendingen van licentievoorwaarden zijn misschien niet gemakkelijk te bepalen. Toch is het belangrijk om bij deze Requirement aandacht te schenken aan de gevolgen van dergelijke schendingen, bijvoorbeeld met een beschrijving van sancties ten aanzien van de toegang tot of het gebruik van data en metadata nu en in de toekomst. Het openbaar maken van gevoelige persoonlijke informatie kan leiden tot zware juridische sancties met gevolgen voor zowel de gebruiker als het digitale archief. Digitale archieven dienen bij voorkeur een gepubliceerd beleid voor schending van licenties en licentievoorwaarden te hebben.

Als het digitale archief op dit moment toegang verleent tot gevoelige data of metadata, is het gewenste compliancieniveau “Implemented: the requirement has been fully implemented by the repository” (Geïmplementeerd: aan de vereiste wordt door het digitale archief volledig voldaan).

Continuity of Service (R03)

R03. The Repository has a plan to ensure ongoing access to and preservation of its data and metadata. (Het digitale archief heeft een continuïteitsplan om toe te zien op blijvende toegankelijkheid en preservatie van zijn data en metadata.)

Zelfverklaard compliancieniveau:

Antwoord

Toelichting

Het digitale archief moet maatregelen hebben getroffen tegen de risico's van veranderingen, bijvoorbeeld in de missie en/of scope. Bij deze Requirement gaat het over de manier(en) waarop het digitale archief in de loop van de tijd stabiel blijft functioneren (bedrijfscontinuïteit) en hoe het inspeelt op problemen in de dienstverlening (rampenplan). Hieronder vallen ook voorbereidingen op de overdracht van digitale objecten en diensten aan een ander digitaal archief

⁶ <https://localcontexts.org/>

(opvolgingsplan). De diensten ten behoeve van deponering, opslag, conservering en toegankelijkheid die het digitale archief verleent aan depotgevers en gebruikers, vallen alle onder de scope van deze Requirement.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de functies en diensten die het digitale archief aanbiedt aan depotgevers en gebruikers;
- de aanpak van snelle veranderingen in omstandigheden en de langetermijnplanning;
- de opties voor de verplaatsing of omzetting van de activiteit naar een ander digitaal archief, bijvoorbeeld in geval van onverwachte stopzetting van de financiering of een verschuiving in de belangen van de host-instelling, of de manier waarop het digitale archief beleidsregels, procedures en andere bedrijfsinformatie in de loop van de tijd beheert.

Ook al kunnen opvolgingsovereenkomsten moeilijk te realiseren zijn, het is belangrijk om de mogelijkheid onder ogen te zien dat een digitaal archief ophoudt te functioneren of te bestaan. Als er geen formele schriftelijke overeenkomst tussen het digitale archief en een opvolger bestaat, kan het compliancieniveau niet hoger zijn dan “In Progress: the repository is in the implementation phase” (In uitvoering: het digitale archief bevindt zich in de implementatiefase).

Alle technische aspecten van bedrijfscontinuïteit, rampenplan en opvolgingsplanning moeten worden behandeld bij R15 (Technical infrastructure).

Digitale archieven moeten toezien op de continuïteit van hun collecties en hun verantwoordelijkheid nemen in geval van een tijdelijke of permanente onderbreking van de dienstverlening.

Uit de antwoorden en onderbouwingen moet blijken welke verantwoordelijkheid wordt genomen voor de digitale objecten, welke risico's het digitale archief loopt en wat het niveau is van het opvolgingsplan voor de toekomst van de datacollectie.

Relevante informatie is bijvoorbeeld of de aanvrager de primaire of de enige conservator is, of de depotgever medeverantwoordelijk is voor de toekomst van de digitale objecten en of het digitale archief de toegankelijkheid, conservering en/of opslag van data tot een bepaald minimum kwaliteitsniveau of voor een bepaalde minimumtermijn garandeert.

Mogelijkerwijs ligt de verantwoordelijkheid voor de duurzaamheid niet bij het digitale archief zelf maar bij een hostingorganisatie of een bovenliggende organisatie, of bij een andere organisatie die deze verantwoordelijkheid op zich neemt in geval van discontinuering van de dienstverlening. Zo ja, dan dient dat duidelijk te worden aangegeven.

Het aanwijzen en formeel contracteren van een opvolgende organisatie die hetzelfde niveau van zorg en dienstverlening kan bieden, is voor veel digitale archieven een uitdaging.

Daarom is een voortgezette ‘In progress’-status acceptabel bij verlenging van de certificering, mits voldoende toegelicht.

Als er geen formele schriftelijke overeenkomst tussen het digitale archief en een opvolgende organisatie bestaat, kan deze Requirement niet worden beoordeeld als ‘Implemented’.

Legal & Ethical (R04)

R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms. (Het digitale archief ziet erop toe dat de totstandkoming, het beheer, de toegang en het gebruik van data en metadata voldoen aan wettelijke en ethische normen.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Deze Requirement betreft het bewustzijn en de procedures van het digitale archief rondom wettelijke en ethische kwesties, zoals privacy en vertrouwelijkheid, die gevolgen hebben voor de totstandkoming, de preservering en het gebruik van digitale objecten.

Voor het vertrouwen van degenen die zich bereid hebben verklaard hun digitale objecten aan het digitale archief toe te vertrouwen, moet uit de onderbouwing van het antwoord blijken dat het digitale archief goede maatregelen heeft getroffen voor de bescherming van persoonlijke en gevoelige data en dat het depotgevers en gebruikers hier ook goede ondersteuning bij biedt.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- Hoe kiest het digitale archief relevante wettelijke en ethische normen die gevolgen hebben voor zijn werkwijze?
- Hoe zorgt het digitale archief voor naleving van de relevante wettelijke en ethische domeinspecifieke normen?
- Vraagt het digitale archief om bevestiging dat data zijn verzameld of tot stand gekomen conform de wettelijke en ethische criteria die van toepassing zijn op het geografische gebied of de discipline van de maker of depotgever (bijv. ethische toetsingscommissie, institutionele toetsingscommissie, wetgeving gegevensbescherming)?
- Is er sprake van vertrouwelijk data of metadata, bijv. gegevens van depotgevers/gebruikers, persoonlijke, culturele of milieu-informatie?

Voor aanvragers met vertrouwelijke data of metadata moeten verwijzingen worden opgenomen naar de volgende zaken:

- speciale procedures voor het beheersen van het risico van schending van de vertrouwelijkheid;
- voorwaarden voor verspreiding, toegangsbescherming en gebruik;
- procedures voor het beoordelen van het vertrouwelijkheidsrisico en het treffen van maatregelen voor ofwel anonimisering van bestanden of beveiligde toegangsverlening;
- scholing van medewerkers in het beheer van digitale objecten met een vertrouwelijkheidsrisico;
- richtlijnen voor het verantwoord deponeren, downloaden en gebruiken van (potentieel) vertrouwelijke data en metadata.

Het beheer van de bijbehorende rechten en compliancecontroles moet worden behandeld bij Rights Management (R02). Maatregelen voor de bescherming van digitale objecten moeten worden geadresseerd onder Security (R16).

Alle organisaties met een verantwoordelijkheid voor data hebben de morele plicht die data zodanig te beheren dat het niveau van dat beheer voldoet aan de verwachtingen van de Designated Community.

Voor digitale archieven met data van individuen, organisaties, inheemse volkeren of beschermde onderwerpen of soorten, gelden aanvullende wettelijke en ethische normen ten aanzien van de bescherming van hun rechten.

Openbaarmaking van deze data zou kunnen leiden tot persoonlijke schade, schending van commerciële vertrouwelijkheid of bekendmaking van cruciale informatie, zoals de locatie van een bedreigde diersoort of een archeologische site.

Als er een risico bestaat dat er bijvoorbeeld per ongeluk traceerbare data worden aangeleverd, dan dient het digitale archief passende maatregelen te treffen voor de verwerking (en verwijdering) van die data in overeenstemming met de wet.

Als het digitale archief op dit moment toegang verleent tot gevoelige data of metadata, is het gewenste compliancieniveau “Implemented: the requirement has been fully implemented by the repository” (Geïmplementeerd: aan de vereiste wordt door het digitale archief volledig voldaan).

Uit de onderbouwing moet blijken dat de aanvrager inzicht heeft in het wettelijk kader en de relevante gedragsregels en hiervoor ook gedocumenteerde procedures heeft vastgelegd om naleving af te dwingen.

Deze Requirement omvat ook de passende verwerking van data en metadata over de gebruikers van digitale archiefdiensten.

Governance & Resources (R05)

R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission. (Het digitale archief beschikt over voldoende financiële middelen en voldoende gekwalificeerd personeel dat op een heldere manier wordt aangestuurd voor een doeltreffende uitvoering van de missie.)

Zelfverklaard compliancieniveau:

Antwoord

Toelichting

Deze Requirement weerspiegelt de noodzaak van transparantie over financiering, bestuur, verantwoordelijkheden en besluitvorming. De onderbouwing moet aantonen dat het digitale archief een duidelijk systeem van governance heeft en over voldoende personeel en financiën beschikt om zijn missie te vervullen.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- beschrijvingen en diagrammen van bestuurlijke instanties, groepen en hiërarchieën;

- tijdlijnen voor de verkrijging en verlenging van financiering van operationele kosten en aanwerving, waarbij in aanmerking wordt genomen dat permanente financiering niet absoluut kan worden gekwantificeerd of gegarandeerd;
- bewijs dat het digitale archief een erkende instelling is of wordt gehost door een erkende instelling (die stabiliteit en duurzaamheid op lange termijn ondersteunt) die past bij de Designated Community;
- bewijs dat het digitale archief kan voldoen aan zijn verplichtingen, waaronder voldoende financiële en personele middelen, IT-middelen en een budget voor de nodige externe betrokkenheid.

De beschikbaarheid van toereikende expertise wordt behandeld onder Expertise (R06).

De antwoorden en onderbouwing moeten aantonen dat het digitale archief kan voldoen aan zijn verplichtingen, waaronder voldoende financiële en personele middelen, IT-middelen en een budget voor de nodige externe betrokkenheid.

De besluitvormingsprocessen van bestuur en management en andere betrokken entiteiten in de organisatie moeten inzichtelijk worden gemaakt, bijvoorbeeld met organigrammen.

In de onderbouwing dient te worden toegelicht hoe vaak de periodieke verlenging van de financiering plaatsvindt.

Hierbij wordt in aanmerking genomen dat digitale archieven volgens uiteenlopende financieringsmodellen werken, vaak met beperkte middelen, maar transparantie over deze zaken is van belang voor de betrouwbaarheid.

Uiteraard is financiering in het verleden geen garantie voor toekomstige financiering, maar het kan wel indicatief zijn om de historische ontwikkeling van het digitale archief te schetsen.

Andere relevante gegevens zijn mogelijk de balans tussen structurele en projectfinanciering, het totale aantal medewerkers in fte's en de verhouding tussen vast en tijdelijk personeel.

Expertise & Guidance (R06)

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback-either in-house, or external. (Het digitale archief wint structureel advies en feedback van deskundigen in, zowel intern als extern.)

Zelfverklaard compliancieniveau:

Antwoord

Toelichting

Een digitaal archief moet weten welke vaardigheden noodzakelijk zijn om de aangeboden diensten te kunnen leveren en ervoor zorgen dat die vaardigheden aanwezig zijn, hetzij bij eigen medewerkers, hetzij door externe betrokkenheid. Een doeltreffend digitaal archief speelt in op ontwikkelingen op het gebied van datatypes, datavolumes en dataverwerkingsnelheden. Daarnaast maakt het gebruik van de meest effectieve nieuwe technologieën om toegevoegde waarde te kunnen blijven bieden aan de Designated Community.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- hoe de begeleiding en de expertise een afspiegeling zijn van de wetenschappelijke scope van het digitale archief, voor zover relevant;
- hoe het digitale archief de interne aanwerving en externe betrokkenheid afstemt op de diensten die het verleent;
- hoe het digitale archief erop toeziet dat zijn personeel toegang heeft tot blijvende scholingsmogelijkheden en professionele ontwikkeling;
- de breedte en diepte van de deskundigheid van zowel de organisatie als haar personeel, inclusief relevante gelieerde organisaties, zoals (inter)nationale instanties, met betrekking tot de missie;
- eigen adviseurs of externe adviescommissie bestaande uit technici, conserveringsdeskundigen, datawetenschappers of vakspecialisten;
- de wijze waarop het digitale archief met de adviseurs communiceert.

Uit de antwoorden en de onderbouwing moet blijken dat het digitale archief over voldoende interne deskundigheid beschikt en is verbonden met een breed advies- en begeleidingsnetwerk.

De onderbouwing moet een beeld schetsen van zowel de dagelijkse werkzaamheden als het monitoren van mogelijke toekomstige uitdagingen (d.w.z. om voeling te houden met technologische ontwikkelingen en de Designated Community).

Beheer van digitale objecten

Provenance and authenticity (R07)

R07. The repository guarantees the authenticity of the digital objects and provides provenance information. (Het digitale archief waarborgt de integriteit van de digitale objecten en verschaft informatie over hun herkomst.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Het digitale archief moet aantonen dat het een beheersysteem voor data en metadata heeft dat herkomstinformatie bijhoudt om tijdens de deponering, bij de preservatie en bij de toegang tot die data de authenticiteit te waarborgen. Alle bewuste wijzigingen van data en metadata moeten worden vastgelegd, met vermelding van de reden en de initiator van de wijziging. Bij authenticiteit gaat het om de mate van betrouwbaarheid en de herkomst van de oorspronkelijke aangeleverde data, inclusief de relatie tussen de oorspronkelijke data en de data zoals ze worden uitgeleverd.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- het beleid voor wijzigings- en versiebeheer en de wijze waarop dit beleid en de geregistreerde wijzigingen worden bekendgemaakt aan depotgevers en gebruikers;
- de herkomstinformatie en audit trails die worden geregistreerd bij de

- verwerking en het versiebeheer van data en metadata;
- de wijze waarop het digitale archief de essentiële kenmerken van verschillende versies van hetzelfde bestand met elkaar vergelijkt;
 - identificatiecontroles van depotgevers.

De antwoorden en de onderbouwing moeten een duidelijk inzicht geven in de processen waarmee de data-authenticiteit wordt gewaarborgd tijdens de gehele cyclus van curatie en preservering, inclusief het niveau van handmatige en geautomatiseerde praktijken.

In de onderbouwing moeten audit trails, d.w.z. schriftelijke registraties van op met de data uitgevoerde activiteiten, worden beschreven.

Deposit & Appraisal (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users. (Het digitale archief accepteert data en metadata op basis van vooraf gedefinieerde criteria, zodat datagebruikers er zeker van kunnen zijn dat die data en metadata voor hen relevant en begrijpelijk zijn.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

De Appraisal-functie ('waardering') is cruciaal om te kunnen beoordelen of digitale objecten voldoen aan alle selectiecriteria en om het beste beheer te waarborgen met het oog op hun preservering. De juiste waardering betekent dat gedeponeerde digitale objecten relevant en begrijpelijk (kunnen) zijn voor de Designated Community.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- elk gedocumenteerd deponeringsproces waarin maatregelen zijn opgenomen die waarborgen dat data en metadata toereikend zijn voor duurzame preservering;
- een collectiebeleid of procedures met richtsnoeren voor de selectie van digitale objecten;
- criteria voor prioriteiten en verschillende curatie- of preserveringsniveaus die bij de waardering worden vastgesteld;
- het beleid voor digitale objecten die niet binnen de missie of het collectieprofiel passen;
- procedures om vast te stellen dat de voor interpretatie en gebruik van de digitale objecten benodigde metadata aanwezig zijn;
- automatische beoordeling van de aanwezigheid van metadata voor relevante schema's;
- het beleid van het digitale archief indien de verstrekte metadata ontoereikend zijn voor duurzame preservering;
- een lijst met voorkeursformaten;
- aanwezige controlemechanismen om erop toe te zien dat depotgevers zich aan de voorkeursformaten houden;
- de aanpak van digitale objecten die worden gedeponerd in niet-voorkeursformaten;
- de overdracht van beheer en verantwoordelijkheid tijdens de overgang van de

depotgever naar het digitale archief.

Deze Requirement heeft betrekking op de selectiecriteria die bij deponering worden toegepast. Voor de stappen die het digitale archief tijdens de preservingsproces zet, moet Data Quality (R11) worden gebruikt.

De antwoorden en de verantwoording moeten aantonen dat in het digitale archief alleen data en metadata worden geaccepteerd die aansluiten bij het collectiebeleid.

Voor duurzame preservering van de data en relevant gebruik door de Designated Community moeten medewerkers met alle benodigde informatie en procedures bekend zijn en over de nodige deskundigheid beschikken.

Wellicht moeten de selectiecriteria na verloop van tijd worden bijgesteld en moeten digitale objecten opnieuw worden gewaardeerd om de collectie relevant en bruikbaar te houden voor de Designated Community, met name vanwege nieuwe technologieën, sociale normen of wetgeving (denk aan databescherming of IE- rechten). Dit kan gevolgen hebben voor de herwaardering; zie Preservation Plan (R09).

Preservation plan (R09)

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way. (Het digitale archief neemt verantwoordelijkheid voor duurzame preservering en doet dit op een gestructureerde en goed gedocumenteerde manier.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Het digitale archief, de depotgevers van de data en de Designated Community moeten inzicht hebben in de verantwoordelijkheden die de duurzame preservering van data en metadata met zich meebrengt. Er moeten gedocumenteerde procedures zijn en garanties dat die procedures worden nageleefd.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- het gedocumenteerde preservingsbeleid, inclusief de vraag of hierin formaatmigratie, emulatie e.d. zijn opgenomen; waarborgen van de integriteit op bit-niveau is van groot belang maar niet toereikend voor preservering;
- bestandsformaten en metadata-schema's voor duurzame preservering;
- hoe de mate van verantwoordelijkheid voor de preservering van elk object is gedefinieerd;
- plannen met betrekking tot toekomstige migraties of soortgelijke maatregelen om de dreiging van technologische veroudering af te wenden;
- gedocumenteerde activiteiten die relevant zijn voor de preservering, waaronder beheeroverdracht, criteria voor te verstrekken informatie en metadata voor

preserveringsinformatie;

- maatregelen om te waarborgen dat deze activiteiten plaatsvinden;
- de minimale bewaar- en/of preserveringstermijnen;
- hoe vaak de digitale objecten opnieuw worden gewaardeerd en wat de mogelijke uitkomsten van herwaardering zijn;
- het beleid van het digitale archief voor de verwijdering van data en metadata uit de collecties, en wat de gevolgen voor persistent identifiers zijn.

De rechten van het digitale archief, inclusief het preserveringsrecht, worden behandeld onder Rights Management (R02). Integriteit op bit-niveau wordt behandeld onder Storage and Integrity (R14). Aanvaardbare bestandsformaten bij deponering dienen aan de orde te komen bij Deposit and Appraisal (R08). Maatregelen om ervoor te zorgen dat bestandsformaten, schema's en content geschikt zijn voor de Designated Community vallen onder Reuse (R13).

Het begrip 'Preservation plan' verwijst naar het feit dat er een gedocumenteerd beleid moet zijn voor het definiëren en uitvoeren van preserveringsactiviteiten. De Requirements maken geen onderscheid tussen een preserveringsbeleid, -plan, -strategie of -actieplan.

Uit de antwoorden en de onderbouwing moet blijken dat er heldere en beheerde documentatie is voor het waarborgen van: (1) een gestructureerde benadering van duurzame preservering, (2) blijvende toegankelijkheid voor datatypen ondanks formaatwijzigingen en (3) toereikende documentatie voor het gebruik door de Designated Community. Geef in het antwoord op de Requirement aan of het digitale archief preserveringsniveaus heeft gedefinieerd en, zo ja, hoe deze worden toegepast. Het preserveringsplan moet zodanig worden beheerd dat tijdig en op een stabiele manier wordt ingespeeld op veranderingen in de datatechnologie of de behoeften van gebruikers.

Zijn er verschillen tussen de preserveringsniveaus van bepaalde soorten objecten of collecties? Leg dan uit wat de verschillen in het preserveringsbeleid zijn en welke criteria worden toegepast om het preserveringsniveau te bepalen. Dat kan bijvoorbeeld relevant zijn als de bestandsgrootte van een object of de gevoeligheid van de desbetreffende data bepaalt hoeveel redundante kopieën er worden gemaakt, of wanneer alleen in voorkeursformaten aangeleverde objecten naar standaard preserveringsformaten worden geconverteerd en in de toekomst worden gemigreerd.

Er dienen een beleid en gedocumenteerde procedures voor herwaardering te bestaan om veranderingen in de preserveringsniveaus van digitale objecten (of hun verwijdering uit het digitale archief) te beheren.

Staat in het antwoord geen link naar een gedocumenteerd preserveringsbeleid, dan kan het compliancieniveau niet hoger zijn dan 'In Progress'. Bovendien dient dan voor de volgende review wel zo'n gedocumenteerd preserveringsbeleid beschikbaar te zijn.

Quality Assurance (R10)

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations. (Het digitale archief heeft voldoende deskundigheid in huis om de technische kwaliteit van de data en metadata te garanderen en zorgt ervoor dat eindgebruikers over voldoende informatie beschikken om die kwaliteit te beoordelen.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Verschillende digitale archieven hanteren verschillende conserveringsniveaus voor data, metadata en documentatie, afhankelijk van de behoeften en verwachtingen van hun depotgevers en de Designated Community. Kwaliteitsborging door het digitale archief garandeert dat digitale objecten voldoen aan een aantal standaardcriteria, onder meer voor aanvaardbare formaten, metadata-schema's, metadata-content en links naar andere digitale objecten. Deze borging betreft veeleer de 'technische kwaliteit' dan de 'wetenschappelijke kwaliteit' van de oorspronkelijke totstandkoming of verzameling van digitale objecten vóór deponering, al moet het digitale archief ook zorgen voor voldoende informatie over de digitale objecten waarmee de Designated Community hun bruikbaarheid kan vaststellen. Data of de bijbehorende metadata kunnen kwaliteitsproblemen hebben die relevant zijn voor hun wetenschappelijke waarde, maar dit mag niet verhinderen dat ze worden gebruikt wanneer een gebruiker dankzij de beschikbare documentatie op goede gronden kan besluiten dat ze bruikbaar zijn.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de door het digitale archief gekozen benadering van data- en metadatakwaliteit, inclusief variaties voor verschillende niveaus van preservering;
- de normen waaraan data, metadata en documentatie moeten voldoen om te worden geaccepteerd voor preservering en toegang; of het hierbij gaat om algemene externe standaarden, intern ontwikkelde standaarden of standaarden die specifiek zijn voor een bepaalde doelgroep of werkwijze;
- de kwaliteitscontroles die worden uitgevoerd om de volledigheid en inzichtelijkheid van data en metadata te waarborgen;
- het beleid voor het oplossen van problemen, bijv. of problematische digitale objecten voor herstel worden teruggestuurd naar de depotgever, hersteld door het digitale archief, voorzien van kwaliteitswaarschuwingen en/of opgenomen in de bijbehorende metadata;
- het beleid voor het beheer van veranderingen in verwachte standaarden (bijv. nieuwe of gewijzigde dataformaten of metadata-schema's) als antwoord op veranderingen in de technische omgeving of in de behoeften van de Designated Community;
- links naar andere data en metadata van andere digitale objecten, zoals gerelateerde digitale objecten, publicaties of gecontroleerde vocabularia en ontologieën.

Deze Requirement heeft betrekking op kwaliteitsstandaarden voor data en metadata en de kwaliteitsborging tijdens de preservering. Selectiecriteria komen aan de orde bij Deposit and Appraisal (R08). Maatregelen om digitale objecten in de loop der tijd geschikt te houden voor het beoogde doel worden behandeld onder Preservation Plan (R09).

Maak in het antwoord duidelijk dat het digitale archief ervan doordrongen is welke kwaliteitsniveaus redelijkerwijs van depotgevers kunnen worden verwacht.

Zorg ervoor dat uit de onderbouwing blijkt hoe kwaliteit tijdens het conserveringsproces wordt geborgd. Beschrijf ook welke verwachtingen de beoogde doelgroep heeft ten aanzien van kwaliteit.

Van zowel het digitale archief als de depotgevers wordt verwacht dat elk mogelijk aspect van data of metadata dat niet aan de verwachte standaard voldoet, goed wordt gedocumenteerd.

De kwaliteitsbeoordeling is nog belangrijker wanneer de beoogde doelgroep multidisciplinair is, omdat de gebruikers mogelijk geen persoonlijke ervaring hebben met het vaststellen van de kwaliteit aan de hand van alleen de data.

Workflows (R11)

R11. Digital object management takes place according to defined workflows from deposit to access. (Bij het beheer van digitale objecten wordt gebruikgemaakt van gedefinieerde workflows vanaf het moment van deponering tot en met de ontsluiting.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Om Quality Assurance (R10) te kunnen realiseren, is het noodzakelijk om ad hoc-activiteiten te vermijden en een consistente werkwijze voor alle digitale objecten en bij alle functies van het digitale archief door te voeren. Hiervoor moeten workflows zijn gedefinieerd en gedocumenteerd en moeten wijzigingen in die workflows worden beheerd. Workflows kunnen worden gespecificeerd in een mix van standaard werkprocedures, beschrijvingen van bedrijfsprocessen en diagrammen, waarin de gangbare praktijk is vastgelegd met mechanismen voor de afhandeling van uitzonderingen.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- beschreven workflows en bedrijfsprocessen met betrekking tot de uitgevoerde conserveringsniveaus;
- de wijze waarop workflows worden afgestemd op verschillende typen data en metadata;
- de besluitvorming binnen de workflows;
- veranderingmanagement van workflows;
- de mogelijkheid om de uitvoering van workflows te bewaken, inclusief mechanismen voor de afhandeling van uitzonderingen.

Het doel van deze Requirement is te laten zien dat alle workflows zijn gedocumenteerd. Hierbij moet worden vermeld of er verschillende workflows zijn voor verschillende beveiligingsniveaus die zijn genoemd in de antwoorden onder Legal and Ethical (R04). Workflows kunnen kwalitatieve en kwantitatieve outputcontroles bevatten, maar de details van controles en naleving moeten worden behandeld onder Quality Assurance (R10).

Uit de antwoorden en de onderbouwing moet blijken dat alle activiteiten in alle processen op een consistente, nauwgezette en goed gedocumenteerde manier worden beheerd en dat alle mogelijke wijzigingen in die processen correct worden uitgevoerd, geëvalueerd, opgeslagen en beheerd.

Er kan worden gelinkt naar gedetailleerde beschrijving van workflows als die openbaar zijn, maar deze Requirement moet vooral de zekerheid bieden dat de workflows bestaan en dat ze goed gedocumenteerd zijn.

Workflows kunnen eventueel worden geïllustreerd met procesdiagrammen of beslisbomen.

Het benadrukken van de relaties met processen uit de overige Requirements kan inzichtelijk maken hoe afzonderlijke workflows samen een compleet systeem vormen.

Discovery and Identification (R12)

R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation. (Het digitale archief stelt gebruikers in staat de digitale objecten in het archief te ontsluiten en er altijd met correcte citaties naar te verwijzen.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Om data en metadata te kunnen delen, moet je ze op een doeltreffende manier kunnen vinden en ontsluiten. En op het moment dat digitale objecten ontsloten zijn, moet je er goed naar kunnen verwijzen, onder andere met persistent identifiers die ervoor zorgen dat de data ook in de toekomst toegankelijk blijven.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de zoekfuncties die het digitale archief aanbiedt;
- de standaarden waaraan een doorzoekbare catalogus van metadata voldoet;
- de manier waarop wordt gewaarborgd dat identifiers uniek en persistent zijn;
- geautomatiseerd verkrijgen van metadata;
- of het digitale archief, of de data en metadata, zijn opgenomen in een of meer specifieke of generieke bronnenregisters;
- aanbevelingen voor datacitaties.

Aanvragers moeten aantonen hoe zij gebruikmaken van een extern systeem van persistent identifiers (PIDs), of hun eigen aanpak beschrijven om te waarborgen dat identifiers wereldwijd uniek en persistent blijven. De enkele inzet van een derde partij ten behoeve van PID-creatie en -gebruik is niet toereikend. Aanvragers moeten ook beschrijven hoe zij erop toezien dat identifiers in de loop der tijd naar de juiste data of metadata blijven leiden, inclusief de versieregels die van toepassing zijn wanneer een nieuwe identifier voor een digitaal object

wordt gemaakt. Digitale archieven die geen eigen oplossing voor persistent identifiers hebben, kunnen voor deze Requirement niet het niveau “Implemented: the requirement has been fully implemented by the repository” behalen.

Toon in de onderbouwing met bewijs aan dat de preservering van data en metadata bevorderlijk is voor het vinden en ontsluiten van duidelijk gedefinieerde en geïdentificeerde digitale objecten. Toon ook aan dat gebruikers in staat worden gesteld om conform relevante (bijv. domeinspecifieke) standaarden koppelingen met gerelateerde digitale objecten te maken.

Het moet duidelijk zijn hoe data worden geciteerd, zodat individuen en organisaties die een bijdrage hebben geleverd aan het maken van die data, op een correcte manier worden aangehaald en de data aan hen worden toegeschreven.

Reuse (R13)

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use. (Het digitale archief maakt hergebruik van de digitale objecten voor de lange termijn mogelijk en zorgt ervoor dat de juiste informatie beschikbaar is voor een goed begrip en gebruik ervan.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Digitale archieven moeten ervoor zorgen dat data altijd begrijpelijk zijn en ook in de toekomst op een doeltreffende manier kunnen worden gebruikt, ook als er iets verandert in de technologie of de basiskennis van de Designated Community. Het doel van deze Requirement is om te bepalen of de getroffen maatregelen afdoende zijn om hergebruik van data te waarborgen.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de manieren waarop het digitale archief de contacten met zijn Designated Community onderhoudt om te weten wat de behoeften van gebruikers zijn;
- de dataformaten, metadata-schema's, gecontroleerde vocabularia en ontologieën waarmee hergebruik mogelijk wordt gemaakt, en in hoeverre deze voorzien in de behoeften van de doelgroep;
- de bij uitlevering van de data verstrekte metadata en documentatie ter bevordering van inzicht en hergebruik, toegesneden op de Designated Community; dit kan informatie omvatten die specifiek is voor een datatype, bijv. handleidingen, calibratiegegevens, foto's of protocollen;
- maatregelen om te waarborgen dat data en metadata begrijpelijk blijven;
- het beheer van veranderingen in data, metadata, documentatie of andere informatie ten behoeve van hergebruik.

De beantwoording van deze Requirement dient zich te concentreren op de betrokkenheid bij de

Designated Community, de identificatie van haar behoeften en de wijze waarop in die behoeften wordt voorzien.

Uit de antwoorden en de onderbouwing moet duidelijk worden dat er bij het digitale archief voldoende kennis aanwezig is over vormen van hergebruik en over de behoeften van de Designated Community wat betreft gangbare praktijken, technische omgeving en (de naleving van) relevante standaarden.

Veranderingen in de technologie en in de door de Designated Community gebruikte methodieken en normen kunnen betekenen dat nodig eens moet worden nagedacht over het formaat waarin de data worden verspreid.

Ook relevante hoogwaardige metadata die voldoen aan een generieke en/of domeinspecifieke standaard moeten in de onderbouwing aan bod komen.

Deze informatie is van groot belang voor het ontwerpen van conserveringsprocessen die ervoor zorgen dat digitale objecten ook in de toekomst begrijpelijk en bruikbaar blijven voor de Designated Community.

Gebruikt het digitale archief alleen een generieke metadatastandaard (zoals Dublin Core of DataCite)? Maak dan in de onderbouwing duidelijk dat hiermee gewaarborgd is dat de gepreserveerde content ook in de toekomst begrijpelijk blijft voor de Designated Community.

Informatietechnologie en beveiliging

Storage & Integrity (R14)

R14. The repository applies documented processes to ensure data and metadata storage and integrity. (Het digitaal archief maakt gebruik van gedocumenteerde processen om de veilige opslag en de integriteit van data en metadata te waarborgen.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Behalve dat ze ‘archiefexemplaren’ van digitale objecten in stand moeten houden, dienen digitale archieven de data en metadata ook op te slaan vanaf het moment van deponering, ten behoeve van de curatie en preservatie, en om ze te ontsluiten voor gebruikers. Voor elke opslaglocatie moeten maatregelen van kracht zijn om te waarborgen dat onopzettelijke of ongeoorloofde wijzigingen kunnen worden gedetecteerd en dat de correcte versies van data en metadata kunnen worden hersteld.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- processen en documenten waarmee wordt geborgd dat de medewerkers van het digitale archief een goed inzicht hebben in alle opslaglocaties en

hoe deze worden beheerd;

- de strategie van het digitale archief ten aanzien van meerdere kopieën;
- de risicobeheertechnieken waarmee deze strategie wordt uitgevoerd;
- procedures voor de bewaking van en het omgaan met kwaliteitsverlies van opslagmedia;
- procedures om te waarborgen dat data en metadata alleen worden verwijderd in het kader van een goedgekeurd en gedocumenteerd proces;
- controles (stabiliteitstests) die worden uitgevoerd om te verifiëren dat een digitaal object niet is gewijzigd of beschadigd tussen archivering en gebruik.

Opslag- en integriteitsmaatregelen moeten hier (R14) aan de orde komen, niet bij de beantwoording van Technical Infrastructure (R15) of Security (R16). Details over de registratie van opzettelijke veranderingen aan de data en metadata moeten worden gegeven onder Provenance & Authenticity (R07).

Uit de antwoorden en de onderbouwing moet duidelijk worden op welke opslaglocaties preserveringsprocessen plaatsvinden, hoe data en metadata in elk van die omgevingen worden beheerd, en dat er is voorzien in processen om wijzigingen in opslagdocumentatie te bewaken en te beheren.

Standaardprocedures moet zodanig toereikend zijn dat verschillende opslagbeheerders tot dezelfde uitkomsten komen, ook als zij afzonderlijk dezelfde taken uitvoeren.

Bewijzen kunnen bijvoorbeeld bestaan uit datastroomdiagrammen waarin de deponerings-, preserverings- en toegangslocaties (met eventuele toegangsbeperkingen) zijn opgenomen.

Voor de archiefopslag zou het bewijs beschrijvingen kunnen omvatten van multisite-afspraken (on-site, near-site, off-site), de mix van opslagmedia en de redundantie (inclusief integriteit via checksums).

Technical Infrastructure (R15)

R15. The repository is managed on well-supported operating systems and other core infrastructural software and hardware appropriate to the services it provides to its Designated Community. (Het digitale archief wordt beheerd met goed ondersteunde besturingssystemen en andere belangrijke infrastructurele software en maakt gebruik van hardware- en softwaretechnologieën die geschikt zijn voor de dienstverlening aan de Designated Community.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Voor maximale beschikbaarheid van de dienstverlening moeten digitale archieven over betrouwbare, stabiele infrastructuren beschikken.

De details van de technische infrastructuur verschillen sterk per digitaal archief. De antwoorden en de onderbouwing moeten aantonen dat de oplossing van de aanvrager,

inclusief hardware en software, goed wordt beheerd en relevant en geschikt is voor de functies van het digitale archief en het gebruik door de Designated Community.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de software die het digitale archief gebruikt voor deponering, curatie, preservatie en toegangsbeheer; wordt de software door gebruikers ondersteund, is deze open source of lokaal ontwikkeld?
- de gekozen aanpak van het IT-servicebeheer en de daarvoor gespecificeerde functies (zoals systeemdokumentatie, softwareregisters, code-archieven, infrastructuurplanning);
- de geldende internationale, door gebruikers ondersteunde of andere standaarden voor technische infrastructuur en de wijze waarop de naleving wordt bewaakt;
- het versiebeheersysteem dat wordt gebruikt voor door het digitale archief gegenereerde software;
- getroffen maatregelen om ervoor te zorgen dat de beschikbaarheid, bandbreedte en connectiviteit toereikend zijn voor de behoeften van de Designated Community;
- aanwezige processen om de noodzaak van technische wijzigingen te bewaken en te beheren, ook in reactie op veranderende behoeften op het gebied van Preservation (R10) en Reuse (R13) bij de Designated Community.

De technische aspecten van de bedrijfscontinuïteit, het rampenplan en de opvolgingsplanning zijn hier weliswaar relevant, maar het beheer daarvan moet aan bod komen bij Continuity of Service (R03). Deze Requirement heeft geen betrekking op maatregelen voor Security (R16) en Storage & Integrity (R14).

Informatie over bestandsformaten en metadata-schema's moet worden gegeven bij Deposit & Appraisal (R08) en Reuse (R13). Standaarden die niet gericht zijn op techniek of beveiliging moeten worden behandeld onder Quality Assurance (R10).

De workflows en de mensen die de dienstverlening van het digitale archief verzorgen, moeten worden ondersteund door een adequate technologische infrastructuur die aansluit op de behoeften van de Designated Community en die het digitale archief in staat stelt kortstondige rampen het hoofd te bieden.

De reviewers willen bewijs zien dat de aanvrager inzicht heeft in het bredere ecosysteem van de standaarden, instrumenten en technologieën voor het beheer en de preservatie van (onderzoeks)data.

Ook moet duidelijk worden gemaakt dat de gekozen technische opties aansluiten bij de lokale vereisten, zoals de technologieën die door de Designated Community worden gebruikt of een bandbreedte die toereikend is voor de verwachte vraag.

Voorbeelden van relevante technische standaarden zijn die van W3C, ISO en IEEE.

Security (R16)

R16. The repository protects the facility and its data, metadata, products, services, and users. (Het digitale archief beschermt zowel de faciliteit zelf als de data, producten, diensten en

gebruikers.)

Zelfverklaard compliancenniveau:

Antwoord

Toelichting

Het digitale archief brengt mogelijke bedreigingen in kaart, bepaalt de risico's en zorgt voor een consistent beveiligingssysteem.

Er moet een beschrijving zijn van de scenario's die het digitale archief hanteert in geval van kwaadwillige handelingen, menselijke fouten of technische storingen die een bedreiging vormen voor het digitale archief zelf of voor de data, metadata, producten, diensten of gebruikers. Het digitale archief bepaalt hoe waarschijnlijk dergelijke scenario's zijn, hoe groot de impact ervan is, welke risiconiveaus acceptabel zijn en welke maatregelen moeten worden getroffen om de bedreigingen voor het digitale archief en de Designated Community af te wenden. Dit dient een doorlopend proces te zijn.

In het antwoord en de onderbouwing moet worden verwezen naar de volgende zaken:

- de voor verschillende data, metadata en omgevingen vereiste beveiligingsniveaus en hoe die worden ondersteund;
- het IT-beveiligingssysteem, de medewerkers die op een of andere manier betrokken zijn bij de beveiliging en de instrumenten voor risicoanalyse;
- maatregelen om de faciliteit te beschermen; de beveiliging van de gebouwen en ruimtes waar digitale objecten worden bewaard;
- de veiligheids- of beveiligingsstandaarden waarnaar het digitale archief verwijst of waaraan het voldoet;
- de authenticatie- en autorisatieprocedures die worden gehanteerd voor het waarborgen van beveiligde toegang tot de gebruikte systemen.

De antwoorden hoeven geen betrekking te hebben op maatregelen voor Storage and Integrity (R14) of de algemene Technical Infrastructure (R15).

Uit de antwoorden en de onderbouwing moet blijken dat de aanvrager begrijpt welke technische risico's verbonden zijn aan zowel de digitale en fysieke omgeving als de dienstverlening aan de Designated Community.

Er moeten voorzieningen zijn getroffen om beveiligingsincidenten te voorkomen, op te sporen en te bestrijden.

De authenticatie- en autorisatieprocedures moeten toereikend zijn voor het waarborgen van de beveiliging van de data en metadata in het digitale archief tijdens alle stappen van de workflow (bijv. met tweetraps-authenticatie voor gevoelige informatie).

Aangetoond moet worden wat het algemene beleid voor de beveiliging van alle systemen is. Denk hierbij aan onder andere netwerkbeveiliging, detectie van ongeautoriseerde toegang, fysieke beveiliging van de faciliteit en het wachtwoordbeleid.

Als in de beantwoording bij Legal and Ethical (R04) wordt verwezen naar de bewaring van gevoelige digitale objecten, moet hier expliciet worden vermeld welke aanvullende maatregelen zijn getroffen om deze data en metadata te beschermen.

Opmerkingen/feedback

Feedback aanvrager

Deze Requirements dienen niet als statisch te worden beschouwd. We staan open voor input en ideeën waarmee we de certificeringsprocedure van CoreTrustSeal kunnen verbeteren. In toekomstige versies nemen we uw opmerkingen en bijdragen over de kwaliteit en relevantie van de Requirements graag mee.

Antwoord