



Assessment Information

[CoreTrustSeal Requirements 2020–2026](#)

Repository:	E-depot of Erfgoed Leiden en Omstreken
Website:	https://erfgoedleiden-e-depot.access.preservica.com/
Certification period:	Feb. 27, 2026 - 26 February 2029
Requirements version:	CoreTrustSeal Requirements 2023-2025

This repository is owned by: **Erfgoed Leiden en Omstreken**

CORE TRUSTWORTHY DATA REPOSITORIES REQUIREMENTS

Background Information

Re3data Identifier

Please fill your Re3data identifier from the website: <https://www.re3data.org/>

Response:

<https://doi.org/10.17616/R31NJNT9>

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Repository type

Please select your repository type.

Response:

- Generalist repository

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Overview

Provide a short overview of key characteristics of the repository, reflecting the repository type selected. This should include information about the scope and size of data collections, data types and formats. Further contextual information may also be added.

Response:

Erfgoed Leiden en Omstreken (ELO) is part of the municipality of Leiden. ELO performs services related to historical preservation, archaeology and archiving for the municipality of Leiden, as well as ten other surrounding municipalities and services such as the fire department and municipal health services. More on the services provided to the municipalities can be found here: <https://www.erfgoedleiden.nl/werkgebied/partners>. ELO is responsible for physical archives and digital born and digitised archives. In accordance with the Dutch Public Records Act (Archiefwet) 1995, the e-depot of ELO functions as a repository for our partners. Currently the municipalities of Katwijk, Leiden, Oegstgeest and Noordwijk have joined the ELO e-depot. Kaag en Braassem and Nieuwkoop are expected to do so in the near future. Because of the obligation to deposit one's digital archives to a depository 20 years after closure of the dossiers (10 years when the new Public Records Act comes into effect), we expect more of ELO's partners to join the e-depot in the (near) future. The e-depot, hosted in the cloud edition of Preservica, serves as a repository for digital born archives, or digitised archives of which the original physical document has been replaced by the digital one (and the physical document destroyed). Digital representations of ELO's physical records are stored in another system, and are out of scope for this application. The content of the e-depot mainly consists of municipal archives that, according to the Dutch Public Records Act 1995, have to be stored in perpetuity. Which documents have to be archived is based on the Selection lists by The Association of Dutch Municipalities (VNG). See <https://vng.nl/artikelen/selectielijst>. Archives stored in the e-depot mainly consist of building permits, recordings of council meetings, zoning plans, websites and the content of records management systems. These are all stored together with the accompanying metadata. Metadata are stored according to the MDTO (Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie) standard. See <https://www.nationaalarchief.nl/archiveren/mdto>. ELO also stores digital archives of private persons or organisations if they are of historical value to the municipality of Leiden and/or one of our partners. Private collections tend to have less metadata attached to them than those of local governments. File

E-depot of Erfgoed Leiden en Omstreken

formats can vary, but most are pdf, docx, xlsx, jpeg, jp2, tif, png, mp3, mp4 and obj. ELO has listed all accepted file formats in the e-depot in the Delivery requirements. See https://www.erfgoedleiden.nl/images/e-depot/Aanlevervoorwaarden_Digitaal_Archief_Erfgoed_Leiden_eo_v30_22-09-2025.pdf.

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Designated Community

A clear definition of the Designated Community demonstrates that the applicant understands the scope, knowledge base, and methodologies—including preferred software/formats—of the group(s) of users at whom the curation and preservation measures are primarily targeted. The definition should be specific so that reviewers can assess whether that community is being served in the responses to other requirements.

Response:

The designated community of ELO is described in paragraph 11.1 of the Preservation Policy (https://www.erfgoedleiden.nl/images/e-depot/Preserveringsbeleid_ELO_v10.pdf). It consists of two main groups: - The general public - The local government employee. Because transferred municipal archives are supposed to be made public according to the Dutch Public Act 1995, these digital archives need to be open to all, and understandable to all. The general public can be split up into two groups. The first is the researcher. This group is looking for larger datasets with clear provenance. They are mostly capable of handling more complicated file formats that might need specific software to be rendered and processed. The second is the citizen. This group will look for a specific document, for example a building permit of their own house or a council meeting in which a specific subject relevant to them is being discussed. The government employee is only in scope when dealing with archives that are not open to the general public (yet). This can be the case when archives are transferred to the e-depot before they have reached the date (20 years after closing of dossiers) of becoming public records, or in the case of an outplaced archive. Because the knowledge base of these groups can vary, ELO presumes a low knowledge base so everybody can work with our archives. This means we provide file formats that, if possible, are based on an open standard, are well known and don't need specific software to render them. Whenever this is not possible, for example with geographical file formats, we will provide the original documents (for those who need them and know how to work with them) as well as an easily accessible derivative. This could for example be a static pdf of a map that would have been interactive in a GIS application. ELO also creates filters and facets based on the search behaviour of the different groups. A search term used by a government employee will differ from that used by a citizen, for example the use of a case number versus the use of a street name to find a building permit. We take this into account and build in these various options of finding a document.

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Levels of Curation

Please fill you level(s) of curation.

Response:

- C. Enhanced curation – e.g. conversion to new formats during ingest, enhancement of documentation and metadata

Reviews

Reviewer 1:

Comments:

Reviewer 2:

E-depot of Erfgoed Leiden en Omstreken

Comments:

Levels of Curation - explanation

Please add the description for your Level(s) of Curation.

Response:

Before municipalities can do an official transfer to the e-depot, the ELO digital archiving adviser works closely with the records creators to make sure their collections are in line with the delivery requirements (https://www.erfgoedleiden.nl/images/e-depot/Aanlevvoorwaarden_Digitaal_Archief_Erfgoed_Leiden_eo_v30_22-09-2025.pdf). This means the structure of the archive is optimised and metadata are mapped to the Dutch governmental metadata standard, the MDTO (Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie). If obligatory MDTO metadata elements are missing, these will be created in collaboration with the archive creator. With the use of our pre-ingest tool Bitstop some technical checks (and if needed improvements) can be performed. These consist of: o Virus check o File format check o Fixity check o Validity and completeness of the metadata o Sidecar structure (each file has its own metadata file) o Empty files and folders o Zipped files o Filenames with invalid signs and sign combinations and length. Before doing a complete transfer ELO always performs a test ingest with a small subset of the digital archive to rectify any possible remaining issues. On ingest files might need to be migrated to more recent and/or durable file formats. ELO never deletes or alters the original files but simply adds to it. In some cases, ELO will also add an access copy to the original file. This is done when the original is very large, and a smaller file format serves the designated community better. After ingest a persistent identifier is added to every folder and asset. After ingest data is checked daily on integrity and fixity. If needed this is automatically fixed by Preservica. Re-characterisation is also performed on a regular basis by Preservica. If any previous mistakes are found, a re-characterisation is saved in the metadata and if needed migrations are performed. In some cases, ELO will perform minor data cleaning of the metadata, for example changing a title that is in all upper case to lower case or correcting a spelling error. Actual content in the metadata is not changed. All data cleaning is logged in the metadata.

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Cooperation and outsourcing to third parties, partners and host organisations

Please describe any cooperation and outsourcing to third parties, partners and host organisations.

Response:

Preservica provides the SaaS software, hosting and storage for the ELO e-depot. Agreements are laid out in a contract and data processing agreement. ELO and Preservica also have an Escrow Source Key agreement in case the continuity of Preservica is threatened. Preservica is, amongst others, ISO 27001, ISO 9001 and OAIS ISO 14721 certified. More information about Preservica's certifications can be found here: <https://preservica.com/trust-center>. Preservica stores our data on Amazon servers. Amazon's certificates can be found here: <https://aws.amazon.com/compliance/iso-certified/>. ELO has no direct contract with Amazon. ELO is part of the Preservica Dutch User Group. This group was founded, and is hosted, by the Dutch users of Preservica (currently 16 members). Together we share experiences, questions and suggestions, and keep in contact with Preservica to discuss our shared wishes. The idea is that there is strength in numbers to make sure our needs and wishes get heard and are prioritised. Our pre-ingest tool, Bitstop, is built by Van Kaliber. ELO has worked with Van Kaliber as a testing client in the development of this tool. However, ELO does not own the tool. Van Kaliber is responsible for the updates, bug fixing, support and further developments of Bitstop. Agreements are laid out in a contract. ELO has commissioned Van Kaliber to build PID manager. This is the software that we use to create persistent identifiers and place them in our e-depot. ELO is the owner of PID manager, but we do have a contract with Van Kaliber for the technical support in the usage and development of the software. Our persistent identifiers are created using Handle. Surf provides us with the PID Hosting Service, for which ELO has a contract with them. Surf is certified with ISO 27001:2013 (<https://www.surf.nl/files/2022-11/iso-certificaat-surf-2022.pdf>). Other relevant policies can be found on <https://www.surf.nl/informatiebeveiliging-surf-diensten>. ELO makes use of a virtual server to receive, check and upload digital archives to Preservica. The server is hosted by OpenLine. Maintenance and support are delivered by both OpenLine and the ICT department of the Municipality of Leiden. OpenLine is an outsourcing partner of the Municipality of Leiden and has signed an SLA with them for a set of delivered products and services. OpenLine is ISO 9001, ISO 1 4001, ISO/IEC 20000-1, ISO/IEC 27001 and NEN 7510 certified (<https://openline.nl/over-open-line>).

Reviews

Reviewer 1:

Comments:

E-depot of Erfgoed Leiden en Omstreken

Reviewer 2:

Comments:

Applicants renewing their CoreTrustSeal certification: summary of significant changes since last application.

Please fill this field when you are renewing your CoreTrustSeal Certification.

This field can be marked with not applicable (N.A.) if you are acquiring a CoreTrustSeal certificate for the first time.

Response:

N.A.

Reviews

Reviewer 1:

Comments:

Reviewer 2:

Comments:

Organisational Infrastructure

R1 Mission & Scope (R01)

R01. The repository has an explicit mission to provide access to and preserve digital objects.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

The mission of ELO noted in the Strategic Vision 2022-2025 is as follows: 'Erfgoed Leiden en Omstreken is the place for people with a passion for the past. We activate and help people to discover and experience history. We do this because the past is a source of knowledge and inspiration. We have to take care of this, because heritage is vulnerable in such a densely populated country. That's why we show the value of buildings, archaeology, archives and stories. In Leiden and surrounding areas. We secure this heritage by preserving it, sharing it and making it accessible for everyone. We do this together with municipalities, communities, peers, volunteers and the wider public.' Priorities for the coming years are: o Preserving heritage o Enriching collections o Entice and involve the public o Continue and improve on collaborations o Strengthen the organisation For the archives, and thus also the e-depot, this mission is largely based on the Public Records Act 1995. Focus points for the archives specifically are discussed in paragraph 2.2 of the Strategic Vision 2022-2025. This mainly focusses on preparing ourselves for the new Public Records Act (expected around 2027). We do this by helping and advising our partners on getting their information management in order (even before transfer to the e-depot), improving the accessibility of our collections in the e-depot (making it more user-friendly, linking it to other collections, building more filters, etc.) and continually working on improving our quality as a whole, this application playing a large role in that. ELO is currently working on an updated strategic vision that will be in place in 2025-2030.

Links:

- [Strategische visie 2022-2025](#)
- [Public Records Act 1995](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

E-depot of Erfgoed Leiden en Omstreken

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R2 Rights Management (R02)

R02. The repository maintains all applicable rights and monitors compliance.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Archives from governmental institutions under the care of ELO are public and can be consulted by users on the grounds of article 14 of the Public Records Act. There are no licenses or admission criteria necessary. Even though governmental archives are open according to the Public Records Act 1995, the law provides specific exceptions to public accessibility in article 15 a, b and c. These exceptions are limited in time and are specifically in place to safeguard: o a subject's privacy, or; o the interests of the state or its allies, or; o disproportionate disadvantage of legal persons or entities or third parties. If any of these restrictions are in play, ELO does not show the digital record to the public. The specific reason is always registered in the MDTO metadata. Copyright can be another reason for access restriction. According to the Dutch Copyright Law (digital) objects cannot be shared without consent from the creator. Digital objects for which this is the case, and for which we do not have consent are only available in our reading room. These objects get assigned a reading room security tag within Preservica, that makes sure they are only accessible in that physical location through a login used by reading room staff. If known, we register the author and the possible end date of the restriction in the MDTO metadata. Whenever we have official consent, recorded in a license agreement between the author and ELO, we make the records public, always showing the author and, if applicable, the Creative Commons license of the record in the MDTO metadata. For building permits, a process for making the material public is followed as set out by The Amsterdam City Archive (Stadsarchief Amsterdam). This process consists of two steps. First, ELO publishes an announcement for the publication in relevant trade journals and a widely read local newspaper. In this announcement, copyright holders are called upon to contact ELO if they do not want their material to be made public. This remains possible even after publication. In the event of a complaint from a copyright holder, ELO will limit the accessibility of this specific material. All other documents will be made public. Secondly, as mentioned above, a disclaimer will be displayed in the MDTO metadata, informing users that this material is protected by copyright. Users are requested to contact copyright holders if they wish to reproduce or otherwise use this material. Lastly, we adhere to the GDPR (Algemene Verordening Gegevensbescherming, AVG in Dutch). If a record or its metadata contains personal information that is in conflict with the GDPR, we close this record and/or metadata off for the public. It also won't be available in the reading room. Records containing personal information will be made public after the death of the involved individuals. The use of our collections, and the possible restrictions are laid out to the public on our portal (<https://erfgoedleiden-e-depot.access.preservica.com/over-het-e-depot/>). This page explains restrictions based on copyright law and the GDPR, repercussions when sharing restricted records outside our reading room, and how to use the Creative Commons licenses. When a governmental institution joins ELO for its e-depot services, the archive creator and ELO enter into a service agreement (DVO) and a processing agreement. If the archive creator already has a service agreement with ELO for their physical archive at the time of joining the e-depot, ELO will add an addendum to this. This contains agreements about services, activities, transfers and handling of personal data. In addition, ELO draws up a deed of transfer for every collection that is placed in the e-depot. The archive creator indicates whether there are exceptions to public access, and if so, on what basis and for which period this applies. In addition, it is stated that the municipal archivist can also decide to limit or entirely restrict public access. When a private collection is donated or loaned to the e-depot, ELO draws up a deed of donation or a loan agreement, stating that ELO becomes the owner or in the latter case the caretaker of the archive, and has the right to publicly share the records under the CC BY-SA license. As with governmental archives ELO will not publish and share records containing personal data of living people. Rights and licences are discussed in paragraph 8 of the preservation policy.

Links:

- [About the e-depot \(including restrictions\)](#)
- [Article 14 Public Records Act](#)
- [Article 15 Public Records Act](#)
- [Copyright Law](#)
- [Transfer to Erfgoed Leiden en Omstreken](#)
- [Uitvoeringswet algemene verordening gegevensbescherming \(Dutch GDPR\)](#)
- [MDTO](#)
- [Preservation policy](#)

Reviews

Reviewer 1:

E-depot of Erfgoed Leiden en Omstreken

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R3 Continuity of Service (R03)

R03. The Repository has a plan to ensure ongoing access to and preservation of its data and metadata.

Compliance level:

In Progress: the repository is in the implementation phase - 0

Response:

The continuity of our e-depot is guaranteed due to its statutory task. The Public Records Act prescribes that all governmental institutions must designate a repository. Archives are deposited, managed, published, and made available through the repository and meant to be kept for eternity. Because ELO is part of the municipality of Leiden the available financial resources are included in its long-term budget. In 2015, the Municipal Executive of the Municipality of Leiden made structural budget available for the realisation and upkeep of an e-depot. Furthermore, the costs are also covered by the budget and cost price for the affiliated municipalities and other parties. This guarantees the continuity of the e-depot for the future. Further elaboration on the financial continuity can be found in R05. Nevertheless, a wide range of threats can obstruct the continuous operation of the e-depot. To map out these threats and implement appropriate measures, ELO has drawn up a continuity plan. The purpose of the continuity plan is to provide an overview of the possible threats for the continuity of the e-depot and the measures that are needed to prevent them. A threat is an event that has such negative consequences that the vital business processes (or a part of them) of the e-depot are disrupted and the service is disrupted or discontinued. These may be threats that can occur in relation to any party in the e-depot – ELO itself, the Municipality of Leiden, the depositor, the supplier of the e-depot repository environment or other relevant hardware and software parties. The following threats are discussed in the continuity plan: o Organisational changes in the municipalities that are affiliated with the e-depot (such as municipalities that are split up). o Participation of new municipalities or other parties in the e-depot (and thus more workload for the e-depot team). o Withdrawal of municipalities or other parties from the e-depot. o ELO will cease to exist (in its current form). o Municipality of Leiden merges. o ELO receives less/insufficient financial resources from the Municipality of Leiden. o Municipalities in the ELO working area are postponing participation in the e-depot (and we therefore can't depend on their budget). o ELO switches to a new e-depot supplier. o Bankruptcy or takeover of e-depot supplier. o Bankruptcy or takeover of process supporting software- and hardware suppliers. o Reduced or no accessibility to e-depot due to malfunctions and calamities (including natural disasters like floods and fires, but also security issues like data hacks). o Deterioration or interruption of service due to malfunctions and calamities in process supporting hardware and software. o Information security is not sufficiently guaranteed. o Privacy insufficiently guaranteed (regarding information like phone numbers, email addresses, etc.). o Copyright insufficiently guaranteed. o The staffing is (temporarily) reduced (due to illness, pregnancy, resigning staff members, etc.). o Roles and the associated knowledge are too much based on one person. For each of these threats the plan discusses who is responsible for prevention, what the risk and impact is and which measures are taken to prevent it. The most important measures discussed in the continuity plan are the Service Level Agreement, the Escrow Agreement, the exit strategy, and the back-up and recovery strategy. These will be shortly summarised here. ELO has signed a Service Level Agreements (SLA) with Preservica. The SLA lays out agreements regarding uptime of the system, the processing time for fixing bugs, the scope of the support and the availability of the supplier in case of emergencies. To prevent the loss of (access to) digital archives, ELO has entered into an Escrow Agreement with Preservica. This means that a third party holds Preservica's source code and can provide them to ELO in the event of bankruptcy. The source code allows us to manage our account within the Preservica software ourselves and to have the time to properly migrate our data to another e-depot system. Thanks to the Escrow Agreement, services will not be completely disrupted, although some temporary delays are expected. Preservica recognizes how important it is for users of cloud-hosted systems to be able to extract a complete set of information from their content, metadata, and audit trails at any time, with no data lock-in and no additional costs. ELO can start its own export workflow with which it extracts data and metadata from the digital repository and can store it somewhere else. This workflow can be set up by yourself and it is possible to determine what the content of the export should be. ELO can choose to start an export including metadata and/or including content. In addition, it is possible to include all generations of files that have been migrated to another format, including both the original and the preservation copy(s). The export workflow ultimately facilitates a download of a ZIP file containing the entire folder hierarchy. This can then be migrated 1-to-1 to another digital repository. ELO makes use of Preservica's Enterprise Private Cloud that is hosted and maintained by them. The system is upgraded regularly, so ELO has the latest features and all important security updates. Preservica uses self-healing and replicated storage. Preservica regularly backs up all operational and service information, in order to quickly restore the service if necessary (with a minimum of three back-ups). With Preservica's cloud solutions, secure hosting, upgrades, backups and disaster recovery are all taken care of and included as standard.

E-depot of Erfgoed Leiden en Omstreken

Links:

- [Public Records Act 1995](#)

Reviews

Reviewer 1:

Compliance level:

In Progress: the repository is in the implementation phase - 0

Comments:

Reviewer 2:

Compliance level:

In Progress: the repository is in the implementation phase - 0

Comments:

R4 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.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

As discussed in R02, digital files managed in the e-depot of ELO are in principle public, based on the Public Records Act 1995. It is however possible to impose publication restrictions for a certain period of time, based on the Public Records Act 1995, article 15 a, b or c, the GDPR (AVG) or Dutch Copyright Law. The GDPR prescribes that organisations must be cautious with the publication of personal data. Therefore, ELO does not actively publish files with personal data of living people. According to the Dutch Copyright Law (digital) objects cannot be shared unless there is consent from the author. Copyright expires 70 years after the passing of the author, or 70 years after the organisation that holds the copyright ceases to exist. Only when this time has passed, or when we have official consent, ELO will actively publish these records outside of the reading room. During the time of restricted access these files cannot be downloaded or shared, only the metadata is visible (metadata never contains personal data). Rules of conduct for users of this data inside of the reading room can be found at <https://erfgoedleiden-e-depot.access.preservica.com/over-het-e-depot/>. The archive creator indicates which documents should have restricted access, on which grounds and for what period. This is checked and approved by the e-depot team and archive inspectors based on Excel files containing all metadata and sample testing of the actual digital files. All restrictions are recorded in the MDTO metadata. ELO matches this value to a security tag recorded in the XIP metadata (a metadata standard developed by Preservica to record technical and administrative metadata). Based on the metadata the system is able to switch the security tag to 'public' once the restricted period has passed. All members of the e-depot team are trained in understanding the different grounds on which records can be closed off, how to record this information, and how to make sure to close off the relevant digital documents. The training is done by more experienced colleagues, with support from external advisors and courses if needed. Moreover, all members of the e-depot team must comply with rules of conduct by (as all public servants do) swearing the oath or making the affirmation. Employment is only possible on the basis of a positive Verklaring Omtrent het Gedrag (Declaration of Conduct, VOG). This VOG is issued by an external agency, the Ministry of Justice. Secondly, as part of the Municipality of Leiden all employees of ELO adhere to the Code of Conduct for the Leiden Region (Gedragscode Leidse Regio) and the Integrity Code for the Leiden Region (Integriteitsbeleid Leidse regio). Both documents are shared with the reviewers in confidence. These documents discuss the proper way to deal with (sensitive) data by adhering to the GDPR and the Baseline Informatiebeveiliging Overheid. BIO is a security standard based on ISO 27001:2017 and ISO 27002:2017. This security standard has multiple requirements concerning privacy, such as required Data Processing Agreements with IT-suppliers and privacy by design demands for applications and systems. The archive creators themselves have accurate procedures concerning personal data as well. As governmental institutions they also have to adhere to the BIO. The source systems of the digital archives being stored in Preservica therefore have to be BIO compliant. The transfer of their archives to the e-depot is done via a secure FTPS connection limited to a specific IP address and password, making sure the data is being securely handled at all times in the pre-ingest phase. For digital archives donated to ELO by private persons and organisations these responsibilities fall on ELO. In these cases ELO will check the archive for sensitive information, and if needed add the proper metadata to handle such documents in the e-depot. As stated in R06 our outsourcing partners Preservica, Amazon and Surf are ISO 27001 certified, providing assurance for the security of our data.

Links:

E-depot of Erfgoed Leiden en Omstreken

- [About the e-depot \(including restrictions\)](#)
- [Copyright Law](#)
- [Uitvoeringswet algemene verordening gegevensbescherming \(Dutch GDPR\)](#)
- [Baseline informatiebeveiliging overheid \(BIO\)](#)
- [Certificate of conduct \(VOG\)](#)
- [Swearing the oath](#)
- [Public Records Act 1995 article 15](#)
- [MDTO](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R5 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.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

The continuity of financial resources to maintain our e-depot is guaranteed due to its statutory task. The Public Records Act prescribes that all governmental institutions must designate a repository. Because ELO is part of the municipality of Leiden the available financial resources are included in its long-term budget. In 2015, the Municipal Secretary of the Municipality of Leiden made structural budget available for the realisation of an e-depot. In 2022 an additional structural budget was made available by the Municipal Secretary. This budget is used for the e-depot as a whole: policy, processes and procedures, financial management, personnel, data management and security and the necessary hardware and software required to store and preserve digital archives. In addition, a cost-covering license fee is charged to the municipalities and other parties that are affiliated with ELO's e-depot. They pay a percentage of the total costs for the e-depot that is based on the total number of inhabitants per municipality. The annual costs of the e-depot consist of: o License costs o Consultancy o Personnel o Monitor Digital Information (annual storage measurement) o Server costs o Pre-ingest tool o Enterprise Source Key and Escrow service In addition, education, outsourcing, development, developing and maintaining policy, processes and procedures are also part of the costs. This guarantees the continuity of the e-depot for the future. The core e-depot team is formed by the Digital Archiving Advisor (0,8 fte), E-depot Project Leader (0,8 fte) and E-depot Administrator and Data Controller (1 fte). The core team is managed by the Municipal Archivist (0,94 fte) who is one of three members of ELO's management team. In addition, there are a number of roles that work together with the e-depot team at various parts of the process and are involved in the work. These are: - Senior data quality officer (acting as User Experience Specialist for the e-depot (0,8 fte)) - Archive Inspector (2 fte) - Archivist (1 fte) - Regional Representative (1 fte) - Staff member acquisition, events and collection emergency response officer (0,8 fte) These fte's are not fully dedicated to the e-depot. They give input on the basis of need. The core e-depot team will involve them if necessary. The responsibilities of each of these roles are listed in R06.

Links:

- [Public Records Act 1995](#)

Reviews

Reviewer 1:

E-depot of Erfgoed Leiden en Omstreken

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R6 Expertise & Guidance (R06)

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback-either in-house, or external.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

As mentioned in R5 ELO has multiple employees concerning the e-depot. They all have their own specific field of expertise. The list below shows their specific responsibilities. Digital Archiving Advisor: - Advising affiliated partners and private individuals on how to digitally archive documents; - Developing policy; - Certification; - Improving work processes; - Guidance of partners on migrations of systems and digitisation projects with regard to export and archiving functions, metadata and digitisation requirements; - First contact for transfers and outplacements; - Carrying out preparations for transfers and outplacements (mapping, export, etc.). - Monitoring digital collections of affiliated partners and their transfer periods (when should an archive be sent to the e-depot?). - Keeping up to date with new developments and possibilities in digital archiving. E-depot Projectleader: - Technical advice on deliveries of transfers and outplacements; - Ingesting and checking deliveries; - Developing policy; - Preservation watch; - Certification; - Improving work processes; - Making the collection accessible; - Web archiving; - Initiating and supervising technical improvements (e.g. development or use of new tools or scripts); - Keeping up to date with new developments and possibilities in digital archiving. E-depot administrator and Data Controller: - Ingesting and checking deliveries; - Ingesting and migrating digital archives from analogue collections; - Server management; - Functional management Preservica; - Making the collection accessible; - Web archiving; - Cleaning up provided metadata; - Keeping up to date with new developments and possibilities in digital archiving. - Testing and carrying out technical improvements (e.g. development or use of new tools or scripts). Senior data quality officer (0,8 fte): - Advice on publishing the collection; - Advice on setting up the e-depot visitor portal; - User research on e-depot visitor portal. Archive Inspectors (2 fte): - Advice on relevant legislation and regulations; - Guidance on digitalisation projects; - Advice on transfers and outplacements with regards to public access; - Monitoring digital collections of affiliated partners and their transfer periods (when should an archive be sent to the e-depot?). Archivist (1 fte): - Inventory of digital private archives; - Selection of digital private archives. Municipal Archivist (0,94 fte) - System owner of e-depot; - Advice on relevant legislation and regulations; - Advice on relevant standards and requirements; - Drawing up a general information plan; - Drawing up an acquisition policy; - Approving policy documents and process descriptions for the e-depot; - Member of the management team. Regional Representative (1 fte): - Drawing up service level agreements and other agreements; - Advice on finances of e-depot; - Drawing up a Products and Services Catalogue; - First contact for financial issues associated with partners. Staff member acquisition, events and collection emergency response officer (0,8 fte): - First contact for private archives - Acquisition of private archives Together they orchestrate the functional processes concerning the e-depot. Employees are selected on having a background in digital archiving, legislation and/or data management. Further training on the job is provided by more experienced members of the team. In the initial phase of the e-depot (2019-2020) the first members of its team were trained by an external party (Van Kaliber) with broad experience on digital archiving and e-depot management. Members of the e-depot team make sure they keep up with new developments and possibilities in digital archiving. There are a number of national and international communities where knowledge and advice can be gathered, such as Kennisnetwerk Informatie en Archief (Knowledge Network of Information and Archives, KIA), the Preservica Community Hub, the Digital Preservation Coalition and the Netwerk Digitaal Erfgoed (Network Digital Heritage, NDE). Employees make sure they keep up to date with the information provided by such communities and attend relevant lectures and/or workshops they offer. Furthermore, employees attend relevant congresses such as iPres and the Preservica User Days. Employees are also encouraged to keep expanding their knowledge by following courses. This can vary from a training on legislation, digitisation, project management, and so on. There is training budget available for all ELO employees. ELO also works together with other archives to solve problems and share knowledge. We do this in two ways: - Participating in (countrywide) working groups, set up to solve a specific problem or develop a specific product. - Being a member/partaking in the committee of the Dutch User Group Preservica (DUGP). This group consists of all the Dutch users of the Preservica cloud editions. Together we share experiences and communicate with Preservica about our shared prioritisations. Specifically for Preservica, ELO can make use of their support desk, but we also have a contract with Preservica for their Accelerated Success Services. This means that we have a designated technical success manager, helping the e-depot team and providing them with adequate advice on digital preservation and developments within Preservica. As mentioned above, Preservica also has a community hub, on which members from all over the world can share experiences and ask for help. The community hub also provides members with educational videos, guides and release notes. As mentioned, the e-depot team visits the yearly Preservica User Days to keep up to date with the latest possibilities and developments. Moreover, the DUGP and Preservica have initiated a yearly Dutch Summit hosted by one of the DUGP's members. This day is used to show Preservica employees how Dutch archiving and legislation works, and to get

E-depot of Erfgoed Leiden en Omstreken

our shared wishes prioritised on their roadmap. In addition to internal competencies and expertise and collaborations with other archives, ELO also hires external parties. The latter mainly happens when carrying out technically advanced actions. For example, developing a tool or writing a script. In addition, ELO can outsource projects when extra resource or expertise is needed to ensure they progress. Both the core team of the e-depot and the management team can identify if certain expertise is lacking. The management team makes decisions about expanding the team or temporarily hiring external expertise.

Links:

- [KIA](#)
- [Van Kaliber](#)
- [Netwerk Digitaal Erfgoed](#)
- [Community hub Preservica](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Digital Object Management

R7 Provenance and authenticity (R07)

R07. The repository guarantees the authenticity of the digital objects and provides provenance information.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Visitors of the e-depot must be able to assume that digital objects are authentic. A file is what it says it is and has not changed since it was submitted to the e-depot. ELO conforms to the Open Archival Information System (OAIS) standard. The OAIS model defines authenticity as "The degree to which a person (or system) views an object as what it claims to be. Authenticity is judged on the basis of evidence." The authenticity of a digital object is determined by its integrity and provenance. ELO watches over the integrity of its digital objects by performing fixity checks based on the checksum SHA256. This check takes place at three moments: 1. Upon delivery of the objects. The archive creator is obliged to provide checksums for all objects. Before ingesting objects ELO uses this checksum to determine whether any damage has occurred during transport. If this is the case, the archive creator must provide a new submission of the digital objects. Our pre-ingest tool Bitstop is used to determine whether the fixity has remained unchanged during transport. 2. On ingest. Preservica's ingest workflow will calculate the fixity of each object and compare it to the one provided in the metadata. If the checksum is not the same, ELO will re-execute the ingest. 3. After storage of the digital objects. The system performs daily automatic integrity checks on all objects in the e-depot. The system will perform an automatic recovery if necessary. Moreover, upon delivery ELO will check the file formats using Bitstop. This check will show whether the correct extensions have been used, and if the file formats are conform to ELO's preservation policy. Preservica's ingest workflow makes use of the PRONOM register, containing information about object properties, and the file format identification tool JHOVE. These properties and identifications are stored in the XIP metadata, together with any potential errors. The OAIS model describes provenance as "The information that documents the history of the Content Information. This information tells the origin or source of the Content Information, any changes that may have taken place since it was originated, and who has had custody of it since it was originated." ELO records the original provenance of a digital object (its origins with the archive creator) in the metadata in accordance with the MDTO. The MDTO contains several fields that record the people, processes and systems involved. All MDTO metadata are checked in our pre-ingest tool Bitstop, by using the MDTO xsd. Any errors or lacking metadata will be solved with the archive creator before ingesting the digital object. In addition, all actions related to the digital object in Preservica are recorded in the so-called XIP metadata, logging the audit trail. This is part of the Archival Information Package (AIP). Authenticity and integrity are discussed in

E-depot of Erfgoed Leiden en Omstreken

chapter 3 of our preservation policy. ELO considers the original file to be the primary authentic and unique object, (or the most closely related surviving surrogate or copy). This concerns the digital object as it was stored in the archive creator's source system and delivered as such to ELO. ELO will always retain the original version of a digital object. Any applied normalisation, migration and conversion therefore do not mean that the original object is replaced. In all cases, ELO merely makes a copy of the object. Preservica attaches this copy to the original object and adds technical metadata about the preservation action carried out to this package. This way, the original object can always be traced and exported if necessary. The same goes for the original metadata. This will never be deleted or altered (with exceptions of minor data cleaning such as changing all upper case to lower case, as explained in the levels of curation). Additions to the metadata are logged in the XIP metadata. During the authenticity checks discussed above ELO takes the following five essential characteristics of digital files into account: - Content: Is the textual, visual and/or audiovisual content of the object available and unchanged after archiving, preservation, migration and publishing? - Context: Is the context of the digital object recorded correctly and completely in the metadata? - Appearance: Is the appearance of the digital object unchanged after archiving, preservation, migration and publishing? - Behavior: Is the behaviour of and interaction with the digital object the same as that of the original object? - Structure: Is the structure and hierarchy of the original object unchanged after archiving, preservation, migration and publishing? These matters are discussed in chapter 2 of our preservation policy.

Links:

- [MDTO](#)
- [Bitstop](#)
- [Preservation policy](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R8 Deposit & Appraisal (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

The Public Records Act 1995 is the most important guidance for the selection of data eligible for digital archiving in the e-depot. Governmental institutions are obliged by this law to transfer archives which need to be kept for eternity and have been in their care for 20 years or more to an appropriately designated repository. Which documents have to be archived is based on the Selection Lists by The Association of Dutch Municipalities (VNG). Once the files are transferred to ELO they are, based on the Public Records Act 1995, meant to be made public and to remain public. Stored files in the repository are never deleted. They therefore are all treated with the highest level of preservation. To determine the correct metadata to use ELO adheres to the Metadata for Sustainable Accessible Government Information (MDTO) metadata schema. This is the Dutch national standard used for archiving digital documents and its metadata. Our depositors are obliged to transfer their archives accompanied by metadata files that are in accordance with the MDTO, as stipulated in chapter 2.2 and 2.3 of our Delivery Requirements. Furthermore, digital archives need to be delivered with Open Exchange (OPEX) metadata. This is a metadata standard created by Preservica used to ensure that the archive lands in the correct place in the e-depot and that fixity can be checked by the system. The delivery of the metadata is checked on completeness and correctness before ingest. ELO does this using the tool Bitstop. Based on the xsd files of the MDTO and OPEX metadata schemas, all xml files are checked. If any metadata files or metadata fields are missing, or have been used incorrectly, Bitstop will display an error message. The archive creator will be asked to correct these errors before ELO can continue ingesting the digital archive. Besides the above standards, ELO commits to a list of preferred and accepted file formats to maintain sustainability based on PRONOM. This list can be found in chapter 2.6 of the Delivery Requirements and in chapter 2.5 of the Preservation policy. Bitstop checks all incoming files against this list. File formats that are not on this list will prompt an error message. In these cases ELO will discuss the possibilities with the archive creator. Sometimes the archive creator will not have files available that are in line with ELO's preferred and accepted file formats. Luckily, Preservica has a large

E-depot of Erfgoed Leiden en Omstreken

array of preservation and migration pathways available. A set of standard preservation and migration workflows has been set up in our system. This way we can ensure that a more sustainable version of a file format that is not on our list is added to the original digital object. Archive creators can make use of our Guide for transferral of digital governmental archives. While the Delivery Requirements mainly discuss the technical requirements, the Guide for Transferral provides a complete step to step overview of the transfer process. This includes steps such as an intake meeting (a starting meeting with the archive creator to discuss the basic information about the collection, such as size, file formats, metadata, encryption, etc.), test ingests and signing the deed of transfer. Before files are transferred to ELO, the responsibility for these files lies with the governmental institutions. This responsibility consists of making sure the files are in good condition and accessible, as is stated in the Public Records Act 1995. After the files are transferred to ELO, the responsibility for the condition of and access to the files transfers to ELO. However, the governmental institutions are still the owners of their deposited data. The obligation to deposit archives according to the Public Records Act does not apply to private archives. Files from private archives can be donated or lent to ELO. Selection of digital private archives is done based on the Acquisition Plan. Chapter 2 explains the criteria by which an archive can be selected: - An archive must be related to the history of the municipality - An archive must be a representation of the population, or of a unique character of the municipality - An archive must add an additional aspect to the archives already in the depot in order to qualify for active acquisition. These conditions apply to all of ELO's archives, both physical and digital. The municipal archivist makes the ultimate decision whether the acquisition of a private archive is worthwhile. The delivery requirements for private archives are less strict than those for governmental bodies. Private persons and organisations are not obliged to deliver their archive with MDTO and/or OPEX metadata. However, as explained in chapter 2.4.4 of the Guide for transferral of digital archives of private organisations the provision of metadata is very much appreciated and encouraged. The digital archiving advisor supports in this. Although MDTO metadata are not obligatory for private archives, they do have to inform ELO about the accessibility of all digital objects. Restrictions based on Copyright or GDPR have to be known. ELO will add some basic metadata to all private collections, using a basic set of MDTO and OPEX metadata using Bitstop. These metadata consist of: - Identification number - Title - Basic description - Aggregation level - Language - Is part of (to show the parent of the digital object) - Valuation - Name of the archive creator - Limitations to the use (e.g. Copyright or GDPR) - Fixity - Security tag (to indicate the level of accessibility in Preservica) As stated in chapter 2.5.1 of the Guide for transferral of digital archives of private organisations, private persons and organisations are expected to adhere to a list of preferred and accepted file formats. As with the governmental archives, migrations are possible in Preservica if this is deemed impossible. As opposed to governmental archives, private archives are donated or lent to ELO. Up until transfer and ingest the responsibility for, and the ownership of these files lies with the private organisations and individuals. After the files are ingested and the deed of donation is signed, the responsibility for the condition, access to the files and the ownership of the files, transfers to ELO. As mentioned before private organisations can also loan their collection to ELO in which case a loan agreement is signed.

Links:

- [Public Records Act 1995](#)
- [VNG selectionlists](#)
- [Delivery requirements](#)
- [Attachment 1 delivery requirements](#)
- [Attachment 2 delivery requirements can be found on this page](#)
- [Guide to transferral of private digital archives](#)
- [MDTO](#)
- [Bitstop](#)
- [Preservation policy](#)
- [Guide to transferral](#)
- [Acquisition policy](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R9 Preservation plan (R09)

E-depot of Erfgoed Leiden en Omstreken

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

ELO has planned and documented the preservation of the digital objects in the e-depot in its preservation policy. In this preservation policy we describe how we preserve digital objects durably while maintaining authenticity. By preservation we mean 'The recording, storage, management and making available of digital documents (in the broad sense of the word) in such a way that they can also be consulted, accessible and authentic over time', as defined by OAIS. When drawing up this preservation policy, the framework of the Preservation Policy Guide of the Netwerk Digitaal Erfgoed (managed by the Cultural Heritage Agency of the Netherlands) was followed. This focuses on ten areas of interest within digital preservation and has the following chapters (each with a set of paragraphs going into further detail): The digital object (chapter 2), Authenticity (chapter 3), Passive preservation (chapter 4), Active preservation (chapter 5), Certification (chapter 6), Metadata (chapter 7), Rights (chapter 8), Standards (9), Organisation (chapter 10) and Access (chapter 11). For this requirement subchapters 'Deletion and destruction' (2.2), 'Preservation watch' (2.5), 'Pre-ingest checks' (4.1), 'Checks on ingest' (4.2), 'Post ingest checks' (4.3), 'Backups and measures in case of data loss' (4.4), 'Preservation strategies' (5.1) and 'Preservation metadata' (7.1) are most important. As discussed in chapter 2.2 'Deletion and destruction' ELO distinguishes between deletion and destruction. In the event of destruction, no traces of the digital object may remain in the e-depot. Digital objects deleted from Preservica are automatically destroyed after 90 days. What remains is only the name of the object(s) and the notice that it has been destroyed. According to the Public Records Act 1995, Article 6, destruction can only take place with the approval of the municipal archivist. Governmental archives that are archived in the e-depot, should under no circumstances be destroyed. However, an archive can be transferred to another digital archive at the request of the archive creator. In the case of private archives, the municipal archivist can decide to destroy or transfer to another archive if a digital object no longer fits the collection. In the case of an outplaced archive, it is possible that (part of a) transferred archive must be destroyed after a certain period. Here too, the municipal archivist approves the destruction on the basis of the destruction list. In addition, destruction as well as removal is carried out in accordance with a 'four eyes principle'. A second (manager) account is required to approve all deletions. Removal takes place when errors are found in the digital objects and/or associated metadata supplied by the archive creator. The deleted object is replaced by an object in which the inaccuracies have been corrected. As discussed in chapter 11.7 'PID's', if an object is removed from the collection or transferred to another archive, a 'tombstone' will be connected to the PID with an explanation, so the user understands why the object is absent. Chapter 2.5 'Preservation watch' states that the e-depot team is responsible for preservation watch. At least once a year the list of preferred and accepted file formats is checked, and if necessary adjusted. We also research whether our strategies for preservation are still up to date. This is done by asking ourselves the following questions: - Are there file formats in our e-depot that are in danger of becoming outdated or no longer supported? - Are there file formats in our e-depot that we can migrate to a more accessible file type? - Are there (new) file formats on the market that better meet the needs of our users? - Are there (new) file formats on the market that provide a better guarantee of durable storage? - Are there new techniques on the market with regards to migration, preservation and accessibility? Chapter 2.5 lists all accepted and preferred file formats (accompanied by their fmt code as used in the PRONOM register). This list is also provided in our Delivery requirements. As discussed in 5.1 'Preservation strategies' this list has been composed by taking the following aspects into consideration: - Adoption and support: Is the format widely used? - Independence from external software and hardware - Transparency: Is the digital object easy to interpret with basic tools such as a text editor? - Self-documentation: Does the file format already record some (technical) metadata? - Patents and licenses: Can the file format also be opened without these? - Protection methods: Is there no encryption on the file? - Open Standards In this chapter we also discuss that we adopt the preservation strategies of normalisation, migration and conversion. When transferring, archive creators must adhere to the accepted and preferred formats. In practice, however, this is not always possible because in most cases the archives supplied were already created before the existence of e-depots and the associated delivery requirements. To prevent a proliferation of file formats or different versions of file formats in the e-depot, ELO normalises the incoming formats where possible to a format from our Delivery requirements. This way the management and preservation watch of the various formats becomes clearer and more manageable. A file can be migrated to a different file format if it has not been deemed durable enough to have been placed on our list of preferred and accepted file formats. With conversion we update files to a newer version of the same file format. This can help opening a digital object in the future. For example, very outdated versions of Word can hardly be opened anymore. This can be prevented by converting the file format to a newer version in a timely manner. Chapter 4 discusses passive preservation. By passive preservation, ELO means carrying out checks, before, during and after ingest, that guarantee that the digital objects (including metadata) are and remain complete and intact. This is extra important because there are no physical derivatives of the digital objects in the e-depot (or they are too weak to re-digitise). If problems emerge from these checks, active preservation can be initiated. Before ingest ELO performs a number of checks using the pre-ingest tool Bitstop. These checks include: - File formats - Viruses - Fixity - Validity and completeness of metadata - Structure - Empty files and folders - Zipped files - Invalid filenames - Number of digital files and folders and their size On ingest Preservica automatically repeats the file format, virus and fixity checks, making sure that no damage to the bits and bytes has occurred during the upload. Daily integrity checks are automatically run by the system to check for any bitrot. Preservica repeats the characterisation of file formats (without fixed regularity) if improved tooling is integrated in the system during an update. Such recharacterisation occurs in the background and can reveal past mischaracterisations. Technical developments and improvements are a continuous process. As discussed in chapter 4.4, Preservica uses Amazon Web Services (AWS) to store the digital objects in the e-depot. All content is stored in at least three different locations (availability zones) within the EU, with primary storage in Dublin, Ireland. Amazon automatically creates daily snapshots that serve as a backup. These backups are also stored in at least three different locations. The automated snapshots are supplemented by daily independent backup snapshots by Preservica. The system is self-healing in the event of errors and is designed to recover from simultaneous data loss at two different locations. In the event of data loss, the contents of the e-depot can be reconstructed based on one of its copies. In addition, ELO uses Preservica's Enterprise Source Key and Escrow service. In the event that Preservica ceases to exist, ELO will have access to the source code of the program so that ELO can access the system and associated data

E-depot of Erfgoed Leiden en Omstreken

under its own management. Chapter 7 of the preservation policy discusses that ELO conforms to the national standard Metadata for Sustainable Accessible Government Information (MDTO) as established by the National Archives of The Netherlands. This is a standard for recording and exchanging governmental information. The supply of digital objects and metadata in accordance with MDTO is one of the delivery requirements of ELO that archive creators (with the exception of private individuals) must meet as implementation of Article 3 of the Archives Act 1995. In some cases, digital objects contain very sector-specific metadata for which MDTO alone is not sufficient. If this is the case, ELO applies, where possible, other national metadata standards, and where necessary ELO develops these itself. However, these metadata standards never stand alone, but are always used as a supplement to MDTO. Besides original, structural and describing metadata, ELO also logs preservation metadata. This is done in the XIP metadata schema, developed by Preservica. Preservica automatically identifies the technical metadata of a digital object upon ingest and records it in the XIP metadata. This concerns metadata such as the file format, file size, hardware, software and integrity. Metadata about the preservation process is data about active preservation actions that ELO carries out within the system. Preservica keeps a log of this. All migrations, normalisations and conversions are tracked in the XIP metadata.

Links:

- [Delivery requirements](#)
- [Framework Preservation Policy Guide](#)
- [MDTO](#)
- [Article 3 Public Records Act](#)
- [Bitstop](#)
- [Article 6 Public Records Act](#)
- [Preservation policy](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R10 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.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Quality requirements for digital archives submitted to the e-depot are described in the Public Records Act 1995. Article 3 of the Public Records Act stipulates that governmental institutions are obliged to ensure that the files entrusted to them are and remain in a good, orderly, and accessible condition, which is in line with the Delivery requirements of ELO. Archive regulation article 17 stipulates that the following aspects of every stored file in the e-depot can be accessed at any time: a. The content, structure and appearance when it was received or created by the governmental organisation insofar as these aspects had to be known for the execution of the work process concerned; b. When, by whom and on the basis of what task or work process it was received or created by the governmental organisation; c. The relationship to other digital objects received and created by the governmental organisation; d. The management activities carried out in relation to the digital objects; and e. The operating system or applications used to store or manage the digital objects. Article 19 of the Archive regulation prescribes requirements about metadata and the metadata schema: 1. The governmental organisation uses a metadata schema as referred to in NEN-ISO 23081:2006. 2. The governmental organisation records metadata linked to the digital objects from which the aspects referred to in article 17 can be traced at any time. Article 11 of the Public Records Act stipulates that measures should be taken to assure that archives meet such a quality that if 'archive documents are consulted after at least one hundred years, no significant deterioration will be observed.' In

E-depot of Erfgoed Leiden en Omstreken

practice, this means that governmental organisations are obliged to deliver their metadata conform MDTO and must be valid according to the MDTO-XSD schema. MDTO is the national metadata standard for governmental archives as established and managed by the National Archives of The Netherlands. This and other requirements are stipulated in our Delivery Requirements. The requirements in this document are mostly derived from the quality requirements in the Public Records Act 1995 and the above mentioned articles of the Archive Regulation. In the case of an official transfer the depositor must make sure the documents and metadata meet these requirements. More explicitly this means: - The digital archive must be free from data corruption, malware, viruses and zero-byte files. - File names may not include certain special characters. - File and path names must not be longer than 255 characters. - File encryption is not allowed (the depositor must provide valid decryption keys if digital objects are encrypted). - Compressed file archives such as RAR, TAR and ZIP are not allowed. - Provided file formats must be on our list of preferred and acceptable file formats. - All files and folders must be linked to a metadata file (sidecar structure). - The metadata must comply with the metadata standard MDTO. - Digital objects need to be delivered together with their fixity hash code according to SHA256. Requirements for private archives are a little less strict. These requirements are laid out in the Guide for transferral of digital archives of private organisations. Many of the above listed requirements also count for them, except for the requirement to deliver with MDTO standard metadata. However, basic metadata is needed to provide the user with the proper description, context, origins and rights about the collection. The advisor digital archiving will provide the private archive creator with the guidance needed to deliver this basic information to ELO. ELO's e-depot team will make sure that these metadata are placed in the e-depot using the MDTO standard. All delivered files and metadata are checked in the pre-ingest phase by using the pre-ingest tool Bitstop. Further checks are done on ingest and on a daily basis in Preservica. All these checks are described in R09 Preservation Plan. As described in chapter 3 of the Guide for transferral of digital governmental archives all transfers first undergo a testing phase using a small portion of the archive. Once this has been approved the entire archive is transferred and checked again. If errors or anomalies are found, the archive creator is asked to make adjustments and to provide a new delivery of the archive, or the part of the archive that was incorrect. Members of the e-depot team will guide the archive creator through the process of making the needed adjustments. ELO conforms to the national metadata standard as set up by the National Archives. This means that when the standard changes, we will also change this in our delivery requirements. In 2021 MDTO replaced TMLO. Any older collections that were already in the e-depot at the time of this change will be mapped and transformed to MDTO by ELO. The Delivery Requirements as a whole are monitored on a yearly basis, and adjusted where needed. Changes to the preferred and accepted file formats are implemented in the e-depot by performing new conversions, migrations and normalisations. Once ingested the presentation of the digital collection in the user portal is discussed with ELO's Senior data quality officer who acts as user experience specialist for the e-depot (see R06 Expertise and guidance). Because of the varying knowledge of ELO's designated community (see Background information) digital collections are presented in a way that is easy to understand for those users with a limited knowledge of digital collections and files. On the other hand, we also make sure we provide the information that is needed for users with more experience like researchers or the government employees who might have created the documents.

Links:

- [Delivery requirements](#)
- [Article 11 Public Records Act](#)
- [MDTO](#)
- [Article 3 Public Records Act](#)
- [Bitstop](#)
- [Preservation policy](#)
- [Guide to transferral](#)
- [Article 17 Archive Regulation](#)
- [Article 19 Archive Regulation](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R11 Workflows (R11)

E-depot of Erfgoed Leiden en Omstreken

R11. Digital object management takes place according to defined workflows from deposit to access.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

The business processes related to the workflows in the repository are completely based on the OAIS model and, naturally, the requirements of the Public Records Act apply. ELO has multiple guides and policies in which these workflows are documented. The Guide for transferral of digital governmental archives (Handleiding overbrenging digitaal archief) documents the steps that ELO undertakes for each transfer of a digital archive of a governmental body. This guide is shared with all our partners, so that the steps and involvement of all players are clear at any time during the process. The steps consist of the following phases: - Intake meeting (a starting meeting with the archive creator to discuss the basic information about the collection, such as size, file formats, metadata, encryption, etc.) - Mapping the metadata of the collection to MDTO - Preparing of the transfer of a subset as a test - Test ingest of a small subset - Testing the accessibility of the subset - Preparing the transfer of the whole collection - Ingest in the e-depot - Making the collection accessible - Signing the deed of transfer - Closing the case The guide discusses these steps in more detail. Furthermore, the entire process from the intake to the closure is drawn up in a flowchart, which can be found in appendix 4 of the guide. Further details about the requirements during the transfer to the e-depot are listed and explained to our partners in the Delivery Requirements as explained in R10 Quality Assurance. The way ELO makes sure that transferred archives are well preserved, accessible and understandable for our designated community is documented in our Preservation policy. As discussed in R09 the policy consists of the following chapters: The digital object (chapter 2), Authenticity (chapter 3), Passive preservation (chapter 4), Active preservation (chapter 5), Certification (chapter 6), Metadata (chapter 7), Rights (chapter 8), Standards (9), Organisation (chapter 10) and Access (chapter 11). As mentioned in R10 ELO also has a Guide for transferral of digital archives of private organisations. This document discusses the requirements for private digital archives. A flowchart for the transfer of private digital archives to the e-depot has also been drawn up in the process modelling software Engage. For the harvesting and archiving of websites ELO has drawn up a separate policy, the Guide to webarchiving. This policy discusses the techniques used, the frequency of harvesting, the scope, chosen file formats, metadata, costs, folder structure and the different processes in harvesting and archiving websites. Web archiving flowcharts can be found on pages 9-11. All policies and guides are updated when needed and checked with a minimum of once a year. Any revisions need to be approved by the management team of ELO. ELO has drawn up flowcharts for a number of workflows in the process modelling software Engage. These flowcharts show all steps in a process together with the responsible team members and, if applicable the estimated time required for a certain step. The project leader of the e-depot is responsible for the creation of these flowcharts, in cooperation with the other team members of the e-depot. All e-depot workflows have been approved by the management team of ELO. The project leader also has the responsibility to keep all workflows described in Engage up to date. This is checked at least twice a year. All alterations to the workflows have to be approved by the management team. The flowcharts are used to make sure all workflows follow pre-set steps and rules. Therefore, they mainly serve as an internal instrument. However, as mentioned before, several of the workflows are also shown in our policies as a helpful insight for different archive creators. The following workflows have been approved by the management team and can be found in Engage: - Archiving governmental websites (see page 10 of the Webarchiving policy) - Archiving websites of private individuals or organisations (see page 9 of the Webarchiving policy) - Archiving websites for a hotspot (see page 11 of the Webarchiving policy) - Digital preservation - Transfer of private digital archives to the e-depot. - Transfer of governmental digital archives to the e-depot (see appendix 4 of the Guide for transferral of digital governmental archives) - Outplacement in the e-depot ELO does not use different preservation levels for different kind of archives. All archives placed in the e-depot are preserved with the intention of indefinite preservation, and all receive the same amount of care. There are some differences in the required quality (and complexity) of metadata for governmental archives versus private archives. Therefore, separate policies and workflows have been drawn up. As discussed in R02 and R04 digital files managed by ELO in our e-depot are in principle publicly available, on the basis of the Public Records Act 1995. At most, it is possible to impose publication restrictions for a certain period based on the Public Records Act 1995, article 15 a, b or c, the GDPR or Dutch Copyright Law. All digital objects are handled with the same security measurements, but for those with one of the restrictions mentioned above a different security tag is set within Preservica. This is based on the MDTO metadata. The Engage workflows for the transfer of governmental and private collections both have the creation of MDTO as a necessary step. Although ELO does not have the same MDTO requirements for private collections as we do for governmental collections, the MDTO element 'Beperking gebruik' (Limitations to use) is required in both workflows.

Links:

- [Article 15 Public Records Act](#)
- [Copyright Law](#)
- [Uitvoeringswet algemene verordening gegevensbescherming \(Dutch GDPR\)](#)
- [Public Records Act 1995](#)
- [Delivery requirements](#)
- [Guide to transferral of private digital archives](#)
- [MDTO](#)
- [Guide to webarchiving](#)
- [Preservation policy](#)
- [Guide to transferral](#)

E-depot of Erfgoed Leiden en Omstreken

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R12 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.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

The collections within the e-depot can be found through the search function of the main website of ELO <https://www.erfgoedleiden.nl/>. This gives the visitor the total amount of hits for a specific search term, and leads the visitor onwards to the search results on the publication portal of the e-depot <https://erfgoedleiden-e-depot.access.preservica.com/>. Visitors can also search directly within this portal. The portal is reachable either through the direct URL, or via the e-depot page on the main website <https://www.erfgoedleiden.nl/collecties/e-depot>. The search capabilities within the portal are more extensive than the search button on ELO's central website. Visitors have the option to do a full text search, either in all of the collections, or within a specific subset, using the SOLR search engine. Facets and filters have been set by the e-depot team to make the search experience easier. Tips and tricks for using the search engine are listed for the visitors on this page <https://erfgoedleiden-e-depot.access.preservica.com/zoektips/>. The full text search will search within a document's text as well as in the metadata. As explained in requirements 8 and 10, all collections are provided with MDTO metadata, making it possible to narrow down a search and search documents without text (videos, images, etc.). The MDTO metadata shows at least a title, description, archive creator and, if applicable, licenses and copyrights. The user will thus be able to identify the object correctly. Preservica provides an OAI-PMH Data Provider implementation for metadata harvesting. This can be used by an external system, such as a cataloging application, to retrieve information about the hierarchy of logical objects - structural objects (folders) and information objects (assets) - in the archive. All requests to the Preservica OAI-PMH Data Provider require authentication. All requests must include a valid Preservica access token in a Preservica-Access-Token HTTP header. Data returned from any method on the API will be based on the access permissions of the user for whom the access token was generated. Unauthenticated access to the OAI-PMH Data Provider is not supported. For backward compatibility reasons, the OAI-PMH Data Provider also supports HTTP basic authentication, where a valid Preservica user name and password are encoded into an HTTP Authorization header. Furthermore, Preservica provides (amongst others) a content API. This is a search-based, read-only API for accessing metadata and content for display on discovery platforms. This is currently used for the search function on our main website (as described above) and for xSitu. The latter is an inhouse content management system for archaeological data, used by ELO's archaeologists. Through the content API, content and metadata are linked to xSitu. However, it is important to note that broader use of the Preservica APIs and OIA-PMH by multiple parties is not yet in place and is not actively encouraged at this time. For this we need to develop a deeper understanding of the implications and functionalities of these tools. As we gain expertise, we anticipate expanding access to a wider audience. ELO provides the visitor with a best practice regarding citation and gives some examples. This can be found here <https://erfgoedleiden-e-depot.access.preservica.com/verwijzen/>. In English the best practice translates to: When you refer to a collection or information object in the e-depot, you can use different systems. In any case, it is important to include in the reference: - Any rights to the information object (creator, rights holder and license); - The persistent identifier. We also recommend to include the following: - Heritage Leiden and Surrounding Areas. Completely spell out this name at least once, after that the abbreviation ELO will suffice; - A logical and recognisable title of the collection or information object; - Any restrictions on access. ELO makes use of persistent identifiers using the Handle system. Every digital object, file and folder, is supplied with a PID, for example <https://hdl.handle.net/21.12164/b128d47d-5946-4b75-a7ea-93dbc3686824>. This way it is possible for visitors to refer to a (sub)collection or to a specific file. PIDs are created post-ingest using ELO's own tool PIDManager. This tool was developed by Van Kaliber on behalf of Erfgoed Leiden. Technical support is contracted at Van Kaliber. The tool is able to: - Create new PIDs; - Place the PIDs in Preservica; - Register the PID and accompanying URL on the Handle server; - Update the accompanying URL on the Handle server (in case the URL of the publication portal changes); - Verify the correctness of new and previously existing PIDs. This is done on a regular basis; - Delete PIDs. New PIDs are created after each ingest of a new collection and/or object using PIDmanager. This action is triggered manually. This is part of the standard ingest process and the responsibility of the e-depot team members. After creation PIDmanager will create an overview of all successfully created PIDs. In case an error occurs, PIDmanager will give the user a warning and detailed description in the logs. Moreover, at the end of every month a team member will check if all new collections and objects

E-depot of Erfgoed Leiden en Omstreken

within have received a PID. This team member will also check if the PIDs still resolve to the right page. This is done by a manual sampling procedure as well as a fully automated check using PIDmanager. In case the URL of Preservica's user portal changes (which luckily is a very rare occurrence) the PID, or rather the accompanying URL registered on the Handle server, will be updated using the 'replace' module within PIDmanager. ELO doesn't update a PID when the content of an asset changes, following the guidelines of the National Archives of the Netherlands. Preserved objects and their metadata are not changed by ELO (besides the adding of migrated files or minor data cleaning on ingest, as explained in the levels of curation). Therefore, versioning of PIDs is not applicable. In theory, if an object is altered to a large amount, the PID will be replaced by a new one. Using PIDmanager ELO will redirect the old PID to the new PID. Up to this moment this has never been necessary though. As a rule, ELO does not remove PIDs. However, there will always be exceptions, for example in the case of dispossession of a digital object. If an object is removed from the collection or transferred to another digital archive, a 'tombstone' page will be connected to the PID with an explanation so the user understands why the object is absent. Our Handle server is hosted by Surf. Surf is a well-known IT-cooperative for education and research in the Netherlands.

Links:

- [MDTO](#)
- [Main website of Erfgoed Leiden en Omstreken](#)
- [Portal to the e-depot of Erfgoed Leiden](#)
- [Link to e-depot portal on main Erfgoed Leiden website](#)
- [Tips and tricks for searching in the e-depot](#)
- [PID service hosted by Surf](#)
- [Preservica API reference](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R13 Reuse (R13)

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Any governmental digital archive provided to ELO must be accompanied by metadata. This metadata should be in accordance with existing standards. According to the 2009 Archives Regulation, government organisations are required to create a metadata schema based on ISO 23081. MDTO, a metadata guideline conforming to ISO23081 for the Dutch government has been created by the National Archives as discussed in R08 and R10. MDTO provides which minimum metadata is required for long term preservation of digital records, including requirements for contextual, technical and data management metadata. The MDTO metadata is stored in our e-depot system Preservica, together with technical metadata extracted by the system. These requirements are in place to ensure that all users and Designated Communities will get access to unchanged, authentic and understandable information. In addition, to make use and reuse of the archived data easier, ELO has stipulated preferred and acceptable formats (see chapter 2.6 of the Delivery requirements) based on the policy of the National Archives. As explained in chapter 11.3 of the Preservation policy, it is very important to ELO that the digital objects in the e-depot are usable by the general public. This was taken into account when selecting the file formats for our Delivery Requirements. Files must be presentable in our visitor portal and easy to open and view on the user's computer after downloading it. File formats have thus been selected based on the following criteria: - Adoption and support: is the format widely used? - Independence from external software and hardware - Transparency: is the digital object easy to interpret with basic tools such as a text editor? - Self-documentation: does the file format already

E-depot of Erfgoed Leiden en Omstreken

record some (technical) metadata? - Patents and licenses: can the file format also be opened without these? - Protection methods: is there no encryption on the file? - Open standards In addition to the file format, speed of accessibility is also important for usability. Some files are so large that it can take a longer time to display them. In these cases, ELO chooses to make an access copy available in a smaller file format. For example, a JPEG instead of a TIF or an MP3 instead of a WAV. This is only done if the content of the digital object remains unchanged and clear to the user. If a depositor wants to transfer formats that deviate from the preferred or acceptable formats, appropriate measures are assessed on a case-by-case basis. Of course, changes in the (digital) world can affect metadata standards and file format policies. Therefore, these are periodically reviewed by the National Archives with input from different archives in the Netherlands to check if they still fit the needs of the users and the designated community as best as possible. Any changes in the National Archives preferred formats policy will be assessed by the e-depot team and may lead to changes in the delivery requirements and migrations in the e-depot. Changes in the metadata guideline MDTO for the Dutch government created by the National Archives will also be followed by ELO. Thus, ensuring that the metadata and file formats are continuously in line with the needs of the designated communities. The e-depot team monitors the possible obsolescence of file formats in our repository. If deemed necessary, we are able to carry out file migrations within Preservica. At this moment we have no digital archives in our repository with file formats that are in danger of becoming obsolete. Our inhouse senior data quality officer performs periodical user research and advises the organisation on how to best publish digital documents and accompanying metadata. Moreover, as mentioned in R06, the senior data quality officer acts as user experience specialist and advises the e-depot team on how to best publish the collection and set-up the e-depot visitor portal. Archive creators are also consulted about the accessibility of their collections, especially in cases where government employees form the main user group.

Links:

- [Delivery requirements](#)
- [Archive Regulation](#)
- [MDTO](#)
- [Preservation policy](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Information Technology & Security

R14 Storage & Integrity (R14)

R14. The repository applies documented processes to ensure data and metadata storage and integrity.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Storage As stated in the background information ELO makes use of Preservica as the software for our e-depot. Preservica uses Amazon Web Services (AWS) to store the digital objects in the e-depot. All content is stored in at least three different locations (availability zones) within the EU, with primary storage in Dublin, Ireland. Amazon automatically creates daily snapshots that serve as a backup. These backups are also stored in at least three different locations. The automated snapshots are supplemented by daily independent backup snapshots by Preservica. The system is self-healing in the event of errors and is designed to recover from simultaneous data loss at two different locations. In the event of data loss, the contents of the e-depot can be reconstructed based on one of its copies. ELO uses Preservica's Enterprise Source Key and Escrow Service. In the event that Preservica ceases to exist, ELO will have access to the source code of the program so that ELO can access the system and associated data under its own management. In addition to cloud storage, ELO also manages digital objects that are temporarily stored on physical data carriers before they are ingested in the e-depot. In almost

E-depot of Erfgoed Leiden en Omstreken

all cases, these are digital archives of private individuals or institutions that have been transferred to ELO. Here too, ELO uses the principle of multiple backups at different locations. Until the relevant digital objects have been ingested in the e-depot, these digital archives are stored on three different hard drives, one working disk and two backup disks. The backup drives are stored in two different physical depots. Storage and back-ups are discussed in chapter 4.4 of the Preservation policy. Integrity As discussed in chapter 3.1 of our Preservation policy, ELO monitors the integrity of its digital objects by performing fixity checks based on the checksum SHA256. This check takes place at three moments: 1. Upon delivery of the objects. The archive-creating organisation is obliged to provide checksums for all objects. Before ingesting objects, ELO uses this checksum to check whether damage has occurred during transport. If this is the case, the archive creator must deliver intact versions of the relevant objects. 2. During the ingest of digital objects. Preservica's ingest workflow checks for all objects whether the supplied checksum still matches the checksum of the object as soon as it enters Preservica. If the checksum does not match, ELO re-executes the ingest. 3. After the ingest of digital objects. Preservica carries out daily integrity checks on the digital objects on the various storage adapters that ELO uses: Glacier adapters and S3 adapters. ELO uses the Glacier adapters for heavy files that are not often consulted. The S3 adapters are used for lighter files and access copies. Preservica performs automated quick checks where the file size is checked. In addition, a full check takes place that checks the checksum. If errors are discovered, the system sends a notification to Preservica's operations team who will restore the damaged digital object from one of the backups. Besides integrity checks based on the SHA-256 hashcode, all files are characterised to see if the file format is in line with our Delivery requirements and if the stated file extension is correct. Again, this takes place at three moments (chapter 4.3 of the Preservation policy): 1. Upon delivery of the objects. Before ingest we check the file formats with our pre-ingest software Bitstop. 2. During the ingest of digital objects. Preservica's ingest workflow characterises all the files using JHOVE. 3. After the ingest of digital objects. Preservica repeats the characterisation of file formats if improved tooling is linked to the system during an update. Such recharacterisation occurs in the background and can reveal past mischaracterisations. Technical developments and improvements are a continuous process. Preservica automatically identifies the technical metadata of a digital object upon ingest and records it in the XIP metadata. This concerns metadata such as the file format, file size, source hardware/software and integrity. Metadata regarding the active preservation that ELO carries out is also logged by Preservica. All migrations, normalisations and conversions are tracked in the XIP metadata. ELO makes a distinction between removal and destruction. In the event of destruction, no traces of the digital object may remain in the e-depot. Deleted digital objects in Preservica are automatically destroyed after 90 days. What remains is just the name of the object(s) and the notice that it was destroyed. According to the Public Records Act 1995, Article 6, destruction can only take place with the approval of the municipal archivist. In the event of a transfer from government archives to the e-depot, digital objects should under no circumstances be destroyed. However, an archive can be transferred to another caretaker at the request of the archive creator. In the case of private archives, the municipal archivist can decide to destroy or transfer to another care provider if a digital object no longer fits the collection (alienation). In the case of outplacement, it is possible that (part of) a transferred archive must be destroyed after a certain period. Here too, the municipal archivist approves the destruction on the basis of the destruction list. Removal takes place when errors are found in the digital objects and/or associated metadata supplied by the archive creator. The deleted object is replaced by an object in which the inaccuracies have been corrected. As stated above, destruction can only take place with the approval of the municipal archivist. In addition, destruction as well as removal is carried out in accordance with a 'four eyes principle'. A second (manager) account is required to approve all deletions. Preservica places these records in a temporary holding area, where they are permanently deleted after a 90-day period. This way, digital records can be restored in the unlikely event of an incorrect deletion.

Links:

- [Bitstop](#)
- [Article 6 Public Records Act](#)
- [Preservation policy](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

R15 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.

E-depot of Erfgoed Leiden en Omstreken

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Our e-depot system Preservica is structured in alignment with the ISO 14721:2012 Space data and information transfer systems - Open archival information system (or short OAIS) Reference model. Furthermore, Preservica has several certificates for security, quality, privacy, accessibility and sustainability which can be found in Preservica's Trust Center. In the attachment 'Image OAIS-Preservica mapping.pdf' OAIS is mapped on the various parts of the Preservica menu. The repository software comes with extensive documentation which can be found in the Community Hub. It consists of: - A logical data model - A system administration guide - A system user guide - A guide to Universal Access (in which the visitors portal is hosted) - A guide to auto preservation The system basically consists of two parts: the core application and the workflows that are the actual workhorses (for ingest, data management, storage, access, etc.). Some Preservica workflows make use of third-party software. These consist of: - Wordpress for access; - Browsertrix for web harvesting; For validation characterisation and property extraction: - JHOVE - Mediainfo - Exiftool - Fiwall - Verapdf - Wavefront-property-extraction - Apache POI Office Open XML validator - epubcheck -The PRONOM registry maintained by the UK National Archives for technical information about file formats; For migration: - LibreOffice CLI - ImageMagick CLI - Calibre - HandBrake CLI - FFMPEG CLI For rendering: - Openseadragon - 3d-renderer - Epub.js - Pdf.js - Prism.js - Replayweb.page - Amazon for storage. Preservica has several product updates every year. Some consist of larger releases, and some of smaller ones. This way Preservica makes sure that its users don't have to wait for a large release to have a minor issue resolved. Releases are accompanied by release notes and are presented in webinars. These webinars, special interest groups and a community hub are used to get feedback from users for product development purposes. A ticketing system is in place for error reporting. Moreover, ELO has a contract with Preservica for their Accelerated Success Services, meaning we can make use of a success manager helping with requests, errors or the more complex archiving matters. A yearly User Group Meeting in the UK is held to jointly establish a product development roadmap. ELO is also part of the Dutch User Group Preservica (DUGP) and takes part in its committee. This group consists of 16 Dutch archives that use Preservica as their e-depot software. Together we gather our wishes and needs and communicate these to Preservica as input for the roadmap. Since 2023 the DUGP and Preservica organise the Preservica Dutch Summit, held at one of the 16 archives. The goal of the Summit is to further communicate the Dutch wishes and needs to Preservica and give Preservica staff a better understanding of the environment and legislation we are dealing with regarding digital archiving. ELO and Preservica have signed a service level agreement in which the technical support, uptime and maintenance are agreed upon. Furthermore, during the tender it was a prerequisite that Preservica complied with the Gemeentelijke Inkoop voor IT toolbox, or short GIBIT (municipal procurement for IT toolbox). This contains a number of quality requirements for IT. Uploading to Preservica is done via a server hosted by OpenLine (as explained in the Background information), making use of a fast internet connection. By contract this speed is guaranteed to never be lower than 250 Mbps for both download and upload. In practice, the speed for downloading and uploading is around 600 Mbps. As stated above, Preservica stores all its clients' data on Amazon servers. ELO makes use of Amazon S3 servers and Glacier servers, all located in the North-Western European region. The Glacier server is used for preservation copies of large file formats that are not consulted often, like tiff or wav. The S3 server is used for smaller file formats and access copies of the files on the Glacier. Storage and back-ups are discussed in R14. Amazon has multiple certificates which can be found on their certificates webpage. ELO makes use of Preservica's private cloud service. While Preservica offers a shared cloud service, ELO opted to transfer to a private cloud in 2019. This way there are no limitations to ingesting files and metadata into the e-depot, other than the speed of the internet connection. The private cloud also makes sure that things such as time-out settings within Preservica can be customised to our needs, whereas this is not always possible in a shared cloud environment.

Links:

- [Trust center Preservica](#)
- [GIBIT](#)
- [Amazon certificates](#)
- [Open Line certificates](#)
- [Community hub Preservica](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

E-depot of Erfgoed Leiden en Omstreken

Comments:

R16 Security (R16)

R16. The repository protects the facility and its data, metadata, products, services, and users.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

Preservica is a trusted partner when it comes to security. Preservica has a dedicated Information Security Team, led by the Chief Information Security Officer (CISO) who reports to the CTO and, if necessary, the CEO and Chairman of the Board. All roles and responsibilities are designated as part of the job descriptions for personnel in the Information Security Team and include appropriate training and experience requirements. Preservica keeps up to date on relevant technology and legislation changes, has an established Risk Management Framework and Vulnerability and Patch Management Policy in line with ISO 27001:2013 control requirements. Preservica also has an established Security Incident Management Procedure in line with ISO 27001:2013. The Terms and Conditions include a Recovery Point Objective of 24 Hours and a Recovery Time Objective of 4 hours. They ensure that confirmed security incidents that affect customer data are reported to customers within 24 hours. No such issue has ever occurred at the time of writing. Moreover, Preservica has an established Backup and Disaster Recovery Plan and Procedures. These are tested at least quarterly and such tests are audited by SOC 2 Type II Auditors. All customer files and sensitive customer data such as keys are encrypted in flight and at rest. Preservica performs the following checks regarding security: - Preservica engages the services of a CREST certified independent 3rd party to conduct annual penetration testing of their services. - Preservica conducts continuous vulnerability scanning of its infrastructure whose results are reviewed at least quarterly. - Preservica conducts dynamic application security testing of all versions of its software prior to release. - Preservica conducts static application security testing of its source code whose results are reviewed at least monthly. All of Preservica's certificates and audit reports can be downloaded or requested from their online Trust Center. Roles and rights within Preservica are based on a security matrix. All files and folders are provided with a security tag, upon which access, ingest, deletion and edit rights are based for each type of user. Only the members of the e-depot team have the appropriate rights to access the back end of Preservica, see all archives and perform actions on them other than reading. Access to the back end is restricted by login with 2FA. This includes a fixed password, together with a numeric code that changes every 30 seconds. The fixed password is regularly changed by the e-depot team members. Only items that have the security tag 'public' are accessible for the wider public on the front end of Preservica, without the need for login. As explained in other requirements, Preservica stores ELO's data on the Amazon Web Services. Physical and Environmental Security are therefore managed by AWS. Amazon has a number of security related certificates, audit reports and compliances, such as ISO 27001, ISO 22301 and SOC II. This can all be found at their certificates webpage. ELO stores digital archives temporarily on a server hosted by OpenLine, in order to perform a number of pre-ingest tasks (see R09, R10 and R11). OpenLine is ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 and NEN 7510 certified. Transfer of digital collections to this server is done via a secure FTPS connection, limited to a specific IP address and password, making sure the data is being securely handled at all times during the pre-ingest phase. ELO has drawn up a continuity plan to manage and control risks regarding the e-depot. The continuity plan discusses: - What risks exist for the continuity of the e-depot? - How great is the risk that an incident, calamity or crisis will occur? - What is the impact if this occurs? - Who is responsible for prevention (archive creator, ELO, municipality of Leiden or software supplier)? - What preventative measures and actions are being taken? Risks regarding security and privacy are also a part of this and can be found on pages 18-21. As discussed in this chapter, all new software or hardware suppliers must complete ELO's Cybersecurity Questionnaire before entering into any new agreement. This questionnaire covers topics such as organisational structure, incident management, data storage security, checks and maintenance, certification, system access, the exit strategy, and subcontractors. If the questionnaire is incomplete or not completed to ELO's satisfaction, the agreement with the supplier should not be signed until the necessary changes or additions have been made. Existing suppliers are also asked to complete the questionnaire. If, based on the answers, gaps in information security appear to exist, ELO will raise this with the supplier. Together, appropriate solutions will be explored. Moreover, suppliers of software and hardware on which data is stored must comply with several demands which are included in a Program of Requirements at the time of a tender. These are also discussed in the continuity plan. Members of the e-depot team must adhere to the following basic rules to make sure that the security of data in the e-depot is guaranteed: - Passwords are changed at least four times a year. - Passwords are stored in a secure location (password vault). - Screens are locked when the employee is not at their desk. - Rights and roles in the e-depot are reviewed at least four times a year. - Rights are revoked as soon as an employee leaves ELO or a temporarily hired external party completes their assignment. - If a departing employee or a temporarily hired external party had access to shared passwords and keys as part of their assignment, these must be changed after the employee leaves the company or the assignment ends. - Only e-depot team members have access to locked data and can ingest, delete, and publish data. - Sharing and receiving digital archives takes place via a secure FTPS connection. - Passwords are not shared with third parties. The Municipality of Leiden, and ELO as a part of this, adhere to the Government Information Security Baseline (BIO), the framework of standards for the entire government, based on ISO 27001 and 27002. The Municipality of Leiden uses the VNG 'framework' that shows the minimum information security policy that must be in place ('see attachment VNG framework security policy.png'). This translates to a wide variety of policies and procedures regarding security and privacy, of which the most important ones are listed below: - Security incidents policy - Hardening policy - Vulnerability management policy - Password policy - Strategic policy for information security - Privacy by design Moreover, ELO has drawn up a Data leak policy. This document describes what a data breach is, the steps to be taken if a data breach occurs and outlines the responsibilities. The policy covers data breaches in the broadest sense, not only those involving personal data breaches but also those involving unauthorized access to other sensitive information. The policy includes a visual workflow which is drawn up in the process modelling software Engage. This can be found in attachment 2 of the Data leak policy.

E-depot of Erfgoed Leiden en Omstreken

Links:

- [Baseline informatiebeveiliging overheid \(BIO\)](#)
- [Trust center Preservica](#)
- [Amazon certificates](#)
- [Open Line certificates](#)

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Applicant feedback

R17 Applicant Feedback

We welcome feedback on the CoreTrustSeal Requirements and the Certification procedure.

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Response:

N.A.

Links:

Reviews

Reviewer 1:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments:

Reviewer 2:

Compliance level:

Implemented: the requirement has been fully implemented by the repository - 1

Comments: