Regionaal Archief Nijmegen (Gemeente Nijmegen)

Notes Before Completing the Application

We have read and understood the notes concerning our application submission.

True

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

CORE TRUSTWORTHY DATA REPOSITORIES REQUIREMENTS

Background & General Guidance

Glossary of Terms

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type. Select all relevant types from:

Archive

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

Brief Description of Repository

Regionaal Archief Nijmegen (RAN) is part of the municipality of Nijmegen. The municipal organization consists of different departments. RAN belongs to the department ‘Personeel, Informatie, Facilitair’. This department is responsible for human resources, personnel administration, managing and developing all kinds of digital services and applications within the organization, advising on and auditing information management and managing the archives of the municipality itself. RAN has been designated as the repository for the municipality of Nijmegen, neighboring municipalities (Berg en Dal, Beuningen, Druten, Heumen, Lingewaard, Wijchen, Mook and Middelaar, West Maas and Waal), a regional water authority (Waterschap Rivierenland) and a number of joint arrangements (cooperative ventures between different public authorities). According to the 1995 Public Records Act we have a legal duty to manage government archives, make them accessible and available to the public. We also manage archives of individuals and private organizations in Nijmegen and the region, audiovisual material and a library. We believe that private archives are an important addition to the government archives we manage.

We carry out different tasks for the municipality of Nijmegen and the neighboring municipalities. Besides managing archives we also inspect and advise on the information management of different municipalities. The terms and conditions of these task are being performed by us through service agreements.

For our digital repository we use two definitions: the broad and the narrow definition. With the broad definition we mean the entirety of the organization, policy, processes and procedures, financial management, data security and hardware and software, which enables the long-term management and consultation of the preserved records. The narrow definition refers to the technical facility for ingesting, preserving, managing and accessing digital information.

For the RAN preservation means the recording, storage, management and availability of digital information in such a way that it can also be consulted, accessed and authenticated over time. In other words, all actions necessary to guarantee the sustainable accessibility of digital information. The scope of our preservation policy extends to all processes surrounding the recording, storage, management and making available of transferred digital information.

The data in our digital repository consists of digitally born or digitized archives of the municipality of Nijmegen and the neighboring municipalities as mentioned above. We currently include only official transferred digital government archives in our digital repository. The different data types are: images, audio files, databases, e-mails, presentations, spreadsheets,

text, video files and websites. More information about the different data types can be found under R12 (Workflows).

More background information on our repository and our digital information policy can be found on our website.

https://regionaalarchiefnijmegen.nl/over-ons/353-e-depot-1

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
Accept

Brief Description of the Repository's Designated Community.

We want our archives to be used to good advantage by an as large as possible community. The information in our repository is accessible to everyone. The designated community of the RAN can be divided into two groups. Producers and users. There is no clear separation between these two groups, because producers can also be users.

The producers group consists of local authorities (the municipality of Nijmegen and the neighboring municipalities. RAN is designated by the municipalities of Nijmegen, Berg en Dal, Beuningen, Druten, Heumen, Lingewaard, Wijchen, Mook and Middelaar and West Maas and Waal as the repository for their archives. Municipalities are obliged to transfer their archives to a repository. After transferring the archives, civil servants of the municipality use our archives in search of information. The municipal archivist visits all the municipalities once a year to maintain a relationship with this designated community.

Producers of archives do not have to be governmental institutions. Private organizations and individuals can also be producers of the archives we hold. So we have governmental and private producers and governmental and private users.

The public, in the broadest sense of the word, is our user and thus our second designated community. The public is welcome to make use of our services, visit the reading room or our website to use our archives. We believe it is important to introduce as many people as possible to our archives by making as many archives as possible available to the public and keep developing our digital services. We offer pupils and students educational projects. We work together with elementary schools, high schools and universities in Nijmegen. So not only pupils and students make use of our archives, but also the teachers, historians and other researchers. We also work together with cultural and heritage partners in the city. We organize activities for the public. With these activities we make use of our historical archival materials.

Reviewer Entry

Reviewer 1

Comments:

accept

Reviewer 2

Comments:

Level of Curation Performed. Select all relevant types from:

B. Basic curation – e.g. brief checking; addition of basic metadata or documentation, C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
Accept

Comments

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

Insource/Outsource Partners. If applicable, please list them.

Picturae BV:

Picturae BV (https://picturae.com/en) is responsible for storage of all our data in our digital repository and they are responsible for hosting the digital preservation system used within our digital repository, that is Archivematica. Archivematica is hosted on the servers of Picturae BV, and the technical infrastructure complies with various ISO standards for safe and sustainable storage. It is an open source system based on the principles of the "Open Archival Information System" (OAIS), a widely supported guideline for sustainable accessibility. Archivematica is designed to automatically and in a controlled way record, preserve, manage and make available digital archives to other linked systems, such as in our case the Atlantis collection management system. Picturae BV is responsible for the technical infrastructure of Archivematica and they provide us with updates of Archivematica. They are not the developers of Archivematica - the developer is Artefactual (https://www.artefactual.com). Besides updates, Picturae also provides backup and disaster recovery solutions for all our data on their servers. The terms and conditions of our collaboration with Picturae BV are described in detail in our service agreement.

DEVENTit BV:

The collection management system we use to manage, record and make our archives available is Atlantis. Atlantis is hosted on the servers of DEVENTit BV (https://www.deventit.nl/?lang=en). The physical data storage facilities are located in the Netherlands. DEVENTit is responsible for the technical infrastructure of Atlantis. They are the developers of Atlantis and they also provide us the updates. DEVENTit also provides backup and disaster recovery solutions for all our data on their servers. The terms and conditions of our collaboration with DEVENTit are described in detail in our service agreements.

More information on our insource/outsource partners can be found in R15 (Technical infrastructure) and R16 (Security).

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

Summary of Significant Changes Since Last Application (if applicable).

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
N/A

Other Relevant Information.

Two attachments:

- 20220405_OverviewOfDocumentation
- 20220401_PrivateArchivesDepositAgreement

Link to the website: https://regionaalarchiefnijmegen.nl/
Link to the documentation on the website: https://regionaalarchiefnijmegen.nl/over-ons/353-e-depot-1 (at the bottom of the page)

Link to the English landing page on the website: https://regionaalarchiefnijmegen.nl/english

-

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

ORGANIZATIONAL INFRASTRUCTURE

1. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
accept

Response:

Regionaal Archief Nijmegen (RAN) collects and stores historical sources on the history of Nijmegen and its surroundings to make these sources available to researchers and other interested parties. Our mission is to ensure that our sources are available to and used by a wide range of individuals and communities. We collect and store historical resources for the public and we preserve the data for eternity. By preserving we mean the act of capturing, storing, managing and making

available digital information in such a way that it remains available, accessible, and authentic over time. Or, in other words, all of the necessary actions to ensure the sustainable storage and accessibility of digital information. By doing this we hope to strengthen historical awareness, involvement of inhabitants with their city and region and the social cohesion and identity of the city and region. As mentioned in R0, RAN is part of the municipal organization of Nijmegen. Therefore the ambitions and goals of the RAN align with those of the municipality of Nijmegen. According to our city budget plan, the RAN is part of the culture and cultural heritage program. Our ambitions are to be an attractive city with an accessible and high-quality cultural offering and to have a cultural policy/climate focused on renewal and innovation. Our city is the oldest city in the Netherlands, with a rich history and unique character. We use this unique heritage to increase the attractiveness of our city for (new) residents, businesses and visitors.

Our work is based on the 1995 Public Records Act. It is a Dutch law that prescribes what type of information governmental organizations must save, store and make available to the public. Governmental bodies in the Netherlands are obliged to ensure that their archival records are in good condition, properly arranged and accessible. They must transfer archives older than 20 years to a designated repository. RAN is the designated repository for the municipality of Nijmegen and a number of neighboring municipalities. This means that we have a legal duty to manage government archives, make them accessible and available to the public. This gives the public the ability to audit the government, find legal evidence, and conduct historical research and engage in other ways with our collections. More information about the 1995 Public Records Act can be found in R2 Licenses and in R11 Data Quality. There is also an English version available of the 1995 Public Records Act (https://www.nationaalarchief.nl/sites/default/files/field-file/Netherlands%20Public%20Records%20Act%201995.pdf).

All these agreements with our funders are described in detail in our service agreements. The main contract contains general information about depositor and repository and their mutual obligations. In general the repository is responsible for the conservation and sustainable management of archival records. The repository provides storage of and access to the archival records and advises on transferring archival records between depositor and repository. The main contract also contains information about the duration, how to handle amendments and the termination of the service contract. Also, all service costs, accountability and mandates are specified. Annually, an evaluation between depositor and repository takes place. At this meeting the depositor produces a yearly overview of the amount of archival records and other related matters are discussed.

More information about Regionaal Archief Nijmegen is available on our website. See https://regionaalarchiefnijmegen.nl/over-ons/organisatie for the Dutch version and https://regionaalarchiefnijmegen.nl/english for the English version.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

2. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

On the basis of the 1995 Public Records Act, governmental organizations in the Netherlands are obliged to ensure that their archival records are in good condition, properly arranged and accessible. They must also ensure the destruction of designated archival records. Archival records which are not eligible for destruction must be transferred to a repository no later than 20 years after they are closed. Regionaal Archief Nijmegen (RAN) has been designated as the repository for the municipality of Nijmegen, neighboring municipalities, a regional water authority (partly) and a number of joint arrangements (cooperative ventures between different public authorities).

Archival records (regardless of form) that have been transferred to a repository are publicly accessible according to the 1995 Public Records Act (Article 14). Everyone is entitled to consult these records free of charge and to obtain at their own expense, illustrations, copies, extracts, and revisions of them.

Access restrictions

When transferring records, a governmental organization may, following the advice of the municipal archivist, place restrictions on disclosure for a specified period of time because of:

• Respect for personal privacy;
• The interest of the State or its allies;
• The prevention of disproportionate benefit or disadvantage to the natural or legal persons involved or to third parties.

At the time of transfer, a transfer declaration is drawn up in accordance with Articles 9 and 10 of the 1995 Public Records Decree (https://wetten.overheid.nl/BWBR0007748/2013-01-01). This transfer declaration lays down which archival records are to be transferred to the repository and which of these archival records are subject to restrictions on public access and for how long. In order to draw up this transfer declaration, the RAN uses documentation of the National Organization of Provincial Archive Inspectors (LOPAI).

A restriction on public access is included in the metadata of archival records. This is done both at the archive level and at the level of individual records. On the basis of this metadata, access to archival records can be authorized through the website of RAN and both employees and visitors can see if there is a restriction on public access. At the start of each new calendar year, the municipal archivist checks which restrictions on public access are to be lifted.

Under certain conditions it is still possible to consult transferred archival records that are not yet publicly accessible. The reason(s) for consulting such records should then outweigh the reason(s) to limit access.

If someone wishes to consult a non-public archival record, an application form must be completed and signed (https://regionaalarchiefnijmegen.nl/images/praktische-informatie/Openbaarheid/20210324_Formulier_Toestemming_raadpleging_niet-openbare_archieven.pdf). The applicant has to fill in: Name, E-mail address and/or telephone number and the non-public archival records they wish to consult. In addition, the applicant must declare the following:

1. that information obtained from the archives will only be used
a. in the context of scientific research with the subject:……
b. in the context of:……
2. that he/she will not publish or otherwise make public anything that could cause disproportionate harm to the interests of living persons;
3. that he/she will use any photocopies supplied to him/her only for his/her own use;
4. that he/she will use any other information from the archives that come to his/her notice, and for which no permission to publish has been obtained, only for his/her own use use them only for his/her own study and not to publish them or make them public in any other way or communicate them to third parties;
5. that he/she will indemnify the municipality of Nijmegen against claims by third parties for all damages that they suffer as a result of the consultation or other use by the applicant.

The form can then be handed in at the RAN-reading room or sent digitally (by scan) to hetarchief@nijmegen.nl. Within five working days, the municipal archivist will decide whether permission will be granted. An appeal is possible if the request is denied. A granted permission is valid for the duration of the research with a maximum of one year. If the research has not been completed after one year, permission must be requested again. The completed forms containing personal information are retained for as long as the disclosure restriction rests on the archival record(s), whether or not permission to consult the records has been granted.

Whenever permission is granted to consult non-public documents, the archival records concerned should be consulted in the reading room regardless of whether they are analog or digital. In certain cases, copies of archival records may be made. However, this only applies to analog archival records.
The above information regarding the public accessibility of archives can also be found on the RAN-website (https://regionaalarchiefnijmegen.nl/praktische-informatie/openbaarheid).

Private archives

RAN also manages private archives. These archives are not subject to the 1995 Public Records Act. However, the depositor of these archives may, in consultation with the municipal archivist, decide to restrict the public access of specific archival records for a certain period of time. The initiative to limit the public accessibility of specific records for a certain period of time can also come from the municipal archivist. These restrictions are mentioned in (annexes to) the deposit agreement which is drawn up when private archives are taken in by RAN. These restrictions are also included in the metadata of archives and archival records.

A agreement format is used to create a customized agreement for each private archive being deposited depending on the type of archive and specific arrangements made with the depositor. Within the format, the following subjects are addressed: Deposited archive (Article 1), Transfer of ownership (Article 2), Obligations of depositor (Article 3), Obligations of recipient (Article 4), Disclosure under the Copyright Act (optional), Terms of use of disclosure and reproduction regarding third parties (optional), Terms of use for publication and reproduction related to Regionaal Archief Nijmegen (optional), Indemnification (Article 5) and Applicable law and competent court (Article 6). The format is attached as an appendix to the application.

In the case of non-public records from private archives, permission must sometimes be obtained from the depositor. In that case, RAN will refer to the person or organization from whom that permission should be obtained and will explain how to contact them.

Data types

RAN holds and accepts different types of data. These different data types are: images, audio files, databases, e-mails, presentations, spreadsheets, text, video files and websites. Whether access restrictions apply to records depends on their content, not their appearance or type of data. More information about the different data types can be found under R12 (Workflows).

Copyright

In addition to records that are not publicly accessible, there are also records that, because of copyright, can only be consulted in our reading room or can only be (re)used with the permission of the copyright holder. Copyright information is provided at the lowest level of description of archives. We use five different types of copyright: (1) Consultation only

possible in reading room, (2) Copyright protected, (3) CC-BY-SA, (4) CC0 and (5) Public domain. Our collection management system automatically determines authorizations (on the basis of the aforementioned five types) for the linked information objects on our website.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

3. Continuity of access

R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
accept

Reviewer 2

Comments:
3 – The repository is in the implementation phase
Accept

Response:

The availability and accessibility of digital archives is primarily guaranteed by the 1995 Public Records Act. It states that governmental bodies are under the obligation to preserve and maintain the archival records under their care in good condition, properly arranged and accessible, as well as to ensure the destruction of the relevant archival records (1995 Public Records Act, Article 3; see also R2. Licenses).

Archival records that are eligible for preservation must be transferred to a designated repository for permanent preservation no later than 20 years after they are closed. When transferring these records to the archival repository, specific rules must be observed (1995 Public Records Act, Article 12). For transferring archival records the mayor and

aldermen of the municipal bodies appoint a repository (1995 Public Records Act, Article 31). The designation of a repository is laid down in an archive regulation. The 1995 Public Records Act requires a municipality to adopt an archive regulation which provides for the care of the archives not only in the designation of a repository but also in people, resources and archive management rules. This archive regulation is an important element in the governance (Article 30). The municipality of Nijmegen has designated Regionaal Archief Nijmegen (RAN) as the municipal repository. In addition, surrounding municipalities have also designated RAN as their municipal repository. RAN is organizationally a part of the administrative organization of the municipality of Nijmegen.

Governance

The municipal repository is managed by a qualified municipal archivist. The municipal archivist also supervises the proper management of yet untransferred archival records of municipal bodies (1995 Public Records Act, Article 32).). The costs involved in the task of archive management and supervision are charged to the municipality in question (1995 Public Records Act, Article 30 Municipalities reserve sufficient financial resources for this within their budgets on a structural basis. RAN receives financial means for the execution of its tasks from the municipality of Nijmegen (as an organizational unit) and from the various surrounding municipalities on the basis of separate service agreements concluded for a minimal period of 5 years. The current funding period is 2021-2025. In the unlikely event that a municipal body no longer is able or wishes to have the archive management and supervision carried out by the RAN, the 1995 Public Records Act requires that the archive management and supervision be arranged elsewhere. For municipalities, the administrative responsibility for the implementation of the 1995 Public Records Act lies at all times with the municipal executive (mayor and aldermen). They must ensure that proper archive management is possible, so that the archives entrusted to them are in good condition, properly arranged and accessible. Thus, there is a sound financial and organizational basis for ensuring the availability and accessibility of both analog and digital archival records.

Policy

The municipality of Nijmegen has also drawn up various policy documents that underline the importance of sustainable accessibility of digital information and archival records and indicate how to achieve this. By using (open source) software with which data can be exchanged in a simple and structured way, by using open and/or widely accepted file formats and by applying specific metadata standards, sustainability becomes a structural part of the information management chain and of digitization projects. The documents in question are ‘Duurzaam digitaal informatiebeheer’ (policy for sustainable digital information management and use of a digital repository) and ‘Digitaal Informatie Beleid 2021-2025’ (guiding framework for the information policy of the municipality of Nijmegen).

Sustainable access

In order to guarantee sustainable access to our digital preservation system Archivematica, RAN is registered as a beneficiary of the Picturae Escrow Scheme. This is important if Picturae, the supplier of Archivematica, can no longer guarantee continuity. In that case, the source codes and documentation of the application curated by the escrow agent will be provided to the end user (RAN). Furthermore, agreements have been made with Picturae in a Service Level

Agreement (SLA) about performance with regard to processes and procedures for aspects such as backup & restore, fixity controls, exit strategy, service provision and hosting. Work is also currently underway to establish an escrow arrangement with the supplier of our Atlantis collection management system, DEVENTit, with which the archival records included in our digital preservation system are made available (via our website). As with Picturae, agreements have already been made with DEVENTit regarding the performance of processes and procedures for aspects such as backup & restore, fixity controls, exit strategy, service provision and hosting, which are included in a Service Level Agreement (SLA).

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

4. Confidentiality/Ethics

R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Regionaal Archief Nijmegen (RAN) ensures that archives are created, processed, accessed and used in compliance with disciplinary and ethical standards. This is done in various ways.

Restrictions on access

As already mentioned in R2 (Licenses), the 1995 Public Records Act states that archives transferred to a repository are in principle accessible to the public. However, when transferring records, a governmental organization may, in consultation with the municipal archivist, limit the public accessibility of records for a certain period of time. This is recorded in the transfer declaration and in the metadata. This restriction can only be lifted on special request and after obtaining written permission from the municipal archivist.

In addition to the 1995 Public Record Act, governmental bodies that place data in the public domain are also subject to the Algemene verordening gegevensbescherming (AVG). The AVG is also known by its English name: General Data Protection Regulation (GDPR, see also: https://gdpr.eu/tag/gdpr). The 1995 Public Records Act and the GDPR partially conflict with each other. The 1995 Public Records Act focuses on active disclosure. The GDPR, however, stipulates that (governmental) organizations should exercise restraint when it comes to the publication of personal data. Archival records sometimes contain personal data. Take for example the details of an applicant for a building permit. In such a case, RAN complies with the GDPR by not (actively) disclosing these personal details or by implemented technical safeguards, such as restriction of public access. This already must be taken into account when compiling the metadata by not including personal data or to include them as separate metadata. We do not anonymize personal data. The depositor indicates whether the archival records hold personal data and if can be made public or not. Also in the pre-ingest phase we check the conditions regarding the processing of personal data. You can find this in the Procedure models for the transfer digital archives. The digital archivist is responsible for this.

Within the municipality there are a few people responsible for the supervision of personal data. We have a Privacy officer, Data protection officer and Chief Information Security Officer (CISO). The Privacy officer supports and advises the municipal organization when it comes to handling and holding personal data. He also works with the organization to create awareness. The Data protection officer advises and provides independent supervision within the municipality of Nijmegen and is the contact person for the GDPR. The CISO functions like a spider in a web when it comes to data security within the municipality. He is responsible for implementing and supervising our data security policy. The CISO has a central role in the management of all personal data related work processes.

Our staff is trained in the management of data with risk. As stated above a number of people fulfill specific GDPR tasks but the rest of staff is also trained. Everyone working for the municipality is required to take online courses about privacy and information safety provided by the municipality.

Risk management

To reduce the risk of digital archival records with a disclosure restriction and any associated metadata ending up in the public domain, a number of safeguards have been built in. These range from technology to procedures and the integrity of employees. For example, the service provision by the municipality of Nijmegen and therefore (as part of the same organization) the service provision by the RAN is in line with the Baseline Information Security Government (BIO). The BIO is a common framework of norms for information security within the entire government, based on the internationally

recognized and current NEN-ISO27001 and NEN-ISO27002 information security standards (https://www.nldigitalgovernment.nl/overview/information-security/government-information-security-baseline/) This means, among other things, that there are specific requirements for the systems (soft- and hardware) used by RAN as well as access to these systems based on authorizations. The information security of the organization is supervised by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO); information security awareness among the employees of the municipality of Nijmegen is specifically stimulated.

Ethical norms

Finally, there are also ethical norms with which the employees of the municipality of Nijmegen (and therefore also RAN) must comply. These are basic norms of governmental organizations laid down in the Civil Servants Act. These standards focus on subjects on which there is general agreement: such as preventing bribery and conflicts of interest, and dealing carefully with confidential information. Public servants must behave professionally and ethically (https://www.government.nl/topics/public-administration/integrity-in-public-administration). They must not commit fraud, accept bribes, or leak confidential information. By taking an oath or promise, a public servant promises to abide by these standards. Public servants who are not employed by the municipality, such as hired workers, sign a declaration stating that they will comply with the integrity rules.

For archivists there are also specific codes of conduct. For example, the Royal Association of Archivists in the Netherlands (KVAN) - the association for Dutch professionals working in the archives sector - has committed itself to the Professional Code for Archivists. This code is a translation of the ICA Code of Ethics formally adopted by the General Assembly of the ICA held in Beijing China in 1996 (https://www.ica.org/en/ica-code-ethics). The association has also committed itself to the Universal Declaration on Archives. This is a translation of the Universal Declaration on Archives that was adopted by the 36th Session of the General Conference of UNESCO on 10th November 2011 (https://www.ica.org/en/universal-declaration-archives).

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

5. Organizational infrastructure

R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Institutional embedding

Regionaal Archief Nijmegen (RAN) is a part of the administrative organization of the municipality of Nijmegen and fulfills a statutory task. As mentioned in R3 (Continuity of access), the 1995 Public Records Act requires governmental agencies, including the municipality of Nijmegen, to designate a repository for permanent preservation of archival records no later than 20 years after they are closed. The municipality of Nijmegen has designated RAN as the municipal repository. RAN is responsible for the acquisition, management, accessibility and availability of these archival records (regardless of form) and also for the supervision of the management of both the archival records of municipal bodies that have yet to be transferred and those that will eventually be destroyed (1995 Public Records Act, Article 32).

RAN is not a member of or affiliated to any national or international body. The municipality of Nijmegen though (of which RAN is a part) is a member of the Vereniging Nederlandse Gemeenten (VNG), the association of Netherlands Municipalities. The association represents the interests of all municipalities when dealing with the national government and offers services to those municipalities.

Staff

RAN has a staff of 28 employees. All employees are permanent. These employees work in the following areas: management (1), archival processing (7), public services (5), support work (5), inspection and acquisition (4), digital archiving, digital advice and systems management (4), restoration and repository management (2).

Funding

The municipality of Nijmegen includes structural financial resources in the annual municipal budget for the performance of these tasks. These funds are used to pay for personnel and labor as well as for materials, accommodation and IT and form the basis of the digital repository: the entirety of the organization, policy, processes and procedures, financial

management, personnel, data management, data security and hardware and software that enables the management and accessibility of digital archival records. This also includes payments for hosting and maintenance charged by our suppliers Picturae B.V. (digital preservation system Archivematica) and DEVENTit (collection management system Atlantis).

For the further development of procedures and systems, additional resources are made available on intake basis. During an intake we check whether changes/innovations sufficiently comply with mission and policy. Space is also created for this within the municipal budget on an annual basis. General municipal financial resources are used to finance the management and maintenance of buildings and also the training and development costs of personnel. This ensures access to ongoing training and professional development for RAN staff. The range and depth of expertise of both the organization and its staff is further addressed in R6 (Expert guidance). The amounts set aside always take into account indexation and other changes. The municipal executive must always ensure that sufficient financial resources are available (1995 Public Records Act, Articles 3 and 30).

This applies both to the city council of the municipality of Nijmegen and to the city councils of a number of regional municipalities. For the execution of its tasks, RAN receives financial resources from the municipality of Nijmegen and also from surrounding municipalities that have designated RAN as their repository. In the latter case, these funds are made available on the basis of separate service agreements concluded for a minimal period of 5 years. These agreements take into account the (administrative) size of each municipality and the size of the (digital) archives to be managed. The amount needed for RAN to carry out the archive management for regional municipalities is guaranteed and is provided for proportionately by the affiliated regional municipalities. When a regional municipality no longer participates, the costs will be divided among the remaining regional municipalities.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

6. Expert guidance

R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either inhouse or external, including scientific guidance, if relevant).

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

In-house expertise

In-house staff of Regionaal Archief Nijmegen (RAN) is trained in matters of digital preservation, for example by following the course “Leren preserveren” (https://lerenpreserveren.nl) by the Netwerk Digitaal Erfgoed (NDE, https://netwerkdigitaalerfgoed.nl). In so doing we acquired knowledge and established contacts with other professionals in digital preservation. We update in-house expertise through newsletters, conferences, presentations and research.

We are a part of the municipal organization of Nijmegen. Within the organization we are able to communicate with experts on a variety of subjects like records management, information architecture, information security, privacy and information laws and regulations.

External expertise

We are an active member of the Dutch archives sector; some staff members are a member of the Koninklijke Vereniging van Archivarissen in Nederland (KVAN, https://www.kvan.nl), the Dutch professional association of archivists. This organization promotes archival expertise, supports cooperation between archival professionals and organizations and lobbies on behalf of the archives sector on a national level.

Staff members are active on the website of Kennisnetwerk Informatie en Archief (KIA, https://kia.pleio.nl) a community and knowledge platform for Dutch archives and information professionals. The KIA website is the prime instrument for reaching out to fellow archives professionals and keeping up to date concerning the latest developments in the professional field.

We participate in the Netwerk Digitaal Erfgoed (NDE). The mission of this organization is to develop – with all of the heritage institutions in the Netherlands - a system of facilities and services for improving the visibility, usability and sustainability of digital heritage. Within this framework we can turn to experts on varying matters. As a user of the Archivematica software for digital preservation we participate in the Archivematica user group hosted by our commercial partner Picturae. The group plans a meeting once or twice per year where users hold presentations, demonstrations and discussions.

As a user of the Atlantis software for collection management we participate in the Atlantis user group hosted by our commercial partner DEVENTit. The group also convenes once or twice per year and shares information through presentations, demonstrations and discussions. The group stays in touch through an online forum.

User feedback

We involve users of our archival collections in the development of our website. We do this by participating in the Kwaliteitsmonitor Archieven, a periodical standardized survey that is used by Dutch archival institutions. We do this by posting the survey on the landing page of our website.

The municipal government has instituted a digital city panel. This panel consists of a few thousand citizens from all layers of local society. We sometimes ask citizens in this panel questions pertaining to our (digital) services; this way we gain a broader view of our local and/or digital presence and the quality of our (digital) services.

We have formed a small panel of regular users with the purpose of periodically interviewing them concerning our (digital) services and the usability of our website. We conduct small qualitative tests where we sit next to users and observe them using our website, analyze their behavior and draw conclusions concerning usability.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

DIGITAL OBJECT MANAGEMENT

7. Data integrity and authenticity

R7. The repository guarantees the integrity and authenticity of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:

4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Data integrity

In our requirements for digital archives it is specified that all digital objects must be delivered with inclusion of a checksum created with the MD5 or SHA-256 algorithm. Our requirements for digital archives are described in the document ‘Overdrachtseisen digitaal archief’, an English translation is available in the document ‘Transfer requirements for digital archives’ (https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220313_Transfer_requirements_for_digital_archives.pdf).

The checksum is also a required element in the metada standard Toepassingsprofiel Metadatering Lokale Overheden (https://www.nationaalarchief.nl/archiveren/kennisbank/tmlo). Upon ingest in our digital preservation system all checksums are recalculated and compared with the original checksums. The ingest procedure will stop immediately if one of the objects has been altered.

During the ingest procedure the digital preservation system also calculates checksums for all digital objects, these checksums are validated every time the location of the digital objects changes.

Once the ingest procedure is completed we periodically test the integrity of the stored Archival Information Packages. We use the Fixity application for this purpose (https://www.archivematica.org/en/docs/storage-service-0.17/#fixity). This application is integrated in our digital preservation system. The reports of the scanned Archival Information Packages are displayed in a dashboard called AM-Watch.

Completeness

The completeness of the data is checked during the ingest procedure by a microservice within the digital preservation system. The microservice is called ‘Verify transfer compliance’. This microservice checks if every file is present by validating the checksum that is specified in the metadata file. When a file is missing the checksum can’t be validated, which will result in a failed ingest. The microservice also checks whether every digital object is linked to a metadata file. This means it is not possible to ingest a digital object that is not described in a metadata file.

Authenticity

During the pre-ingest stage we use an intake document to check if the digital archive meets the requirements on paper (described in the document ‘Intakedocument voor het opnemen van digitaal archief in het e-depot’, an English translation

is available: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220317_Intake_document_for_digital_archives.pdf). This document is also used to capture all relevant metadata regarding the depositor and the deposit, including the origin of the digital archive. This information is used to describe the digital archive in our collection management system. The description of the digital archive will be published on our website. Furthermore, metadata regarding the origin of digital objects is also part of the metadata standard TMLO. If the provenance metadata is available it must be included in the metadata file according to our requirements.

Every digital archive and all digital objects belonging to the digital archive receive a unique identifier. The identifiers are stored in a database in our digital preservation system. The identifiers are used to establish a link between the digital objects and the metadata and also to establish a link between the original data and the disseminated data. Through naming conventions it is possible to identify the archive a digital object belongs to. The kind of unique identifier used within the digital preservation system is OSSP UUID, a ISO-C:1999 application programming interface (API) and corresponding command line interface (CLI) for the generation of DCE 1.1, ISO/IEC 11578:1996 and RFC 4122 compliant Universally Unique Identifiers (UUID's). Additionally, every archive is linked to a depositor in our collection management system to document the origin.

The original files and the original metadata files are stored unchanged. This is an important part of our preservation strategy and specified in chapter two of our preservation policy (described in the document 'Preserveringsbeleid', this document is available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210422_Preserveringsbeleid_overgebrachte_digitale_archieven_Website.pdf). Every ingested digital object must be kept unchanged at all times at bit level. This is done by a combination of virus checks, end-to-end controls, integrity checks, security measures and if needed backup and disaster recovery.

Every step during the ingest of a digital archive is logged by the digital preservation system as PREMIS metadata. The PREMIS metadata is captured in a METS metadata file that will automatically be stored within the Archival Information Package of the digital archive after a succesful ingest. The METS metadata file is basically an audit log and can be used to supervise all actions that were carried out during the ingest of a digital archive.

Version control

The digital objects we receive from the depositor are designated as original files once the transmission is official. The original files are stored without any changes. If an original file has a file format that is obsolete or considered as in danger of becoming obsolete we will migrate to another file format. We will always keep the original file after a file format migration. Therefore after a file format migration there will be two versions of the same file in the repository: the original file and a preservation file. The details of a performed file format migration are saved within the METS metadata file. The preservation files are placed in the Archival Information Package in the same directory as the original files. The preservation files receive a filename that is a combination of the original filename and an UUID. Thus ensuring the files do not only have another extension but also a unique name. The filenames of the preservation files are also saved within the METS file. The depositor will be notified if we carry out a file format migration.

Data types

The types of data we manage do not have an impact on our workflows. The workflows can handle all the different data types we accept. The different data types are: images, audio files, databases, e-mails, presentations, spreadsheets, text, video files and websites. At this moment we do not hold all these different data types in our repository but we tested all the workflows with the different data types. More information about the different data types can be found under R12 (Workflows).

Standards and conventions

Archiefwet (1995 Public Records Act, https://wetten.overheid.nl/BWBR0007376/2020-01-01): A Dutch law that prescribes what type of information governmental organizations must save, store and make available to the public in a good condition, properly arranged and accessible. Governmental bodies must transfer archives older than 20 years to a designated repository. Regionaal Archief Nijmegen (RAN) is the designated repository for a number of depositors. There is also an English version available of the 1995 Public Records Act (https://www.nationaalarchief.nl/sites/default/files/field-file/Netherlands%20Public%20Records%20Act%201995.pdf).

Archiefregeling (https://wetten.overheid.nl/BWBR0027041/2014-01-01): The Public Records Decree, an extension to the 1995 Public Records Act that describes in detail what kind of metadata must be recorded and kept in order to meet its requirements.

NEN-ISO 23081-1 (https://www.nen.nl/nen-iso-23081-1-2017-en-240621): Covers the principles that underpin and govern records management metadata. These principles are applicable to: records and their metadata, all processes that affect them, any system in which they reside and any organization that is responsible for their management.

Open Archival Information System (OAIS; https://www.iso.org/standard/57284.html): We use OAIS as a conceptual framework for our data repository. Our digital preservation system was also created with OAIS in mind, it uses the OAIS-functions as building blocks for processing digital objects from ingest to access.

Toepassingsprofiel Metadata Lokale Overheden (TMLO; https://www.nationaalarchief.nl/archiveren/kennisbank/tmlo): Metadata standard for Dutch local governmental bodies determined by the Dutch National Archives. The standard is based on all the metadata requirements in the Archiefwet (Public Records Act), Archiefregeling (Public Records Decree) and NEN-ISO 23081-1.

Toepassingsprofiel XML (ToPX; https://www.nationaalarchief.nl/sites/default/files/field-file/topx-2.3_1.xsd): A technical standard for metadata files. ToPX is the translation of the metadata standard TMLO to a machine-readable XML format. The repository can process this XML format automatically. A microservice checks if the structure is conform the standard and if all the required metadata elements are present.

Metadata Encoding and Transmission Standard (METS; http://www.loc.gov/standards/mets): International standard for encoding descriptive, administrative, and structural metadata regarding digital objects by making use of XML schema language.

Preservation Metadata Implementation (PREMIS; https://www.loc.gov/standards/premis): International standard for metadata to support the preservation of digital objects and ensure their long-term usability. PREMIS is fully implemented in our digital preservation system.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

8. Appraisal

R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Selection of data

Regionaal Archief Nijmegen (RAN) acquires government archives on the basis of its statutory task. Governmental bodies are obliged under the 1995 Public Records Act (Article 12) to transfer archival records that are eligible for permanent preservation to a designated repository no later than 20 years after they are closed. RAN is the repository for the municipality of Nijmegen and a number of regional municipalities and therefore periodically receives from these governmental organizations the archival records designated for permanent preservation.

In order to determine which archival records should be retained and which should be destroyed, Article 5 of the Public Records Act requires governmental bodies to use carefully drawn up selection lists. A selection list applies to a specific governmental body and contains an overview of the tasks of the governmental body. The core of the list is a list of archival records divided into the categories of records to be preserved and records to be destroyed. In the case of records to be destroyed, the list states the period after which the records must be destroyed. The selection list also offers the possibility of permanently preserving items that are eligible for destruction. These must be records that are important to the organization because of the fact that they are representative examples of the tasks and work performed or that provide insight into important trends within society.

Private archives

The Public Records Act does not apply to private archives. For the acquisition of private archives, RAN has drawn up a separate policy document named ‘Beleidsplan acquisitie particuliere archieven en collecties Regionaal Archief Nijmegen’. This document is available in our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20181017_Beleidsplan_acquisitie_particuliere_archieven_en_collectie_Regionaal_Archief_Nijmegen.pdf. This policy document explains the criteria the material must meet to be eligible for inclusion in our collection. Submitting private archives is voluntary, we do not impose the same quality requirements as we do for government archives. We acquire new private archives if they are authentic and unique, are typically Nijmegen or explicitly focused on Nijmegen, and have added value to the existing collection. If this is not the case we will not accept them. We do offer (practical) advice on sustainable storage and accessibility through a publicly available guideline and a brochure on our website (https://regionaalarchiefnijmegen.nl/praktische-informatie/archiefmateriaal-aanbieden). The guideline and the brochure only contain general advice, they do not describe requirements. The recommended file formats for private depositors are the same as the file formats in the list of preferred and acceptable formats for governmental depositors. We use a form to enquire about the technical aspects of the archive, such as: data type, file size, file structure, file formats, compression, encryption etc. This form is included in the guideline as attachment. If we decide to include private archives in our digital repository then these archives are handled with the same transfer procedures as government archives, with the difference that some formal steps or actions do no apply and that we take the responsibility for (extra) metadata. If the archives contain non-preferred file formats we will first examine whether a format migration can be carried out. If this is not possible then only bit preservation is offered. This may have consequences for availability. For more detailed information about preferred and acceptable file formats see the paragraph ‘preferred and non-preferred file formats’.

Procedures

Governmental depositors - in the case of RAN the municipality of Nijmegen and surrounding municipalities - are responsible for selecting and preparing records to be transferred to RAN, as described in article 3 of the 1995 Public Records Act and article 26 of the 2009 Archives Regulation (http://wetten.overheid.nl/BWBR0027041/2014-01-01). They announce an official transfer during monitor consultations with the municipal archivist. The municipal archivist then evaluates whether a transfer process can actually commence. This assessment looks at more general matters such as the applied valuation and selection, the public accessibility and the quality of the descriptions of the archival records. If the outcome of the assessment is positive, an intake is started.

During an intake, in the case of digital archives, we check whether specific transfer requirements as described in the document ‘Overdrachtseisen digitaal archief’ are also being met. For the English version of this document see: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220313_Transfer_requirements_for_digital_archives.pdf. Meeting these requirements is necessary for a digital archive to be properly included in our digital repository and thus for the official transfer of a digital archive. The requirements serve as a guideline for depositors when preparing for a transfer, but also for setting up their digital information management.

The specific transfer requirements relate to the metadata, the digital objects and the method of transfer. Metadata must, for example, be supplied on the basis of a documented metadata schema and associated exchange format that meets the TMLO metadata standard intended for Dutch governmental organizations (see R7 for more detailed information about TMLO). Digital objects must be, among other things, free of viruses, corruption, encryption, and in addition only have file formats that are listed in our "Preferred and Acceptable Formats" overview. The transfer of an information package (metadata and digital information objects combined) must take place via a secure FTP server or another secure service for file transfer. The information package must also include a current, complete and logically coherent overview of the digital archive and an overview of the number of information objects to be transferred per file format, the number of metadata files and the total size of the transfer in bytes.

Preferred and acceptable file formats

The list of preferred and acceptable formats is attached as an appendix to the document ‘Overdrachtseisen digitaal archief’ and also to our preservation policy (see R10 Preservation plan). A separate English version of the document is available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220329_Preferred_and_acceptable_file_formats.pdf. The list contains only open standards and widespread file formats whose future support is not currently under threat. The list has been compiled on the basis of the operation of our digital preservation system and the insights of national and international archives and other cultural institutions such as the Dutch National Archive, The Dutch Institute for Sound and Vision, Library of Congress, The British Library and University of Cambridge. The list is not static in nature and will be updated annually based on technological changes and new insights.

If the file formats of the digital objects supplied by a governmental depositor do not appear on this list, we will first examine whether a format migration can be carried out. If a format does not appear on the list and cannot be migrated to another

format, only bit preservation is offered. The choice for bit preservation may have consequences for the availability. For the purpose of sustainable accessibility we strive for the use of file formats that are also suitable as a preservation format so that there is no need to convert and only one format needs to be preserved that passes as both the original format and the preservation format. We also strive to provide data in file formats that can be readily used by our users for the purpose of public access. When file formats of digital objects are not suited for public access, we make the items available in a derivative file format. All of this is explained in more detail under R10 (Preservation plan) and R14 (Data reuse).

If, during the intake, it is established that all the requirements described above are met, a preliminary technical examination of the digital archive is started (the pre-ingest). If no irregularities are found, the ingest starts with the transfer of the archive to our digital preservation system. For more information about the pre-ingest and ingest phase, see R7 (Data integrity and authenticity) and R11 (Data quality).

After completion of the ingest, we perform a general check of the content, accessibility and availability of the digital archive via the RAN collection management system and our linked collection website. If the result is positive, the official transfer can be arranged. With an official transfer, the depositor declares that the digital archive (digital objects and metadata) has been transferred to the repository and the municipal archivist declares that the digital archive has been taken into custody. The process described here for the transfer of digital archives is described in detail in the document ‘Procedures voor opnemen van digitaal archief in het e-depot’. This document is available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210621_Procedures_opnemen_digitaal_archief_e-depot_Website.pdf. A more compact English version of the procedures in this document is also available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220321_Procedure_models_for_the_transfer_of_digital_archives.pdf.

Removal of items

In the case of removal of items from our collection, there can be two scenarios. In the first scenario, we are dealing with private archive items. In that case, removal will usually mean disposal (and therefore destruction) or return of items in case of custody. This process is usually initiated, executed and administered by RAN itself. The second scenario is based on the removal of transferred archives from the management of the RAN at the request of a governmental depositor. In that case, the removal of items from our collection also implies the removal of items from our digital repository and that requires a very precise and planned approach. The ingested information packages will be migrated from our digital preservation system to a new location at the request of the depositor. In addition, the metadata included in our collection management system will also be migrated. These actions will be discussed in detail with the depositor in question beforehand and test exports will also be carried out. All records and objects in our collection management system have persistent identifiers. To be more specific: we use handles registered under the Handle System, a service provided to us by SURFsara (see also R13, Data discovery and identification). Therefore a request to SURFsara to convert the handles to a new web location will also follow upon removal of items from our collection in the case of scenario two.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

9. Documented storage procedures

R9. The repository applies documented processes and procedures in managing archival storage of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Storage processes and procedures

The relevant storage processes are documented in our preservation policy (described in the document ‘Preserveringsbeleid’). The preservation policy is available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210422_Preserveringsbeleid_overgebrachte_digitale_archieven_Website.pdf. We use the OAIS framework as starting point for all applicable processes. In chapter 3 of the preservation policy we describe how we implemented these processes in our repository. This chapter covers an in depth description of all OAIS functions at a strategic level, from ingest to access. Chapter 4 of the preservation policy covers a description of the functions at a tactical and operational level. Specific measures for backup and recovery for archival storage are documented in chapter 7.

The OAIS framework is also the foundation of our digital preservation system. The online user manual (https://www.archivematica.org/en/docs/archivematica-1.12/#user-manual) describes how the different OAIS functions are implemented within the digital preservation system. The manual also includes a description of the way digital archives are processed and stored.

The relevant storage procedures are documented in ‘Procedures voor opnemen van digitaal archief in het e-depot’. In this

document we elaborate on the internal procedures for processing digital archives from start (deposit) to finish (access). This document is available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210621_Procedures_opnemen_digitaal_archief_e-depot_Website.pdf. A more compact English version of the procedures in this document is also available on our website: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220321_Procedure_models_for_the_transfer_of_digital_archives.pdf.

Storage locations

At this moment we use two different environments to run our digital preservation system: a test environment and a production environment. These environments are hosted by our commercial partner Picturae. The test environment is used to test new features and versions and to test representative subsets of digital archives in the pre-ingest stage. The production environment is only used for full ingests. Both environments have two separate storage locations for archival storage, one called “Regionaal Archief Nijmegen” and the other “Gemeente Nijmegen”. The locations are used to differentiate between various transfers. It is possible, if desirable, to add more environments or storage locations in the future.

Storage strategy

The primary system is located in the Global Switch Data Center in Amsterdam. A secondary system for backups is located at a different geographical location in Heerhugowaard, at the headquarters of Picturae. The data center in Amsterdam is connected to the data center in Heerhugowaard by encrypted TLS. All data in archival storage is replicated from the primary system to the secondary system. More details about the data centers can be found under R15 (Technical infrastructure).

The backup strategy consists of a combination of snapshots and traditional backups. Snapshots are point-in-time copies that can be used for rolling back to a previous state of the data. Snapshots are created 8 times a day and are kept for at least 24 hours. On top of the snapshots we create daily backups of all data, these backups are kept for 62 days. Backup and restore tests are performed regularly to ensure that all data can be fully restored in case of calamities.

Consistency checks

Consistency checks are performed in multiple ways: by the digital preservation system, by the file system and by an integrated application called Fixity (https://www.archivematica.org/en/docs/storage-service-0.17/#fixity). The digital preservation system uses the MD5 checksum algorithm to make sure all copies of the data are consistent during the ingest process. With each change in location the digital preservation system checks if the checksums generated at the start still match the newly generated checksums.

The file system, Zettabyte File System (ZFS), protects against data corruption. It is used in all environments. ZFS utilizes a mechanism of checksums, redundancy, and self-healing data to minimize the risk of data corruption. Data blocks are checked regularly by the file system. ZFS calculates a checksum and compares the checksum with the original stored

checksum. ZFS can self-heal if the checksum values do not match by using another copy of the same data.

We also make use of the Fixity application to ensure all data is consistent. The application calculates and compares checksums at the level of the Archival Information Packages. Currently the application runs periodically but it is possible to run it on demand. The latter option is a standard procedure after a calamity.

Deterioration of storage media

Deterioration of storage media is handled by constantly monitoring all hardware components and replacing them immediately in the case of component failure. All components are hot-swappable: components can be removed and installed without powering down the system. Checksum information is used to ensure that the data is unaltered and complete in the event of a disk replacement.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

10. Preservation plan

R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Documented approach to preservation

Our preservation policy is published on our website and has been sent to all depositors that designated Regionaal Archief Nijmegen (RAN) as repository for digital archives. The preservation policy (described in the document ‘Preserveringsbeleid’) is an extensive document that covers our approach to preservation (chapter 1), the preservation strategy we employ (chapter 2), our current preservation workflows (chapter 3), all preservation actions (chapter 4), metadata management (chapter 5), management of file formats (chapter 6) and the technical infrastructure (chapter 7). The link to the publicly made available preservation policy on our website is: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210422_Preserveringsbeleid_overgebrachte_digitale_archieven_Website.pdf. An extensive English summary of our preservation policy is included in the document ‘Overview of documentation’.

Preservation levels

Our preservation strategy is a combination of bit preservation and functional preservation (also called logical preservation). Bit preservation is the basic level of preservation for every submitted digital object. It includes multiple topics such as capturing integrity information, continuous integrity checks, security measures and backup and disaster recovery. Maintaining the original bitstream is our first priority, it is the foundational building block necessary for functional preservation.

Functional preservation is applied alongside bit preservation. This form of preservation is aimed at usability and accessibility through time. It starts with identifying and validating the file formats. This information is captured and saved in the digital preservation system and will be used to determine if other preservation actions are needed. We do not ingest files that can’t be identified.

A noteworthy functional preservation action is file format migration. This action can be employed when the original file format is in clear danger of becoming technically unprocessable and unreadable. In this case we will make an effort to migrate the original file format to another more durable format, a preservation format. The preservation file does not replace the original file; both files are kept.

Future file format migrations

Future file format migrations are only carried out when deemed absolutely necessary and always in consultation with the depositor. Our digital preservation system supports a re-ingest of Archival Information Packages stored in archival storage. The re-ingest functionality makes it possible to perform future file format migrations. We aim to minimize the need for future file format migrations by using a list of preferred and acceptable file formats (see attachment 1 of our preservation policy). At this moment we have no digital archives in our repository with file formats that are in danger of becoming obsolete. Thus, future file format migrations have not been scheduled yet.

Contract between depositor and repository

All legal responsibilities for repositories with regard to transferred government archives are described in the 1995 Public Records Act (Archiefwet) and further elaborated in local archive regulations and decrees regarding information management. A detailed description of the terms and conditions can be found in the Service Contract between depositor and repository (described in the document ‘Dienstverleningsovereenkomst Beheer Archieven’ or in the document 'Private Archives Deposit Agreement'). In the Service Contract it is made clear that the repository receives the rights to copy, transform and store the digital objects, as well as provide access to them, after a formal transfer.

Preservation actions

All actions that are relevant to preservation are specified in our preservation policy and in our procedures for the transfer of digital archives. An overview of all actions concerning digital objects is available in chapter 4 of our preservation policy, ranging from actions during the ingest and pre-ingest phases to actions within archival storage and data management. A short description of every action is included in this overview. Most actions are performed by the microservices in our digital preservation system. These actions are based on standards for submission information, archival information and dissemination information. These standards are described in chapter 3 & 4 of our preservation policy. To ensure that all relevant actions are taken we use a default processing configuration for all transfers. All actions that are performed within the digital preservation system are logged as PREMIS metadata and captured in a METS metadata file. All actions that are aimed at custody transfer are specified in our procedures for the transfer of digital archives. We use a checklist version of this document during the transfer to keep track of all actions.

Reviewer Entry

Reviewer 1

Comments:
https://regionaalarchiefnijmegen.nl/[…]/20210422_Preserveringsbeleid.pdf --> link to the preservation policy is not working for me

Reviewer 2

Comments:

11. Data quality

R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Quality of data and metadata

On a general level the quality requirements of data and metadata are described in the 1995 Public Records Act (https://wetten.overheid.nl/BWBR0007748/2013-01-01) and an extension called the Public Records Decree (https://wetten.overheid.nl/BWBR0027041/2014-01-01). There is also an English version available of the 1995 Public Records Act (https://www.nationaalarchief.nl/sites/default/files/field-file/Netherlands%20Public%20Records%20Act%201995.pdf). A digital archive is expected to be in good condition, properly arranged and accessible if all the requirements in these two official documents are met.

Article 17 of the Public Records Decree contains requirements regarding context and authenticity of (digital) objects and associated metadata:

a. The content, structure and appearance when it was received or created by the governmental organization 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 organization;
c. The relationship to other digital objects received and created by the governmental organization;
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 Public Records Decree prescribes requirements about metadata and the metadata schema:
1. The governmental organization uses a metadata schema as referred to in NEN-ISO 23081:2006.
2. The governmental organization records metadata linked to the digital objects from which the aspects referred to in article 17 can be traced at any time.

More requirements about technical metadata and digital signatures are described in Article 24. Articles 21 and 26 contain requirements about functionality, usability and file formats.

A more compact version of all these quality requirements can be found in our own requirements for digital archives

(described in the document ‘Overdrachtseisen digitaal archief’ and translated in the document ‘Transfer requirements for digital archives’). The requirements in this document are mostly derived from the quality requirements in the 1995 Public Records Act and the above articles of the Public Records Decree. In the case of an official transfer the depositor must make sure the data 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 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.
• Compression within files is only allowed if it does not result in loss of information.
• File names may not include certain special characters.
• File formats must be open or included on our list of preferred and acceptable file formats.
• All files must be linked to a metadata file and every metadata file must be linked to a file.
• The metadata must comply with the metadata standard TMLO (or another well documented metadata schema that is mapped to TMLO).

Both the Dutch and the English versions of the document ‘Overdrachtseisen digitaal archief’ are available on our website. For the Dutch version see: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210726_Overdrachtseisen_DigitaalArchief_RAN_Website.pdf. For the English version see: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220313_Transfer_requirements_for_digital_archives.pdf.

Quality control checks

We test the quality of data and metadata in multiple ways. In the pre-ingest stage we use an intake document (described in the document ‘Intakedocument voor opnemen van digitaal archief in het e-depot’) as a starting point for discussion. The intake document is basically a form that consists of multiple sets of questions for the purpose of gathering information about the quality of the data and metadata.

Both the Dutch and the English versions of the intake document are available on our website. For the Dutch version see: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20210621_Intakedocument_voor_opnemen_digitaal_archief_e-depot.pdf. For the English version see: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220317_Intake_document_for_digital_archives.pdf.

When the intake document does not show any signs of insufficient quality we proceed with different types of manual checks on samples of data and metadata. If the manual checks are successful we will perform a test ingest with a representative subset in the test environment of our digital preservation system. A microservice in this system called ‘Verify transfer compliance’ performs a set of quality control checks:

• Is the integrity of every file uncompromised?

• Is every file linked to a metadata file?
• Is every metadata file linked to a file?
• Is the metadata structured in the right way?
• Does the metadata conform to the metadata standard TMLO?
• Does the metadata conform to the technical standard ToPX?

Other automatic quality checks within the digital preservation system concern file compression, file names and file formats. A complete list of all the checks is available in chapter 4 of our preservation policy (described in the document ‘Preserveringsbeleid’).

If the test ingest is successful we will schedule a full ingest in our production environment. All above automatic quality checks will be performed again on all transferred data and metadata to ensure full compliance. If one of the checks fails the whole ingest will be aborted. In that case we will reject the transfer, analyze the failure reports and notify the depositor.

The types of data we manage do not have an impact on the quality control checks. Just as all our other workflows this workflow can handle all the different data types we accept. More information about the different data types can be found under R7 (Data integrity and authenticity) and R12 (Workflows).

User feedback

We provide all our archives with an adequate amount of descriptive metadata to make sure they are easily accessible. We implemented multiple widely-used standards (for example ISAD(G), ISAAR (CPF) and TMLO) to facilitate better access to our archives. When applicable we provide citations to related works in the ISAD(G) description, mainly at the level of archival descriptions . See for example: https://studiezaal.nijmegen.nl/detail.php?id=2318517115&tab=verwant. We perform surveys on a regular basis to monitor the designated community and to gather feedback about our online services, among which the quality of provided data and metadata. Users are also able to comment on data or metadata when exploring our online archives. They can leave comments on all levels (fonds, series, item); metadata on our website is constantly supplemented or improved through user feedback.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

12. Workflows

R12. Archiving takes place according to defined workflows from ingest to dissemination.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Workflow and process descriptions

We describe our workflows on a general level in chapter 3 of our preservation policy (described in the document ‘Preserveringsbeleid’). The workflows are based on the OAIS functional model and cover all six functional entities: ingest, archival storage, data management, preservation planning, access and administration. In addition to the six functional OAIS entities we use an extra entity, pre-ingest. In the pre-ingest stage we check various aspects of a digital archive to decide whether the digital archive meets our requirements. These requirements are described in the document ‘Overdrachtseisen digitaal archief’. An English translation is available in the document ‘Transfer requirements for digital archives’: https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220313_Transfer_requirements_for_digital_archives.pdf).

The workflow stages consist of multiple processes. We describe these processes in chapter 4 of our preservation policy and in our procedures for the transfer of digital archives. The procedures for the transfer of digital archives are described in the document ‘Procedures voor opnemen van digitaal archief in het e-depot’. The procedures described in this document are translated in English in the document ‘Procedure models for the transfer of digital archives’ (https://regionaalarchiefnijmegen.nl/images/over-ons/e-depot/20220321_Procedure_models_for_the_transfer_of_digital_archives.pdf).

Communication to depositors and users

Our preservation policy is published on our website and has been sent to all the depositors that designated Regionaal Archief Nijmegen (RAN) as repository for digital archives. Additionally we shared our procedures for the transfer of digital archives and the procedure models for the transfer of digital archives with the depositors. To guide the depositors in the

transfer of digital archives we also sent them our requirements for digital archives.

Security levels

Most digital archives are publicly accessible; this means that in principle everyone can consult them online. Digital archives or objects with access restrictions can only be consulted after obtaining special permission. If applicable, access restrictions are included in the metadata and processed by our collection management system. The presence of access restrictions in the metadata will determine whether or not the public will be able to view the digital archives or objects online.

In relation to security within the preservation system and collection management system: only administrators or employees with special rights based on their function are able to access restricted data. Work processes and actions concerning the ingest, storage, management, preservation and dissemination of digital objects are solely executed by administrators.

Types of data

Appraisal and selection of data are based on the 1995 Public Records Act (government archives), our acquisition plan (private archives) and our mission. The file formats and metadata must be in line with our requirements for digital archives. We do not accept digital archives that fail to meet the requirements. We offer practical advice and assistance to depositors on taking the necessary steps to meet the requirements. The types of data we currently manage do not have an impact on the workflows. At this moment the workflows can handle all the different data types we accept. Specific format policy rules are applied automatically in our preservation system after a file format has been identified.

Decision handling

Decision handling regarding data transformation within the workflows is covered in our procedures for the transfer of digital archives. On top of the automatic verifications we manually check the results and feedback of the microservices in the preservation system after a data transformation. Furthermore we manually check if the Dissemination Information Package has been correctly processed in our collection management system before we approve a transfer.

Change management

Important changes regarding the workflows will result in new versions of our preservation policy and procedures for the transfer of digital archives. These documents are registered, included and logged in a document management system (Corsa) that supports version control. Of course, new versions of these documents are shared with the depositors.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

13. Data discovery and identification

R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
accept

Reviewer 2

Comments:
3 – The repository is in the implementation phase
Accept

Response:

Search facilities

A successful ingest of a digital archive in our preservation system leads to the creation of a Dissemination Information Package. Every night, all new packages are automatically processed in our collection management system: new records will be created using the metadata and containing the (derivative) digital objects. Subsequently we can make the records available on our website.

Our collections are primarily discoverable through the website https://studiezaal.nijmegen.nl; metadata and objects of digital archives can be searched via “Archieven en Archiefstukken” and “Archievenoverzicht”. The user follows the same procedure for non-digital archives. We provide additional search utilities for special collections like visual materials (“Beeldbank”), building and environmental permits (“Vergunningen”), items of genealogical interest (“Personen en locaties”), newspapers (“Kranten”), address books (“Adresboeken”), film and sound items (“Film en geluid”) and publications (“Bibliotheek”). After conducting a search, results can be filtered and sorted in many ways. For example, it is possible to filter out digital (both digital born and digitized) items.

Parts of our collection are discoverable through (international) platforms like Europeana and Archives Portal Europe

among others.

Metadata standards

In the collection management system digital archives are described and structured using the following standards:

• ISAD(G): General International Standard Archival Description - We use this standard to structure metadata of the archival fonds.
• ISAAR (CPF): International Standard Archival Authority Record for Corporate Bodies, Persons and Families - We use this standard to structure metadata of the archival fonds creator(s).
• TMLO: Toepassingsprofiel Metadatering Lokale Overheden - We use this standard to structure metadata of series and items. In time TMLO will be replaced by its successor MDTO: Metagegevens Duurzaam Toegankelijke Overheidsinformatie.

Machine harvesting

Metadata and objects of various collections are machine harvestable using the Open Archives Initiative Protocol for Machine Harvesting (OAI-PMH), using various metadata standards. Our machine harvestable data sets can be found in the municipal open data portal (https://opendata.nijmegen.nl/datasets/query/%2A/filters/tag%3Aregionaal%20archief%20nijmegen/page/1) and in the open data portal of the national government (https://data.overheid.nl/community/organization/nijmegen_gemeente/dataset?sort=score%20desc%2C%20sys_modified%20desc&facet_keyword%5B0%5D=regionaal%20archief%20nijmegen). Metadata and objects belonging to digital archives are not yet available for machine harvesting. We will enable machine harvesting for digital archives in the near future.

Data citations

We offer automatically generated citation instructions (“Citeerinstructie”) on the web page of every archival fonds. See for example: https://studiezaal.nijmegen.nl/detail.php?id=2280568759&tab=aanwijzingen.

Persistent identifiers

All records and objects in our collection management system have persistent identifiers. To be more specific: we use handles registered under the Handle System, a service provided to us by SURFsara. Our machine harvestable data sets contain persistent identifiers for records and linked digital information objects. On our website we provide persistent identifiers for every record (button “Delen”), but not for linked objects. Examples of handles:

• Fonds: https://hdl.handle.net/21.12122/2126496598
• Series: https://hdl.handle.net/21.12122/2417936871
• Item: https://hdl.handle.net/21.12122/2417936875

• Object: https://hdl.handle.net/21.12122/2417936880

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

14. Data reuse

R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Provided metadata

When a user accesses a digital archive, descriptive and administrative metadata are provided at four levels:

• Archival fonds: All ISAD fields with content are displayed on the web page concerning the archival fonds. See for example: https://hdl.handle.net/21.12122/2126496598.

• Archival fonds creator: Some ISAAR fields with content are displayed on the web page concerning the archival fonds,

under the tab “Archiefvorming”. See for example: https://studiezaal.nijmegen.nl/detail.php?id=2126496598&tab=archiefvorming. All ISAAR fields with content are displayed on a web page in our knowledge base: https://www.huisvandenijmeegsegeschiedenis.nl/info/Bestuursdienst_Gemeente_Nijmegen.

• Series: We use a selection of TMLO fields to describe series and make them accessible. We use the following fields (translated): Identification mark, Name, Category, Description, Starting date, End date, Geographical area, External identification mark, Description of access restriction, Notes. Fields that contain content are displayed on the web page of the item. See for example: https://hdl.handle.net/21.12122/2417936871.

• Item: We use a selection of TMLO fields to describe items and make them accessible. We use the following fields (translated): Identification mark, Name, Starting date, End date, External identification mark, Description of usage rights, Documentary form, Notes. Fields that contain content are displayed on the web page of the item. See for example: https://hdl.handle.net/21.12122/2417936911.

In chapters 5.4, 5.5 and 5.6 of our preservation policy (described in the document ‘Preserveringsbeleid’) we document our usage of access metadata, in particular concerning series and items. More details about the metadata standards found under R13 (Data discovery and identification).

Understandability

First, we ensure understandability of the data over time by providing context information in the form of descriptive metadata and adhering to current metadata standards. Descriptions in our collection management system can be corrected or supplemented if needed. Secondly, we ensure understandability of the data over time by monitoring file formats, as explained below.

File formats

We use a list of preferred and acceptable file formats (see attachment 1 of our preservation policy). For the purpose of public access we strive to provide data in file formats that can be readily used by our users. When file formats of digital objects are not suited for public access, we make the items available in a derivative file format. The file format conversion takes place in our preservation system when ingesting or re-ingesting a digital archive. The file formats we use for public access are: gif, jp(e)g, jp2 and png (images), m4a and mp3 (audio), pdf (text), mov and mp4 (video). Digital objects with one of the above file formats are directly accessible within a viewer on our website. Should digital objects have a different file format, they are downloadable and have to be opened with external software. These choices are documented in chapter 6.3 of our preservation policy.

Evolution of file formats

With our preservation system we monitor the possible obsolescence of file formats in our repository. If deemed necessary

we are able to carry out file migrations using the same system. At this moment we have no digital archives in our repository with file formats that are in danger of becoming obsolete. Thus, future file format migrations have not been scheduled yet (see R10, paragraph “Future file format migrations”).

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

TECHNOLOGY

15. Technical infrastructure

R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Reference standards

We use the Open Archival Information System as a reference model for our digital repository (ISO 14721:2012;

https://www.iso.org/standard/57284.html). This standard was last reviewed and confirmed in 2018. Our digital preservation system uses the OAIS functions as building blocks for processing digital objects from ingest to access. The OAIS functions are also implemented in our workflows and procedures for the transfer of digital archives (see R12 for more information).

Our commercial partner Picturae is ISO 9001:2015 certified (https://www.iso.org/standard/62085.html). This is a standard that specifies requirements for quality management systems. Our commercial partner DEVENTit is also ISO 9001 certified. DEVENTit is ISO 27001 certified as well; see R16 for more information regarding standards for information security. The collection management system Atlantis of DEVENTit is NEN 2082 certified by the European Certification Bureau Nederland (ECB) (https://www.deventit.nl/nen2082). NEN 2082 is a national reference standard concerning information management.

Infrastructure development

The technical infrastructure is outsourced to our commercial partners; they are also responsible for developments in that area. Changes to the infrastructure are communicated to us as far in advance as possible. We use the test environments of our digital preservation system and our collection management system to test new setups. Updates to the core software of the digital preservation system and the collection management system are released at least once a year and accompanied by official release notes. We also test these updates on the test environments before enrolling them on our production environments.

Software inventory

The core software of our digital preservation system is Archivematica, which is released under GNU Affero General Public License (https://www.gnu.org/licenses/agpl-3.0.en.html). More in depth system documentation about Archivematica and all the integrated software is available on the official Archivematica website (https://www.archivematica.org/). The core software of our collection management system is Atlantis, a web-based solution for collection management and online publication. System documentation regarding Atlantis is available on the official website (https://www.atlantis-erfgoed.nl). We included a software inventory in our preservation policy (chapter 7: Technical infrastructure). The inventory is based on the software that is integrated in our core software: Archivematica and Atlantis. The integrated software is mostly community supported, free, open-source and released under the GNU General Public License (https://www.gnu.org/licenses/gpl-3.0.html). All software in the inventory supports the processing of digital objects from ingest to access.

Availability, bandwidth and connectivity

Our digital preservation system is hosted in a data center in Amsterdam that is directly connected to the national grid and is carrier and cloud neutral. They use the Tier III specification as basis for their technical infrastructure. Tier classification levels are used as an international standard for data center performance. The systems in the data center are designed to ensure robust resilience with ‘no-break’ IT power. They feature equipment protected by an uninterruptible power supply

(UPS) for power sags, outages, and spikes. The datacenter is covered by redundant capacity components (at least N+1). This means that the datacenter requires no shutdown when equipment needs maintenance or replacement. To sum up: the data center is able to offer reliable, high speed connectivity inside the Netherlands and around the globe. Therefore our host guarantees a 99,9% availability to the users.

Our collection management system is hosted in the NEP data center in Hilversum. They also use the Tier III specification as basis for their technical infrastructure. Availability, bandwidth and connectivity are guaranteed in the same way as above.

Disaster plan and continuity plan

The primary system in Amsterdam concerning our preservation management system is connected to a secondary system for backups in Heerhugowaard by encrypted TLS. All archived data is replicated from the primary system to the secondary system. The data centers are linked to each other by a double fiber optic connection. In theory the secondary system in Heerhugowaard can replace the primary system in case of an emergency but it is not an automatic failover. The data stored in the data center in Heerhugowaard can be used to restore the original data or to set up a new system but there are no recovery time guarantees.

The same applies to our collection management system, the primary system in Hilversum and the secondary system in Bunschoten.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

16. Security

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Data security

The security of the technical infrastructure is controlled by our commercial partners. Picturae controls the technical infrastructure of our digital preservation system and DEVENTit controls the infrastructure underlying our collection management system. Both Picturae and DEVENTit are ISO 27001:2013 certified (https://www.iso.org/standard/54534.html). ISO 27001 is a widely recognized security standard that confirms that the certified organization has an effective management system for information security. Our commercial partners conduct yearly surveillance audits for continuous certification purposes.

Security policies

Picturae has a very strict security policy that includes secure network connections (TLS), logical access control (strong passwords and periodic password changes), measures for physical access (authorized personnel only), screen locks and purpose specific access restrictions.

DEVENTit has also formulated a security policy. When working together with external parties or developing or acquiring information or communication systems, special attention is given to information security. DEVENTit uses a standardized classification schema (known internationally as the “CIA triad”) to determine the level of security for internal processes, information systems and data collections. Members of staff are continually trained and made aware in matters of information security. Only authorized staff members can make use the company’s information and communication systems. DEVENTit has adopted a sanction policy for occasions when laws, regulations or policy principles are breached by members of staff. They have taken measures to secure the physical security of the offices and measures to protect against malevolent software such as viruses, spam and spyware.

Risk management is for both of our commercial partners embedded in all aspects of the quality management system (systems, processes and functions). The identification, qualification and consideration of risks and responding adequately to those risks is an important part of the quality management system. Certification (ISO 9001:2015) provides confirmation that our commercial partners meet the requirements for quality management systems.

Authentication and authorization procedures

Access to our digital preservation system is regulated by the usage of named accounts, passwords and purpose specific

authorizations. Regular users do not have the authorization to delete data; they are only allowed to read or ingest data. The basic deletion function for stored Archival Information Packages is disabled for all regular users. The procedure for deletion of Archival Information Packages requires an official deletion request with a separate account in a different system. This request must be approved before an admin receives a deletion task (four eyes principle).

Access to our collection management system is also regulated by the usage of named accounts, passwords and purpose specific rights. We are currently in the process of implementing two-factor authentication. Some users of our collection management system only have read-only authorizations, some have mutation authorizations, some have deletion authorizations and most have a combination of these authorizations concerning different modules within the collection management system. Mutation and deletion authorizations are extended only to users when necessary for the fulfillment of their tasks. Currently, only the system administrator has the authorization to mutate and delete records within the module that contains our digital archives.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:

APPLICANT FEEDBACK

Comments/feedback

These Requirements are not seen as final, and we value your input to improve the CoreTrustSeal certification procedure. Any comments on the quality of the Requirements, their relevance to your organization, or any other contribution, will be considered as part of future iterations.

Response:

Reviewer Entry

Reviewer 1

Comments:
Thank you for the thorough application and the additional work put into creating English translations of the documentation as well as writing in detail the changes you made since the last version of the application. All that was really helpful in reassessing this application.
I would recommend accepting this application.

Reviewer 2

Comments:
The revisions addressed the previous concerns.