

memo

To: Leighton Christiansen
From: Michael L Nugent
CC: Courtney Mumma
Date: December 13, 2018
Re: CoreTrustSeal Documentation for the Texas Data Repository

Comments: I have attached the CoreTrustSeal documentation for the Texas Data Repository for review. If you have any questions or comments, please let me know.

Sincerely,

Michael Nugent

Background Information

R0. Please provide context for the repository

Type of Repository. Select all relevant types from list given:

- Institutional Repository

Brief Description of the Repository's Designated Community

The Texas Data Repository (TDR) is a service of the Texas Digital Library (TDL), a consortium of higher education institutions in Texas that builds capacity for preserving, managing, and providing access to unique digital collections of enduring value. The TDR is a platform for publishing and archiving datasets created by faculty, staff, and students at Texas higher education institutions. TDR is built in the open-source Dataverse platform, developed and used by Harvard University's Institute for Quantitative Social Science.

The Texas Digital Library was created in 2005 by four Texas members of the Association of Research Libraries: Texas A&M, Texas Tech, the University of Houston, and the University of Texas at Austin. Currently there are 22 member institutions in TDL.

The TDR encourages data deposit from all disciplines and can accept any type of data file. Non-proprietary formats are advisable in order to ensure both access and broader use and 'easier' preservation/migration.

<https://www.tdl.org/2017/01/announcing-official-launch-texas-data-repository/>

<http://data.tdl.org/>

<https://www.tdl.org/>

<https://dataverse.org/>

Level of Curation Performed: A – Content distributed as deposited

The TDR maintains no obligation to monitor the site, service, content, or user uploads and does not review all user uploads before they are made available on the site, or before being published. Administrators and users of a particular Dataverse are responsible for the contents of that Dataverse.

The TDR, and the data contained therein, is provided "as is" and "as available" and without warranty of any kind.

Versioning control is addressed in **R7**.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/295665665/Data+Usage+Agreement>

Outsource Partners:

Information about TDL's partners can be found here: <https://www.tdl.org/about-tdl/partners/>

1) The 22 member institutions: <https://www.tdl.org/members/>

2) TDL has joined the Chronopolis digital preservation network which includes the University of California, San Diego Library; the National Center for Atmospheric Research; and the University of Maryland Institute for Advanced Computer Studies.

This network has been certified by the Center for Research Libraries as a TRAC-certified repository.

<http://libraries.ucsd.edu/blogs/blog/texas-digital-library-joins-chronopolis/>

<https://libraries.ucsd.edu/chronopolis>

<https://www.crl.edu/archiving-preservation/digital-archives/certification-assessment>

<https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac>

3) The TDL is a charter member of the initial launch team for Digital Preservation Network (DPN) project.

<http://dpn.org/>

4) The Texas Advanced Computing Center provides a vital part of the TDL's preservation infrastructure and data storage for the TDL.

<http://www.tacc.utexas.edu/>

5) TDL members can use DuraCloud™ (a service of DuraSpace) for digital preservation.

<http://duraspace.org/>

<http://duracloud.org/>

6) The Public Knowledge Project provides open-source technologies for two of TDL's scholarly communications services.

<http://pkp.sfu.ca/>

Other Relevant Information

re3data.org profile: <https://www.re3data.org/repository/r3d100012385>

Organizational Infrastructure

I. Mission/Scope

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of our repository.

“The Texas Digital Library is a consortium of Texas higher education institutions that builds capacity for preserving, managing, and providing access to unique digital collections of endearing value. Our empowering technology infrastructure, services, and community programs: support research, teaching, and digital curation efforts at our member institutions; facilitate collaboration amongst our community and with external partners; connect local work to a global ecosystem of digital library efforts.”

TDL Mission Statement

<https://www.tdl.org/>

<https://www.tdl.org/about-tdl/>

<https://www.tdl.org/texas-data-repository/>

TDL Projects (digital preservation/data management)

<https://www.tdl.org/about-tdl/projects/>

Access to Data:

Part of the TDL’s vision in establishing a consortium Dataverse is to make research materials freely available to anyone, anywhere, and at any time. The TDL is an advocate for Open Access to scholarly work and the incentives to researchers for publishing and preserving their research data in the Texas Data Repository are:

- data that might be precariously stored on fragile, random, or unsustainable storage devices can be securely preserved for the long term.
- data that might otherwise become neglected over time can be preserved and made accessible for other interested researchers to use and cite, potentially providing wider visibility and impact for the research.
- many funding agencies and scholarly journals require data management plans that detail how the data will be managed, made accessible, and preserved.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

Preservation of Data:

The preservation objectives of the Texas Data Repository are:

- to collect, preserve, and disseminate the data sets and related information generated by researchers affiliated with any of the TDL's member institutions who choose to deposit their content therein.
- to enable researchers affiliated with any of the TDL's member institutions to comply with the mandates of funding agencies to manage, preserve, and share their research data.
- to provide the means for users to discover and access the data sets and metadata generated by academics affiliated with any of the TDL's member institutions over the long term.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

The TDL Administration published the official TDR launch announcement in January of 2017.

<https://www.tdl.org/2017/01/announcing-official-launch-texas-data-repository/>

Members of the consortium also published news releases about the TDR Launch. As an example, in a press release from the University of Texas Libraries, Lorraine Haricombe, the Vice Provost and Libraries Director for the University of Texas at Austin, said:

“The UT Libraries is committed to building the scholarly communications infrastructure needed to support access and innovation at UT. Through its complementary relationship with Texas ScholarWorks, the launch of the Texas Data Repository represents a giant step toward sharing the latest discoveries at the university with a worldwide audience of scientists and researchers for further exploration.”

<https://legacy.lib.utexas.edu/about/news/libraries-launches-texas-data-repository-support-campus-research>

And various TDR liaisons at the different participating institutions created promotional materials and information sheets to help introduce and advertise the TDR to their corresponding constituencies.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/723550233/Texas+Data+Repository+Promotional+Materials>

Organizational Infrastructure

II. Licenses

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of our repository.

The TDR uses the Creative Commons CC0 option as its default license. CC0 is 'No Rights Reserved'.

<https://creativecommons.org/share-your-work/public-domain/cc0/>

TDR users can enter own custom Terms of Use for datasets if CC0 is not feasible by crafting a custom data usage license agreement or using the TDR's restricted data usage license agreement.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/288063559/Licensing+and+Permissions>

To use the TDR service, researchers and users agree to follow the TDR's General Terms of Use; the Privacy Policy; and the Community Site Norms.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289112065/Privacy+Policy>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292094101/Community+Norms>

One specific aspect of TDR's policies dictates that user uploads must be void of all personal identifiable information (for example SSN#s). The TDL requires Texas Data Repository contributors to remove, replace, or redact identifying confidential or sensitive information from datasets prior to upload. There are exceptions to the rule.

Users also agree to grant to TDR all necessary permissions and required licenses to make the submitted or deposited content available for archiving, preservation and access within the site. This includes, without restriction, permission to:

1. re-disseminate copies of the content in a variety of distribution formats according to the standard terms of use of Texas Data Repository;
2. promote and advertise the content in any publicly (in any form) for Texas Data Repository;
3. describe, catalog, and document the user submissions;
4. store, translate, copy or re-format the content in any way to ensure its future preservation and accessibility, and improve usability and/or protect respondent confidentiality; and
5. incorporate metadata or documentation in the content into public access catalogues.

Users must review and agree to TDR's Terms of Use when logging into the system for the first time.

Please see R0 for level of curation, liability assumed by TDR, and the level of responsibility taken for the data.

With respect to noncompliance, the Terms of Use explicitly state that users are held responsible for any and all damages incurred if content is in violation:

“In contributing data to the site, you must ensure that the data complies with the terms of use. If your user upload does not comply with the terms of use, the Texas Data Repository has the right in its sole discretion to take down your User Upload. The Texas Data Repository does not review all user uploads before they are made available on the site, or before they are published. Therefore, you will be held legally and financially responsible for all damages if content you contribute violates anything in this agreement.”

TDR may terminate access to all or any part of the service at any time, with or without cause, with or without notice. Items within the TDR may be deaccessioned for the following reasons:

- copyright violation
- legal requirements and proven violations
- national security
- falsified research
- confidentiality concerns etc.

Organizational Infrastructure

III. Continuity of Access

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of our repository.

The TDR is hosted and maintained by the Texas Digital Library, a consortium of academic libraries in Texas with a proven history of providing shared technology services that support secure, reliable access to digital collections of research and scholarship.

TDR does have a Digital Preservation and Security policy:

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/287965267/Policies>

The TDL accepts the responsibility to preserve and provide access to research data, including associated metadata and documentation that is properly deposited in the TDR. This includes the provision of digital means to preserve and ensure ongoing access to said content for **a minimum of ten years after deposit**.

Beyond the ten-year retention period is subject to the TDL's selection criteria, appraisal of the content, and budgetary and technical support of resources necessary to meet this goal.

The Texas Digital Library began in 2005 as a partnership between four of the state's largest Association of Research Libraries (ARL) universities: Texas A&M University, Texas Tech University, the University of Houston, and the University of Texas at Austin. It has extended membership in the consortium to any of the state's institutions of higher learning and now represents large and small institutions from every region of the state.

In 2012, TDL presented an update to its strategic plan in which it outlined its future direction for the next 3 years.

<https://www.tdl.org/strategic-plan/introduction/>

In 2013, TDL revised its Bylaws describing the organizational structure.

<http://tdl.org/wp-content/uploads/downloads/2013/04/TDL-Bylaws-Revision-04-2013.pdf>

In addition, TDL has released its updated Strategic Plan 2015-2020.

<https://tdl.org/strategic-plan/>

The TDR was launched in 2017 as a new service for TDL's member institutions.

<https://www.tdl.org/2017/01/announcing-official-launch-texas-data-repository/>

And finally, in its 2017 Annual Report, the TDL highlights both its accomplishments and aspirations.

<https://www.tdl.org/2017/12/texas-digital-library-2017-annual-report/>

This timeline is presented as evidence that succession planning for the Texas Data Repository would be required only in the event of the TDL member consortium's dissolution or some other unforeseen calamity.

However, should such an event occur, continuity of access is addressed in both the Memorandum of Understanding template and the Service Level Agreement template, the documents signed by both TDL and the member institution with respect to the TDR. Once a member institution enters into a relationship with the TDL for the TDR service, both partners agree to: "recommend, in conjunction with [the other partner], data repository options should the Texas Data Repository be discontinued."

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/629014529/TDR+MOUs+and+SLAs>

And, the TDL ensures the accurate migration and/or transfer of data between storage spaces, servers, and systems wherever such may become necessary.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Finally, the TDR is hosted by Amazon Web Services (AWS). Using AWS virtually guarantees continuity of service.

<https://aws.amazon.com/compliance/data-center/controls/>

Organizational Infrastructure

IV. Confidentiality/Ethics

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of our repository.

The Texas Data Repository encourages data deposit from all disciplines and does request confirmation that data collection or creation was carried out in accordance with legal and ethical criteria as set forth by a member institutions.

Specifically, the Terms of Use states that “by posting user uploads to your Dataverse or other Dataverses, or by allowing other to do so, you make the following representations and warranties to the Texas Data Repository.” The representations and warranties that follow cover, among other concerns, copyright or other intellectual property rights; relevant, obligatory, and applicable approvals; and personal identifiable information (with exceptions).

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

As an example from a member institution, the University of Texas at Austin’s Office of Research Support and Compliance states that its mission “is to ensure that all research conducted on campus complies with all applicable laws, regulations, and University policies.” This office consists of four main areas: the Institutional Review Board; the Institutional Animal Care and Use Committee, the Institutional Biosafety Committee, and the Conflict of Interest section.

<https://research.utexas.edu/ors/>

Thus, each member institution has codes and guidelines for research conducted by its faculty, students and staff and the TDR’s terms of use explicitly state that depositors made certain guarantees.

There are procedures available to users that can be applied to manage data with discloser risk. First, user uploads must be void of all identifiable information (with exceptions). The TDR does not review data prior to upload so the onus to scrub personal identifiable information lies solely with the depositor.

Second, for other types of data with discloser risk, individual depositors can restrict access to files within a published dataset by describing terms of access for these restricted files. A depositor can also share unpublished datasets with both registered and non-registered TDR users, the latter by way of a private URL.

In these cases, the Dataverse administrators and users assume all liability should possible confidentiality or other privacy issues arise. The TDR assumes no liability.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>
<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/287965260/User+Guide>

If a user does not comply with the terms of use or the community norms, TDR reserves the right to take down the user upload and terminate access to any part of the TDR service.

Depositors, not TDR, are held legally and financially responsible for all damages if content contributed violates anything in the Terms-of-Use.

Users downloading datasets agree to abide by both the TDR's Community Norms and the applicable data usage license agreement attached to the dataset.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292094101/Community+Norms>

Organizational Infrastructure

V. 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.

Statement of Compliance:

4. This guideline has been fully implemented for the needs of the repository.

The Texas Data Repository is a service offered by the TDL. UT Austin services as the lead agency of the TDL and hosts the TDR.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/629014529/TDR+MOUs+and+SLAs>

Funding

The annual membership fees for member institutions in the TDL *and* the fees associated with the TDR can be found here: <https://www.tdl.org/members/membership/>

The relationships automatically renews until terminated by the member institution.

The TDL 2017 annual report has information about both revenues and expenses incurred by the TDL. Please note that the TDR was started in January 2017.

<https://www.tdl.org/2017/12/texas-digital-library-2017-annual-report/>

Staffing

The TDL has 7 FTE staff members, one of whom is directly associated with the TDR:

- Executive Director
- Senior Software Engineer
- Systems Administrator II
- Deputy Director (which includes TDR)
- Communication Strategist
- Senior DevOps Lead
- Administrative Assistant

<https://www.tdl.org/about-tdl/staff/directory/>

The TDL governing board is comprised of library deans and directors from seven TDL institutions: the four founding Association of Research Library members and three members selected at-large. Two non-voting members also sit on the board. Three members of this board act as the executive committee which is responsible for day-to-day operational decisions.

<https://www.tdl.org/governance/>

Member institutions have designated liaisons but those individuals are paid by their respective school, not the TDL. Each institution is responsible for appointing this liaison.

The TDR Steering Committee is the mechanism for local data repository liaisons at TDR member libraries to provide feedback to TDL and make decisions about TDR services. The committee consists of the TDL TDR Services Manager and all member institution appointed liaisons.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/628752385/TDR+Steering+Committee+Charter>

All current liaisons can be found here:

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/495681543/Help>

As each liaison serves as a bridge between the member institution and the TDL, a liaison can both draw on resources from both sides and provide knowledge and talent to both sides. This mutually reinforcing and mutually beneficial relationship greatly expands both the range and depth of expertise of the organization and its staff. This expansion speaks to part of TDL's mission statement: support[ing] "research, teaching, and digital curation efforts at our member institutions."

Training

The TDL provides training opportunities for all faculty/staff from its member institutions.

<https://www.tdl.org/training/>

The Service Level Agreements between an institution and the TDL mentions training possibilities for the liaisons:

- Maintain a tech support helpdesk for the data repository liaisons and for referring requests to them
- Provide training and professional development opportunities to data repository liaisons as needed

And each liaison should have opportunities for professional training/development through his/her own institution. Using UT Austin as an example again:

<http://sites.utexas.edu/oe/ut-staff-professional-development/>

Relevant Affiliations

All four of the founding members of the TDL are also members of the Association of Research Libraries. Please see **RO** for other affiliations and partnerships.

The TDL has also established several Groups for its staff and members. "As a consortium, the Texas Digital Library depends upon the active participation of its members and users to be successful. TDL Users Groups, Working Groups, Committees, and Affinity Groups provide opportunities for member contributions focused on particular services, professional roles, and projects."

<https://www.tdl.org/members/groups/>

Some of these groups extend beyond Texas (South Central States Fedora Users Group) while others do not require membership in the TDL to join (Texas Archivemata Users Group).

Organizational Infrastructure

VI. Expert Guidance

R6. The repository adopts mechanisms(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).

Statement of Compliance:

4. This guideline has been fully implemented for the needs of the repository.

As the TDL is a consortium of 22 current member academic institutions (with 11 institutions participating in TDR), this consortia relationship virtually guarantees that the TDR and its staff can secure ongoing expert guidance and feedback. The TDL can draw on the resources – informational, technical, and disciplinary – from each institution.

Both the TDL Governing Board and the TDR Steering Committee were mentioned previously in **R5**. The Board provides overall stewardship of the TDL and the Steering Committee is populated with data science experts. The member appointed liaisons on the Committee act as points of contact between the repository and its designated community.

In addition, the TDL Users Groups, Working Groups, Committees, and Affinity Groups were also mentioned in **R5**. The User Groups and Working Groups are populated by data science experts and can serve as conduits for communication with, and feedback from, the TDR’s designated community with respect to various projects.

The Member Resources, available through TDL, also provide “access to a number of resources and opportunities to engage with colleagues to facilitate and contribute to wider discussions toward the advancement of digital libraries and related services.”

<https://www.tdl.org/members/resources/>

Through its member institutions, the TDL/TDR can communicate with subject experts in myriad different disciplines and subject-specific librarians. Using the University of Texas at Austin as an example:

UT Experts by Subject: <https://experts.utexas.edu/subject>

UT Subject Librarians: <https://guides.lib.utexas.edu/prf.php>

The TDR is an instantiation of an open source application called Dataverse, originally developed and used by Harvard. Currently, there exist 33 Dataverse installations across the globe and the TDR represents one node in that wider network.

<https://dataverse.org/>

And recently, the Dataverse community formed the Global Dataverse Community Consortium which will “provide international organization to existing community efforts and will provide a collaborative venue for institutions to leverage economies of scale in support of Dataverse repositories around the world.”

<https://dataverse.org/global-dataverse-community-consortium>

The Texas Digital Library plans to be a member of the consortium.

<https://www.tdl.org/2018/06/texas-digital-library-advances-texas-research-to-global-stage/>

Finally, please revisit both **R0 and R5** for additional information about the TDR's connections to affiliates, partners, and networks of expertise.

Digital Object Management

VII. Data Integrity and Authenticity

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

“The TDL actively addresses the need to ensure the accuracy, integrity, authenticity, and permanence of the digital content that it manages, as well as the security of the services and platforms that it provides.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Data Integrity:

The Texas Data Repository provides basic, bit-level preservation through fixity checks and cyclic redundancy checks, both via Amazon S3 host service, and secure backup of deposited content. The TDL has an official backup strategy that requires all digital content to be stored in three distinct locations for all services including the Texas Data Repository. TDL will retain:

1. the copy of the data residing on the production server (currently an Amazon S3 volume),
2. nightly snapshots that can be used to restore the entire service to a particular date within the preceding month,
3. a copy of all data files, made nightly with versioning and kept for one year, stored on Amazon S3 (<https://aws.amazon.com/s3/>); these copies can be used to restore individual files, but not the entire service.

Checksums are generated upon ingest, e.g., MD5 for files. After download, users can generate their own checksum for comparison.

Completeness of the Data and Metadata:

With respect to the data, the TDR does not approve user uploads before they are posted. As such, the TDR does not warrant that the content or user uploads are timely, accurate, **complete**, reliable or correct in their posted forms.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

With respect to metadata, Dataverse requires nine metadata fields describing the dataset be completed before upload. Administrators of the various dataverses can require that additional fields be completed before dataset publication. The TDR User Guide provides instructions (Section 2.3 in the link below).

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243254/Creating+a+Dataverse>

Description and Details of Version Control Strategy:

When initially published, a dataset is automatically assigned to the category “Version 1.” Any subsequent changes to the dataset result in the creation of a new version. A ‘small’ change (correcting a typo) would create a “Version 1.1”. A ‘large’ change (adding a new data column) creates a “Version 2.0”. Adding a new file automatically creates a “Version 2.0”. All versions can be made public.

The TDR gives users the ability to follow the audit trails related to data changes. Users can read information about additions/edits and can also compare versions to identify particular differences (Section 4.3 in the link below).

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243260/Managing+Your+Data>

Usage of Appropriate International Standards and Conventions:

The TDR has created a Metadata Dictionary for users which includes citation and domain specific metadata fields.

<http://data.tdl.org/wp-content/uploads/2016/09/TDR-Metadata-Dictionary.pdf>

The TDR uses and/or recommends the following standards and conventions:

- [Dublin Core](#) (DC) and [Open Archives Initiative](#) (OAI)
- ISO 8601 for date entry
- [GeoNames](#) for geospatial metadata
- [Data Documentation Initiative](#) for social science/humanities metadata
- [SIMBAD](#) astronomical database and [FITS](#) for astronomy and astrophysics metadata
- [NCBI Taxonomy](#) & [NCBO Bioportal](#) for life sciences metadata
- [ISA-Tab](#) for biomedical

<http://guides.dataverse.org/en/latest/user/appendix.html>

Provenance:

Depositors must log-in to the TDR service through their respective TDL member institution. As an example, University of Texas at Austin affiliates must provide their UT-EID and password via Shibboleth internet protocols. If logging-in for the first time, depositors must agree to the General Terms of Use before being allowed to create an account.

Users are required to provide the TDR with accurate and complete registration information. Depositors' first and last names and affiliation are displayed connected to their uploads.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

Each dataset is assigned a persistent ID (doi) and the corresponding metadata is a part of the complete digital object.

The TDR also tracks/records information when a registered or non-registered guest downloads a file. “When you download a file from Texas Data Repository, our software collects user account data such as your name, username, email, institution and position if provided (or the session ID data for guest users) and accompanying download data such as the time of the download.”

Digital Object Management

VIII. Appraisal

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

Collection Policies

The TDR does not have a specific collection development policy with respect to data deposit and “encourages data deposit from all disciplines and can accept any type of data file.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079303/Frequently+Asked+Questions#FrequentlyAskedQuestions-FAQEight>

The TDR does have a policy with respect to long-term preservation. “Long-term preservation of Dataverse content, beyond the ten-year retention period, is subject to the TDL’s selection criteria, appraisal of the content, and budgetary and technical support of resources necessary to meet this goal.” The appraisal criteria are provided:

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

Completeness of Data/Metadata:

The TDR does not currently have quality control checks in place to ensure the completeness and understandability of data deposited. The Terms of Use, signed by all users, state that the TDR “has no obligation to monitor the site, service, content, or user uploads.” The TDR service is provided “as is” and “as available”. As such, the TDR does not warrant that “the content or user uploads are timely, accurate, complete, reliable or correct in their posted forms on the service” or that “any defects or errors will be corrected.” Use of the service is solely at the user’s risk.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

The TDR does have procedures in place with respect to metadata. At minimum, nine metadata fields must be completed before a dataset can be uploaded (Section 2.3 in the link below).

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243254/Creating+a+Dataverse>
Administrators of different sub-dataverses can require that additional metadata fields be completed.

The TDR will provide basic, bit-level preservation through fixity checks, cyclic redundancy checks (CRC), and secure backup of deposited content. The onus for providing metadata sufficient for long-term preservation, above and beyond the nine required fields, falls to the depositors and the administrators of the various sub-dataverses.

Non-Preferred/Preferred File Formats:

While the TDR does not publish a list of preferred formats, it does advise depositors to provide data in non-proprietary formats in order to ensure broader use for research, e.g. CSV or XML. Additional features and support for certain types of data files exist.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079303/Frequently+Asked+Questions#FrequentlyAskedQuestions-FAQNine>

But there are no quality control checks in place to ensure data producers adhere to preferred formats. Non-preferred formats undergo the same preservation and backup strategies as preferred formats.

Depositors grant all necessary permissions and required licenses to the TDR to make submitted or deposited content available for archiving, preservation and access, within the site. Among others this includes permission to “store, translate, copy or re-format the content in any way to ensure its future preservation and accessibility, and improve usability.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

Digital Object Management

IX. Documented Storage Procedures

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

User Documentation:

User documentation, processes, and procedures are available on the TDR's Atlassian wikispace:

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/overview>

This wikispace tracks changes over time so users can access and compare process and procedures as the TDR evolves.

In addition the Harvard Dataverse team maintains online its own set of user guides:

<http://guides.dataverse.org/en/latest/>

As Dataverse is open source software, its code is available on GitHub:

<https://github.com/IQSS/dataverse>

Security:

With respect to security, one must have a TDL/TDR Atlassian account to edit the TDR user documentation. Dataverse source code is open, thus anyone in the community can contribute. Access to TDL services can occur via two channels: a Shibboleth managed log-in or an SSH key log-in. The TDR is hosted by Amazon Web Services (AWS) and all Amazon employees who need access to data centers must be approved before gaining entry.

<https://tdl.org/wp-content/uploads/downloads/2015/04/Texas-Digital-Library-Data-Security-Policy.pdf>

<https://aws.amazon.com/compliance/data-center/controls/>

Data Storage:

Data sets (along with associated metadata and documentation) stored correctly in the TDR will be preserved for a minimum period of ten years. Storage beyond the ten years is subject to the TDL's selection criteria, appraisal of content, and budgetary/technical resources necessary to meet the goal. There is no charge to researchers for deposits, provided a total dataset is not larger than 10GB (although member institutions can consult with the TDR on a case-by-case basis for files and/or sets above the volume limits. And, as mentioned above, the TDR is hosted by Amazon Web Service.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079303/Frequently+Asked+Questions#FrequentlyAskedQuestions-FAQTwelve>

Backup Strategy/Data Recovery

The TDL has an official backup strategy in which TDL retains:

- the copy of the data residing on the production server, which is an Amazon S3 volume;
- nightly snapshots that can be used to restore the entire service to a particular date within the preceding month;
- and one snapshot from each month, retained for one year.

Snapshot backups are stored in Amazon Elastic Block Store (EBS) snapshots, which is replicated storage with regular systematic data integrity checks.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Risk Management:

The TDL actively addresses the need to ensure the accuracy, integrity, authenticity, and permanence of the digital content that it manages, as well as the security of the services and platforms that it provides.

The TDL ensures the security of its Dataverse instance as follows:

- System Security
- Data Integrity
- Regulatory and Legal Considerations

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Consistency across Archival Copies:

Checksums are generated for data files upon ingest (UNF for tabular data, MD5 for other files). Data sets are assigned persistent URLs and DOIs. Changes made to a data set create new versions. The doi is always attached to the most current published version.

Storage Media Monitoring:

Amazon Web Services is responsible for monitoring the status of the servers.

<https://aws.amazon.com/compliance/data-center/controls/>

Digital Object Management

X. Preservation Plan

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

The Texas Data Repository's preservation plan is outlined in its Digital Preservation and Security section of the TDR's policies. The Texas Digital Library "accepts the responsibility to preserve and provide access to research data, including associated metadata and documentation that is properly deposited in the Texas Data Repository. This responsibility includes the provision of digital means to preserve and ensure ongoing access to said content for a minimum of ten years after it is deposited in Dataverse."

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

Parts of the plan are also outlined in the Service Level Agreement (SLA) paperwork signed by a member institution and the TDL. This contract helps to delineate the different responsibilities of the member institution, its designated TDR liaison and the Texas Digital Library.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/629014529/TDR+MOUs+and+SLAs>

Texas Data Repository provides basic, bit-level preservation through fixity checks, cyclic redundancy checks, and secure backup of deposited content. Further and more in-depth digital preservation activities and services must be provided by a digital preservation program at the institution where the research data was originally generated. The aforementioned SLA describes backup "as copying the bitstream and storing that copy in a separate storage space.

The Terms of Use agreement required of an individual depositor provides for all the actions necessary for this bit-level preservation. By agreeing, users grant to TDR "all necessary permissions and required licenses to make the content [they] submit or deposit available for archiving, preservation and access, within the site."

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

The TDR's policies and documentation also cover Submission Information Packages/standards and Archival Information Packages/standards.

A SIP is the content and metadata received from an information producer by a preservation repository. As mentioned in an earlier requirement, the TDR requires a minimum of 9 metadata fields to be completed before a dataset can be uploaded. Different dataverse administrators can require additional fields.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243254/Creating+a+Dataverse>

An AIP is the set of content and metadata managed by a preservation repository, and organized in a way that allows the repository to perform preservation services. Upon ingest, the TDR uses the tool JHOVE to identify aspects of file formats. Provenance data is provided through the depositor and his/her affiliated

institution. Amazon Web Services performs both fixity and cyclic redundancy checks. Backup plans and access rights information are all documented.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

https://aws.amazon.com/s3/faqs/#Durability_.26_Data_Protection

Digital Object Management

XI. 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.

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

The TDR does not review datasets before the sets are uploaded and then subsequently published. As such, the TDR does not endorse, take responsibility for, or make any representations or warranties for any user uploads.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

With respect to metadata, the repository requires at least nine metadata fields be completed before a dataset can be uploaded. Some of these fields have pre-set formats and incorrect responses are rejected, e.g. dates must be entered according to ISO 8601 format. Dataverse and sub-dataverse administrators can require additional metadata fields be completed before datasets are allowed to be published. Administrators can also ask depositors to include a README.txt file if the dataset(s) requires special instructions, disclaimers, or definitions.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243254/Creating+a+Dataverse>

Outside of the aforementioned non-ISO date rejection, there is no automated assessment of metadata. Quality of metadata is the responsibility of depositors and administrators. The TDR metadata dictionary is available for reference.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/493551668/Metadata+Dictionary>

The repository's designated community can comment on and/or rate data and metadata through citing/using datasets. Datasets are assigned DOIs expressly for citation purposes. "Good" datasets will be cited more frequently as shown through different citations indices (Google Scholar, Web of Science, etc).

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289144946/About>

And members can always provide feedback on any aspect of the TDR to their institution's designated liaison.

XII. Workflow

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

Workflows/Process Descriptions:

The Texas Data Repository uses its Atlassian Confluence pages to communicate with depositors, users, and guests about its workflows and its handling of data.

For example, one can find, among others, the Service Level Agreement, Terms of Use, User Guide, Policies, and FAQs all in one location:

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/overview>

These confluence pages come with a page history functionality. It is possible for a user to track changes to workflows over time. And the Service Level Agreement states that the TDL will “provide timely reporting to data repository liaisons regarding any system issues.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/629014529/TDR+MOUs+and+SLAs>

Level of Security:

The TDR does not accept content that contains confidential or sensitive information, and requires that contributors remove, replace, or redact such information from datasets prior to upload.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079303/Frequently+Asked+Questions#FrequentlyAskedQuestions-FAQEight>

Exceptions to this rule are explicitly stated. See the “Restrictions” section in the Terms of Use

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

Depositors and administrators are authenticated via their respective institutions.

<https://tdl.org/wp-content/uploads/downloads/2015/04/Texas-Digital-Library-Data-Security-Policy.pdf>

The TDR is hosted by Amazon Web Services which is responsible for the security of the actual servers.

<https://aws.amazon.com/security/>

Ingest and Output of Data/Datasets:

The TDR does not appraise or select data upon ingest. Depositors from any discipline are encouraged to use the service. While all types of data and formats are accepted, the repository provides full support (i.e. data exploration, analysis, and meta-analysis via the TwoRavens suite of statistical tools) to tabular data.

The repository does make appraisal decisions with respect to long-term preservation (after the 10-year minimum period). The selection criteria are listed in the Digital Preservation Policy section.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

Checksums are generated for data upon ingest. After download, users can generate their own checksums and compare.

Digital Object Management

XIII. Data Discovery and Identification

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

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

The Texas Data Repository has a search box on the left side of the screen that searches within the dataverse. There is also an advanced search feature available that provides faceted metadata searching.

The TDR maintains on its Atlassian Confluence pages the “Texas Data Repository Metadata Dictionary” that contains citation and domain specific metadata fields.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/493551668/Metadata+Dictionary>

There also exists user guides created by the Harvard Dataverse team. These user guides are fully available and users can find more information about the citation and domain specific metadata fields supported by Dataverse.

<http://guides.dataverse.org/en/latest/user/index.html>

<http://guides.dataverse.org/en/latest/user/appendix.html>

Dataverse does support a protocol called OAI-PMH that facilitates machine metadata harvesting from one system to another.

<http://guides.dataverse.org/en/latest/admin/integrations.html?highlight=oai%20pmh>

According to the TDL Dataverse Implementation Working Group’s final report, TDR metadata may be aggregated by other systems using API applications or the OAI-PMH protocol. Permission from the TDL is not needed to harvest metadata into aggregated discovery or repository platforms unless aggregators intend to harvest on a permanent basis.

The Working Group’s report can be found here: <https://tdl-ir.tdl.org/handle/2249.1/76364>

Metadata from the TDR can be exported in Dublin Core, DDI, and JSON.

The repository is included in the re3data.org registry, a registry of research data repositories.

<https://www.re3data.org/repository/r3d100012385>

Finally, the TDR offers both DOIs and recommended data citations. As an example, listed below is the citation for a dataset currently hosted in the University of Texas’s dataverse:

- Dainer-Best, Justin, 2018, "Replication data and materials for Positive Imagery Training Increases Positive Self-Referent Cognition in Depression", [doi:10.18738/T8/RHEMGW](https://doi.org/10.18738/T8/RHEMGW), Texas Data Repository Dataverse, V3, UNF:6:FgY50+UEDA/95sPKids5WA==

Digital Object Management

XIV. 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.

Statement of Compliance:

4. The guideline has been fully implemented for the needs of the repository.

The Texas Data Repository requires a minimum of 9 metadata fields to be completed before a dataset can be uploaded and subsequently published. Those fields are:

1. Title
2. Name
3. Contact with email (not displayed to user)
4. Description
5. Date (must be expressed in ISO format: YYYY-MM-DD)
6. Subject (domain specific)
7. Production date (must be expressed in ISO format)
8. Production place
9. Kind of Data

Other fields can be required by administrators of the different dataverses.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289243254/Creating+a+Dataverse>

The repository maintains a metadata dictionary to help users with citation and content specific fields.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/493551668/Metadata+Dictionary>

According to the Dataverse User Guides hosted by Harvard, many metadata schemas are supported by Dataverse, including Dublin Core's DCMI. Harvard also provides a spreadsheet crosswalk for several schemas.

<http://guides.dataverse.org/en/4.9.1/user/appendix.html>

Data Formats:

Recall that the TDR is an institutional repository and the Designated Community is broad. The repository accepts datasets in a variety of formats. The onus for using a "correct" format lies with the particular researchers/depositors (assuming a "correct" format exists for members of a particular discipline). While virtually all formats are supported by the TDR, additional features/support are provided for only certain types of data. For example, the TwoRavens tool can be used to visualize CSV, Rdata, and dta files. Other software needed for opening and exploring the repository's content is the responsibility of the end user.

Future Migrations:

TDR policies and the Terms of Use agreement require depositors to grant to the repository all necessary permissions and required licenses to make the content [the depositor] submit[s] or deposit[s] available for archiving, preservation and access, within the site. This includes permission to "store, translate, copy

or re-format the content in any way to ensure its future preservation and accessibility, and improve usability and/or protect respondent confidentiality.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/289079299/Terms+of+Use>

The Service Level Agreement indicates that the Texas Digital Library shall “[b]e responsible for the stewardship, technological oversight, and upgrades of the data repository software infrastructure.”

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/629014529/TDR+MOUs+and+SLAs>

Thus, the repository ensures that any and all datasets properly uploaded will be migrated forward when the dataverse software/platform is updated.

Data ‘Understandability’:

The TDR is provided “as is” and “as available” and without warranty of any kind, express or implied. However, integrity of uploaded data is maintained by fixity checks, cyclic redundancy checks, secure backup, network monitoring and protection, and system updates.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/291635428/Digital+Preservation+Policy>

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Technology

XV. 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.

4. The guideline has been fully implemented for the needs of the repository.

Reference Standards:

Dataverse follows the guidance given in the OAIS reference model across the whole of the archival process. For example, the infrastructure supports separation between the Submission Information Package, Archival Information Package and Dissemination Information Package.

Dataverse is committed to using standard-compliant metadata to ensure that Dataverse metadata can be mapped easily to standard metadata schemas and be exported into JSON format (XML for tabular file metadata) for preservation and interoperability. See <https://dataverse.org/presentations/metadata-model-dataverse-project-helping-more-data-become-discoverable>. Detailed below are what metadata schemas are supported for Citation and Domain Specific Metadata in Dataverse:

- **Citation Metadata:** compliant with DDI Lite, DDI 2.5 Codebook, DataCite 3.1, and Dublin Core's DCMI Metadata Terms (see .tsv version). Language field uses ISO 639-1 controlled vocabulary.
- **Geospatial Metadata:** compliant with DDI Lite, DDI 2.5 Codebook, DataCite, and Dublin Core (see .tsv version). Country / Nation field uses ISO 3166-1 controlled vocabulary.
- **Social Science & Humanities Metadata:** compliant with DDI Lite, DDI 2.5 Codebook, and Dublin Core (see .tsv version).
- **Astronomy and Astrophysics Metadata :** These metadata elements can be mapped/exported to the International Virtual Observatory Alliance's (IVOA) VOResource Schema format and is based on Virtual Observatory (VO) Discovery and Provenance Metadata (see .tsv version).
- **Life Sciences Metadata:** based on ISA-Tab Specification, along with controlled vocabulary from subsets of the OBI Ontology and the NCBI Taxonomy for Organisms (see .tsv version).
- See also the Dataverse 4.0 Metadata Crosswalk: DDI, DataCite, DC, DCTerms, VO, ISA-Tab document.

In addition, Dataverse is an open source web application, an application that utilizes the following components:

- Java (dataverse is a Java Enterprise Edition (EE) web application)
- Glassfish
- PostgreSQL
- Solr
- SMTP server
- Persistent identifier service
- R, rApache, and TwoRavens
- Apache
- Shibboleth

- OAuth2
- Geoconnect

There are no significant deviations from the standards.

Infrastructure Development:

The Service Level Agreement (SLA) indicates that the TDL will be “responsible of the stewardship, technological oversight, and upgrades of the data repository software infrastructure.”

The TDL 2017 Annual Report lists a series of accomplishments and aspirations, including goals with respect to the repository.

https://www.tdl.org/wp-content/uploads/2017/10/TDL_AnnualReport_2017.pdf

In late 2018, TDR Dataverse data has been moved to S3. Plans for digital preservation storage may include copying data to the Chronopolis network in 2019-20.

Finally, TDL updates its Operating Systems (OS) quarterly at a minimum, and immediately when important security patches are made available.

Software Inventory/System Documentation:

The software requirements are listed above and in the Dataverse Installation instructions.

<http://guides.dataverse.org/en/4.9.4/installation/index.html>

Most (if not all) of the code is available on GitHub.

<https://github.com/TexasDigitalLibrary/dataverse>

Community Supported Software:

Dataverse is open-source and supported by a growing Global Dataverse Community Consortium (<http://dataversecommunity.global/>).

Different installation versions can be seen here: <https://github.com/IQSS/dataverse/releases>

Other relevant GitHub addresses: <https://github.com/IQSS/> and <https://github.com/IQSS/dataverse>

Connectivity:

The TDR is hosted by Amazon Web Services. As such, the bandwidth is (likely) sufficient to the TDR’s needs. TDL also adjusts it as needed and we are constantly monitoring usage via Munin.

Technology

XVI. Security

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

Statement of Compliance:

4. Implemented: The guideline has been fully implemented for the needs of the repository.

Backup Procedures:

The Texas Digital Library “actively addresses the need to ensure the accuracy, integrity, authenticity, and permanence of the digital content that it manages, as well as the security of the services and platforms that it provides.” The technical infrastructure including the operational servers are located in a secure data center, where only authorized employees have access to the equipment after identification.

The TDL systems and services are hosted with Amazon Web Service (AWS), which provides cloud security services and support (<https://aws.amazon.com/security/>) to include:

- Secure Network Architecture – segmentation and firewalls throughout;
- Secure Access Points – API endpoints allowing HTTPS access;
- Encryption – connections encrypted by SSL;
- Network Monitoring and Protection – against DDoS and MITM attacks, IP spoofing, etc.; and
- Identity Management and Authentication – secure log-in via password and SSH key pair.

Additionally, the TDL updates its Operating Systems (OS) quarterly at a minimum, and immediately when important security patches are made available.

The TDL has an official backup strategy in which the TDL retains:

- the copy of the data residing on the production server, which is an Amazon S3 volume;
- nightly snapshots that can be used to restore the entire service to a particular date within the preceding month;
- and one snapshot from each month, retained for one year.

<https://texasdigitallibrary.atlassian.net/wiki/spaces/TDRUD/pages/292159828/Information+Security>

Backups are stored in Amazon Elastic Block Store (EBS) snapshots, which is replicated storage with regular systematic data integrity checks.

The AWS cloud spans “55 availability zones.” Geographic distribution increases the chances that a major catastrophe will not lead to total system loss.

<https://aws.amazon.com/security/>

A white paper produced by Amazon in May of 2017, *Amazon Web Services: Overview of Security Processes*, discusses, among other topics, both physical and operational security processes as well as business continuity and disaster planning.

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

IT Security System, Disaster Plan, Business Continuity Plan:

As mentioned above, cloud hosting through Amazon Web Services provides coverage with respect to potential disasters. At the same time, the University of Texas System has an Office of Risk Management. This office's web presence has a section devoted to business continuity and emergency management. <https://www.utsystem.edu/offices/risk-management/emergency-management-and-business-continuity>

Finally, the University of Texas at Austin also has an Emergency Operations Plan. <https://preparedness.utexas.edu/sites/preparedness.utexas.edu/files/Emergency%20Operations%20Plan%202018.pdf>
<https://preparedness.utexas.edu/emergency-plans>