Texas Digital Library Data Security Policy

Texas Digital Library is a consortial effort of academic research libraries, cultural heritage institutions and university libraries to provide preservation and access to the scholarly output, research materials, unique collections and other digital items of value in the collections of participating members.

TDL Storage and Infrastructure

All systems and services of the Texas Digital Library are hosted with Amazon Web Service under a state-mandated arrangement via DLT Solutions.

Amazon Web Services provide the Texas Digital Library with infrastructure as well as support and security.

Detail regarding the agreement between Texas Digital Library and Amazon Web Service can be found at:

- the AWS User Agreement, Sections 3 and 4 (http://aws.amazon.com/agreement/)
- Information regarding Cloud Computing Services (http://aws.amazon.com/)
- AWS Identity and Access Management – IAM (http://aws.amazon.com/iam/)

Secure Log-Ins

TDL provides administrator and access to services requiring access via two channels

Shibboleth managed log-in – This option allows TDL hosted services to utilize unique usernames and passwords from institutional ID systems. Member universities must recognize usernames and passwords and then share attributes with TDL systems in order to enable access. (https://www.tdl.org/about-tdl/projects/shibboleth/) and (http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth/)

SSH Key Log-In – administrators and other users requiring access to services are issued a username and password utilizing SSH key pair protection.

Network Firewall

TDL utilizes AWS Security Groups to provide a Network Firewall for our systems. We allow open incoming network ports that are needed by the services in order to function.

Monitoring

TDL uses Nagios reporting to monitor serves and increase uptime. We attempt to identify and fix reported issues before customers have experienced a problem.

Managing Data for Security

TDL provides software which can provide both Open Access and dark (publicly inaccessible) storage of data. However, all users are required to set their own policies regarding the use of services and the use of dark storage versus Open Access options in order to best manage their data.

DSpace provides multiple roles and options. Vireo and DuraCloud are intended to behave as dark storage options with no public access. However, OJS, OCS and WordPress are open services and should expect public access to all materials.

Members with sensitive data will wish to review policies and procedures of their chosen software as they made a decision regarding hosting data they do not wish to make public. Members indemnify TDL against the release of data placed in unsecure locations within services or for not properly managing the settings within their choice of services.

Restricted Data and Protected Data

Member should contact Texas Digital Library and alert them to any items or collections placed into TDL Storage and Infrastructure that requires FERPA, HIPAA or other federal privacy requirements. TDL will provide members with a storage and management plan that will suit the needs of the item(s) or collection.