DIGITAL ANTIQUITY
tDAR The Digital Archaeological Record
A SERVICE OF DIGITAL ANTIQUITY
Box 87202 · Tempe Arizona · 87287-2402 · (480) 965-1369
info@digitalantiquity.org · http://www.digitalantiquity.org

Security and Confidentiality of Data in tDAR
May 2017
Center for Digital Antiquity Staff

Digital Antiquity's Focus on Data Security

The Center for Digital Antiquity (Digital Antiquity) strives to protect and preserve the archaeological and cultural heritage data and information that is deposited in tDAR. We focus on preserving, curating, and maintaining these data. We accept this responsibility as one of our primary missions. This document outlines the various approaches we take to store and secure digital information. We also describe tDAR features that allow data contributors to control and manage access to information that they place in the repository.

Physical Security

Digital Antiquity's offices are located in Hayden Library on the main campus of Arizona State University (ASU) in Tempe. Access to the offices during business hours is controlled by Digital Antiquity staff. The office area is locked when staff are not present. Computers within the offices are password protected. Access to the data is limited to designated Digital Antiquity data curation staff and management during their time of employment. Access is provided via a secure connection.

Technical Aspects to tDAR's Security

Digital Antiquity employs multiple strategies to the security of digital files stored in the repository. tDAR uses 256-bit TLS 1.1 encryption throughout the website and application to secure information. After a user registers and logs in to tDAR, all actions occur over a secure channel (e.g. uploading files, making purchases, viewing resources, etc.). The only actions non-registered users can perform are search and view basic metadata for resources and collections in tDAR, non-registered users cannot access data files.

Files are stored on servers at ASU's data center. A suite of tests is run every time Digital Antiquity makes any modification to tDAR's source code. In addition to the testing by Digital Antiquity technical staff for each release, ASU's data center and Digital Antiquity run audits using a suite of common intrusion testing tools to identify potential vulnerabilities.

Files stored in tDAR are protected by multiple, redundant security measures. Physical access to the data center where tDAR's files are stored is restricted and monitored. Data center staff do not have sign-on permissions to tDAR or the virtual machines that run it. In addition, a firewall has been constructed to prevent tDAR's database and backend file store from communicating with any host other than the tDAR webserver.

To protect files from catastrophic loss, Digital Antiquity maintains two backup procedures for tDAR's data. Both procedures employ strong encryption. One set of backups (updated biweekly) are kept in the Phoenix area in a secure storage area. The second set of backups are maintained in Virginia and utilize Amazon's Glacier storage service.

Security and Access Control for Confidential Files

Contributors to tDAR can control and limit access to files they place in the repository. The metadata about those files are always public, which means that anyone can learn about the existence of the resource. Public metadata in tDAR records, such as title and description, but not exact site location or files, are exposed to search engines (e.g., Google, Bing, etc.) for indexing. Digital files in tDAR can be marked as public, confidential, or embargoed. When a digital file is marked "public" anyone who is a registered tDAR user and logged in may download the file. A file marked "confidential" will be inaccessible to users who have not been explicitly granted access to that file by the individual who has this authority. Records in tDAR that have attached confidential or embargoed files provide a link that can be used to request access. Each request generates an email to the record owner. The record owner may decide to provide or not provide access to this request. Digital Antiquity facilitates communication between the record owner and the individual requesting access, but does not grant or deny such requests. Embargoed files are treated as confidential files for a user-designated period, after which the file becomes publicly accessible. Contributors may change the access designation at any time.

The metadata describing tDAR records allow contributors to designate UTM coordinates or specific site locations on a map. If these spatial designations are smaller than one square mile, the tDAR software will obfuscate the spatial data when displaying this information to users who have not logged in or have not been explicitly granted access. When obfuscated, spatial designations will be randomized and will display an area greater than one square mile.

Many clients choose to provide publicly appropriate redacted versions of digital files to upload to tDAR along with full confidential versions containing sensitive information. Digital Antiquity provides redaction services for clients who wish to take advantage of this option. Using professional redaction tools, data curators permanently remove confidential or sensitive information (e.g. archaeological site locations or other information as designated by the client) from a copy of the complete file. This service produces an edited version of the report that is appropriate for access by registered tDAR users.

For an outside evaluation of tDAR's security please review a 2014 report compiled by Sara Rivers Cofield, Curator of the Maryland Archaeological Conservation Laboratory (MAC Lab), who received a Department of Defense Legacy Grant to evaluate tDAR as a repository for digital portions of collections held at the MAC Lab for Defense agencies. Section 5.2 of the report (pp 54-56) addresses the questions related to data security using tDAR. The full report or a one-page fact sheet can be accessed at: http://core.tdar.org/document/393996/evaluating-a-cooperative-approach-to-the-management-of-digital-archaeological-records.