# Digital Preservation in a High Security Environment

## *Student Records, Encryption, and Preservation*

**Annalise Berdini**
*Princeton University, USA*
aberdini@princeton.edu
https://orcid.org/0000-0001-5385-7356

**Abstract - For the past five years, Princeton University Library – specifically the University Archives – has striven to create a robust digital preservation program for its born-digital and digitized records. Due to lack of time and available staff, the Library decided that a third party digital preservation service would be the best solution. It could be acquired relatively quickly, and it wouldn't require asking for funding to hire multiple dedicated staff to build a home-grown digital preservation system. Obtaining buy-in from stakeholders and finding a service that met Princeton's needs proved to be a challenge, especially due to the sensitivity of student records in the collections, which would require a high level of privacy and encryption key maintenance in addition to standard data integrity and preservation processing tools. Throughout 2018, Princeton worked to partner with a service previously unavailable due to University data sovereignty requirements – Arkivum's Perpetua – and work began to develop a Princeton-specific solution that met the needs of the University: Most importantly, geographically dispersed cloud storage locations, Princeton-based control over data integrity and authenticity checks, an encryption key management system for student records maintained by the vendor but managed by repository staff, and a reliable and quick exit strategy.**

**Keywords – Encryption, student records, privacy, security, preservation**

**Conference Topics – Exploring New Horizons; The Cutting Edge: Technical Infrastructure and Implementation**

Putting the case together for obtaining a digital preservation system was key to the success of the project. Outreach and advocacy for investment in digital preservation is challenging even for institutions where funding is available, and is dependent on more than whether or not the need can be proven and demonstrated. While Princeton is a well-funded institution, proving the case for digital preservation as a concept – and what that preservation system would look like – was still necessary. This process required archivists and IT staff to work together with the product vendor and a special campus-wide digital architecture and security review board, which reviews any digital product or service that pairs with University digital servers or content, and whose approval is required for new services and processing tools.

Student records and their requirements drove much of the preservation system review process and helped bolster the argument for a digital preservation program. Although the most recent push for a digital preservation program began in full force in 2018, Princeton University Library staff had been advocating for a digital preservation system for over five years. Princeton University Archives is responsible for the preservation and accessibility of Princeton student records, which may include anything from student organization records to student academic files and transcripts. Many of these records are mandated collecting materials, designated by the institution as essential to preservation of the history of the business of the University, and in the case of the academic or disciplinary files, are subject to strict confidentiality and security requirements -- some federally imposed. These restrictions are relatively easy to apply to analogue records, which may be physically secured in a pass-coded vault or



16th International Conference on Digital Preservation
iPRES 2019, Amsterdam, The Netherlands.

restricted area in the stacks, with little chance of an outside user finding and being able to gain access to large swaths of the records.

However, the challenges of maintaining that level of security for born-digital records are higher, as they include serious concerns about hacking or unintentional leaks of large quantities of data. Many archivists and repositories have reservations about data encryption, which effectively alters the original data so as to be unreadable. It is (usually) secure, but will it endanger the authenticity and integrity of the data? Who will have access to the keys, and how will they be managed for ever-increasing blocks of data? Working with Arkivum to find an acceptable solution to these questions while also meeting the security concerns of the institution was crucial to the acquisition of the service, and to the long-term preservation of Princeton's student records. The solutions Princeton found may be useful to other institutions searching for ways to protect their content while addressing long-term encrypted data preservation concerns. Additionally, the process of gaining buy-in at Princeton for digital preservation by pointing to some of its high-security records will inform other repositories of methods they can use at their own institutions, especially in the case of institutions that must also collect records requiring high levels of security.

This poster will discuss the process and strategies used to gain support from University administration for digital preservation of highly sensitive records, how to work with a vendor to develop a repository-specific solution for digital preservation, and the process of investigating and developing options for an encryption key management system that protects student records while maintaining preservation goals. It will be useful to other institutions and practitioners seeking buy-in for their own systems, whether in-house or third-party, and will address the question of long-term encryption key management. This poster will be relevant to practitioners interested in preservation of highly sensitive records, encryption and key management systems, and third party digital preservation systems like Arkivum.