



*New York State  
Archives*

## **Records Advisory: Using a Data Storage Vendor**

Issued 8/17/2009

### Outsourcing data storage

Cloud computing, virtualization, hosting, and data vaulting are a few of the current buzzwords applied to the management of electronic records systems and their data. Implicit in each of these concepts is the outsourcing of data storage to someone other than the owner of the data. As local governments and state agencies search for new ways to manage their information, they should be aware of the issues involved in handing over custody and control of data to a vendor or to some other government or agency (as a school district would to a BOCES, for example).

### Data storage and local governments

According to the Arts and Cultural Affairs Law, Section 57.31, "all local government records shall be kept in secure facilities maintained by the local government unless the consent of the commissioner of education is obtained to their transfer and storage elsewhere." The law applies to records in any format, including paper records, electronic records, and email, and they also apply to backups of electronic records, because backups are records. (Backups are listed in the State Archives' retention and disposition schedules for local governments.)

Further, according to 8NYCRR: Regulations of the Commissioner of Education (section 188.11c), local governments are legally required to store backup copies of archival electronic records in offsite facilities. These facilities may or may not be owned by the government, but they should ideally be far enough from the government's primary facility to ensure the accessibility of the records in the event of a regional disaster.

To be legally compliant, local governments must submit a formal letter concerning the storage of their electronic records in a facility that is not owned or maintained by the government to the **State Archives' Director of Government Records Services (9A47 Cultural Education Center, Albany, NY 12230)**, who will review the request to ensure the records will be safe and secure.

.....

## Data storage and state agencies

State agencies are required to transfer electronic records that have been scheduled as archival to the State Archives, and state agencies also have the option of storing backup copies of electronic records in the State Records Center.

In addition, according to 8NYCRR: Regulations of the Commissioner of Education (section 188.17), the State Archives, at the request of the Division of Budget, may review proposals by agencies to establish or lease facilities for records storage or to establish or lease facilities or "to contract for services to store inactive records, vital records, master copies of microforms, or backup copies of electronic records." The State Archives shall recommend approval of such requests when it proves more cost effective (or, in the case of data storage, more feasible) for a state agency to store its records with a commercial vendor or an entity other than the State Records Center, and when the chosen vendor or other entity will adequately provide for the protection and servicing of records.

## Contracts for data storage services

We require that local governments-and recommend that state agencies-have a contract to formalize the relationship between the government or agency and the organization that will be providing storage services. The contract should cover the following issues:

**Costs.** What will be the basis of the fees you pay to the vendor? The storage costs for electronic data are usually based on the storage capacity that a vendor makes available to a customer. The size of storage should be scaled to meet your long-term needs; you should not pay for storage that you will never use. In addition, the contract should list services other than storage that will incur additional fees. Such services may include litigation support, records retrieval, data migration, and data destruction.

**Disaster mitigation.** Will the vendor back up your data according to a schedule that you can stipulate? Are backups maintained at a third site, to ensure they are available if something affects the vendor's primary storage site?

**Ownership.** The contract should clearly state that you are still the legal owner of your records, regardless of where the records are stored physically. This means that the vendor has no right to "repurpose" the data, that is, to sell or otherwise transfer the records to a third party for commercial or other uses, and you should have the ability to regain full physical custody of the records if needed.

.....

**Records transfer.** How do you intend to transfer records to the vendor? If transfer will occur via removable media, you may want to implement measures for securing the records on the media (through encryption, for example). If transfer will be accomplished electronically, you will need to investigate whether you have the technological infrastructure to transmit records via a secure protocol or network.

**Accessibility.** What will be the conditions of access to the records, and who in your government will have access? Direct access to confidential records should be limited to staff who are clearly defined in the contract and be controlled by a system of passwords.

**Security.** What security measures will the vendor have in place to ensure against unauthorized access to your records? These measures should consist of a well-defined intrusion detection system that includes firewalls, virus protection, activity logs, audit trails, and encryption. The contract should also address the physical security of the vendor's facility, electronic systems, and trucks (if records are transferred physically on storage media). Stipulate in the contract the name of the contact person in your government or agency who should be notified if there is a security breach that involves your records.

**Storage.** In what formats will the vendor store your records? You may define in your contract the types of storage methods that are appropriate (and inappropriate) for your records. For example, you may prohibit the vendor from converting your records to proprietary formats that could limit future access to the records. You may similarly define the types of compression techniques that are acceptable (i.e., those that will not result in data loss) to apply to your records. For certain records, you may want the vendor to store exact, uncompressed copies.

**Retention and disposition.** How will you work with the vendor to ensure that records are destroyed after their legal retention periods have expired? Can you request a certificate that verifies records-especially confidential records-were completely and appropriately destroyed? Do not plan to store your records offsite indefinitely, allowing your storage volume to grow inexorably. Determine how you will identify records that are ready for destruction, define the role (if any) the vendor will have in destroying obsolete records, and identify acceptable methods of secure destruction.

**Termination of contract.** If there is a need, how will you terminate your contract? Make provisions for retrieving your records if the vendor goes out of business or is subsumed by another company.

As a final precaution, the State Archives advises that you check whatever references are available to you for the data storage vendor or vendors you are considering.

.....

In short, you should proceed on the premise that your electronic records are an irreplaceable asset to your government or agency. Be sure to write a contract that reflects your needs and your records' value to you and your constituents.