# Improving Electronic Records Programs in the SUNY System
# Technology Infrastructure Checklist

| College or University | | | |
|---|---|---|---|
| IT Contacts | | | |
| Records Management Contacts | | | |
| Person Completing Checklist | | | |
| Date of Completion | | | |

## 1. Funding

Indicate the total amounts spent annually on hardware purchases and maintenance, software purchase and licensing fees, consultants and contractors.   If additional budget items are relevant please include.

| **Total annual funding** | |
|---|---|
| **Annual funding by category** | |
| Software | |
| Hardware | |
| Vendors and contractors | |
| External consultants | |

## 2. Personnel

| **Number of IT staff employed by Campus IT (FTEs)** | |
|---|---|
| **Number of IT staff by category** (FTEs) | |
| Application development | |
| Computer operation | |
| Network administration | |
| Planning | |
| Security | |
| Support | |
| Training | |
| Other (Please explain) | |
| **Are outside vendors or consultants are used to manage IT systems? If yes, provide number of FTEs.** | |
| | |

| |
|---|
| **If yes, what functions are they responsible for?** |
| |

## 3. Planning

| |
|---|
| Does the IT department have an up-to-date strategic plan?  If no, is the IT department included in a broader strategic plan for the campus or as part of another department's plan? |
| |
| **Describe any substantial changes to IT resources (funding, staffing, hardware, software, etc.) expected in the near future** |
| |

## 4. Technical Environment

Describe the configuration of all multi-user application systems and enterprise software, such as financial, student information, human resources, and document management. Many of these systems will appear in the recordkeeping system inventory and information. Does the IT department expect any major changes to the hardware or software? For example, does your IT department plan to move from a Microsoft Windows Server operating system to a Novel NetWare based network or replace or add servers to the network.

**Multi-user systems**

| | |
|---|---|
| Application systems | |
| Business functions supported | |
| Operating systems and versions | |
| Makes and models of machines | |
| Age of hardware | |

| |
|---|
| **Network operating system** |
| |
| **Desktop operating systems and application suites supported by IT** |
| |
| **Anticipated hardware and software upgrades or migrations** |
| |

## 5. Storage

**Estimated overall network storage capacity in gigabytes.** Indicate how many gigabytes of shared storage are available on the campus network. Include storage dedicated to specific systems such as document management systems or database servers as well file server storage. Do not include storage dedicated to system backups.

**Estimated quantity of network storage in use in gigabytes**

**Estimated annual growth of digital files in gigabytes**

**Are storage systems centralized and managed by IT department?** Are the recordkeeping systems and hardware managed by the IT department or are departments responsible for managing their own systems? For example the accounting department may own and operate its own server for accounting software and data.

**If not, how are storage systems managed?**

**Media and configuration of storage systems** Indicate the type of media used to store electronic records on your network and how that media is accessed. Most likely your campus network will use arrays of disk drives. However it is possible that some systems will use other storage systems such as automated magnetic tape libraries, or CD/DVD jukeboxes.

**Physical locations of storage media.** Describe where your storage media are located. Are there dedicated server rooms for networked storage or special storage areas for magnetic or optical media?

**Environmental conditions of major storage locations** (Average temperature, relative humidity, and any known environmental threats)

## 6. Records Management

**Records management controls in place in digital information systems.** Describe any records management controls available in your electronic recordkeeping systems.  Do any of your systems employ automated records retention schedules, allow for automated destruction of records, or automate transfers to long-term storage.

**Are existing retention schedules consistently followed on campus?**

**Email system or systems** Does the campus use a single central email system or do departments or users control what systems they choose?

**Length of time email is retained before automated purging.** Does your campus automatically purge email after a certain period of time?  Does your system employ storage limits for email? Are the criteria set by the IT department or set by individual departments.

**Methods used to retain email**

**Website capture or preservation strategies employed.** Is the content of campus websites preserved?  How often is content captured and what software or procedures are used to capture the sites.   How are sites preserved?

**Does metadata generated by electronic recordkeeping systems conform to professional standards?** Do recordkeeping systems employ standardized metadata such as Dublin Core, Content Standard for Digital Geospatial Metadata, or Directory Interchange Format.  If the systems do not adhere to standardized formats do they use locally developed or proprietary metadata frameworks to manage their contents?

**Are recordkeeping systems able to export metadata?  In what format?**  Common export formats include text, comma separated values, and XML.

## 7. Backups

**Type of backups** Indicate what types of backups are used for each storage system (incremental, differential, full) and the backup software used to produce the backups.

**Frequency of backups** (daily, weekly, etc.)

**Backup media** (cloud, magnetic tape, DVDs, etc.)

**Location of backup media** (include all onsite and offsite copies)

## 8. Security

**Does the IT department have written security policies?**

**Describe any access controls (logical and physical) used to secure electronic records.** How is access to secure IT resources managed?  Are there any security procedures designed to physically protect IT resources (locked server rooms, fire suppression systems, electrical surge protections)?  Are any procedures in place limiting a user's access to certain systems or parts of the network?  How is unauthorized access to systems prevented?

**Does the IT department have a disaster plan or IT continuity plan that is widely distributed and regularly reviewed?**

## 9. Documentation

**Does the IT Department have written policies and procedures governing use of IT systems?**

**Does the IT department have user guides or manuals available?** If yes, indicate what systems.