

Systems Administration		
A. Architectural Flexibility		
1. The OPAC must be accessible from the web with no less functionality than from the terminal and/or dedicated client interface.		
2. If a union bibliographic record architecture is supported (or chosen), all ancillary files, i.e., holdings, circulation, acquisitions, check-in data, must be partitionable and accessible by institution and/or sub-unit.		
3. If a union bibliographic record architecture is not supported (or chosen), then a union view of all bibliographic, holdings, circulation status, serials receipts, and acquisition status data must be provided.		
4. Report generation requests and parameterization should be distributed to the functional units at each institution with full security.		
5. System management of functional parameters must be distributable when at the institution level or below.		
6. To the extent that client/server architecture is used, the delineation of client and server functions should be based on proven criteria which optimizes both the hardware/software and public/staff resources.		
7. The system should support all the levels of record structure necessary to provide for the major functional areas of library service: OPAC, acquisitions, authority control, cataloging, circulation, inventory control, and serials control.		
B. Interoperability		
1. TCP/IP		
2. Z39.50		
3. ISO ILL 10160		
4. MARC BIB in/out		
5. MARC AUTH in/out		
6. MARC HLDG in/out		
7. ALA Extended ASCII character set in/out		
8. X12/EDIFACT		
9. Relational underpinnings for non-bibliographic data		
10. Ability to load data from all current vendors.		
11. Ability to import/export data in physical media (e.g., tape, CDROM), via batch ftp and via single record		

transfer (tftp)			
12. Scripted access to non-Z39.50 sites (not just a telnet connection)			
13. An ADA-compliant method of OPAC access for sightless users, particularly remote users			
14. Multiple sessions in a windowed fashion including sessions on remote or disparate systems such as OCLC			
C. Modifiability			
1. Vendor must offer at least one of the following:			
a. source code			
b. code written in an object-oriented language with well documented object classes in a framework supporting multiple inheritance, with source code software escrowed.			
2. If a relational model is used for data storage, all schemas must be documented to support customer data mining.			
D. Manageability			
1. All functional and operational variables should be fully administrable requiring no more than two interactions to set any particular variable.			
2. The system must not require operating system administrator level privileges for day-to-day operation nor for functional administration; e.g., root level required at most for initial installation.			
3. The system must support a fully-functional test environment simultaneous to the production environment.			
4. All error messages and diagnostics should be meaningful and understandable.			
5. The system must have built-in diagnostic tools to test data integrity.			
6. The system must allow unattended, remote operations such as startup, performance monitoring, and shutdown.			
7. A fully-functional backup system should insure data recovery with no loss of content.			
8. Downtime recovery should not require terminal-by-terminal logon or resetting.			
9. Unexpected downtime should not cause any loss of data other than in transactions underway at the time of disruption.			
10. Batch activities such as report generation, file loads, and backups should be able to be scheduled at specified			

times.			
11. System control policies and parameters should be easily viewable and modifiable online by authorized staff without intervention of the vendor or system technical management personnel.			
E. Performance			
1. 7 days X 24 hours online operations			
2. Online response time for public and staff functions			
3. Efficient and quick batch data loading			
4. Indexing time should not affect response time in other areas			
5. Real-time indexing of all new and modified records			
6. No time restrictions on backups, updates, etc.			
7. Reliable uptime			
8. Handles peak loads			
9. No appreciable response time degradation during loads, backups, report generation and testing			
F. Scalability			
1. System must support:			
a. Current volume of:			
- file sizes			
- user population			
- transaction load			
b. Annual 10 percent growth in each of the above			
2. There should be no limit on concurrent use except as limited by hardware resources or as required by third party license agreement.			
3. There should be no limits on the number of records supported.			
4. There should be no limit on expansion of hardware (CPUs, disks, memory, etc.).			
G. Security			
1. The system should support custom profile for each staff member as needed.			
2. The system should support group profiles for staff not needing individual authorities.			

3. The system should support the ability to block public access to non-public services on both IP address and userid.			
4. The system should ensure that either multiple users are blocked from editing a given record or the system merges the two edits such that no work is lost.			
5. System should provide for levels of security for each major functional area:			
a. users cannot view or change any data;			
b. users can view data but cannot change it or perform any processing or reporting functions;			
c. users can view data, change records, and perform processing or reporting functions as allowed by his or her security profile.			
6. Within each major functional area, there should be specific processes and actions each with its own security.			
7. Security profiles should be accessible and manageable via an online module for authorized staff.			
8. The system should provide a "supervisor" authorization that allows use and control of all aspects of all the major functional areas of the system.			
9. The system should provide for a "system" level authorization for the system administration staff that allows use and control of all aspects of the system.			
10. The system should provide automatic lockout of individual authorizations upon a specified number of unsuccessful logon attempts.			
11. The system should require passwords to be changed at a specified interval and should allow users to change their passwords at any time or upon prompting.			
12. The system should provide a log of unsuccessful logon attempts with sufficient detail to aid in pinpointing the location of the attempt.			
13. The system should track and report regularly the use of overrides with sufficient information to identify the location and authorization in use.			
H. Remote Access			
1. All clients should be available via site license such that copies can be distributed, without limitations, to all members of the SUS community as appropriate.			
2. All client software should accommodate access via dial-in SLIP and PPP.			
3. Access should be restrictable based upon specified			

ranges of valid IP addresses:			
a. the system as a whole			
b. individual modules			
c. individual databases			
4. It should be possible to restrict access to certain data or functions by challenging users for a valid patron ID.			
5. Web access to public databases should not require separate databases or redundant data storage.			
I. Training and user documentation			
1. Vendor should provide machine-readable and customizable public and staff documentation.			
2. System should provide online help function for public and staff modules.			
3. System should provide online tutorials for public and staff.			
4. System should provide online documentation for client installation.			
5. Vendor should provide training support staff available by phone during working hours.			
6. Vendor should provide on-site training.			