As the resources of the Internet—electronic mail, discussion groups, and the World Wide Web—become an integral part of the process of scholarly communication, faculty and students increasingly want access to these resources from the locations where they do their work. And given the asynchronous nature of Internet communication, faculty and students want this access from home as well as from campus. In the summary of his 1995 campus computing survey, Kenneth C. Green noted that between 1994 and 1995, use of e-mail (to cite just the most common Internet utility) increased from 8 percent to 20 percent among faculty surveyed. In the past year, growth in professors’ use of the World Wide Web is likely to prove still more striking. Because computing services departments find it difficult enough simply to meet the needs for on-campus computing, the demand for remote access naturally leads a chief information officer (CIO) or a computing services director to consider three advantages of outsourcing remote access:

- **Improved service**
  Outsourcing can provide broader (and sometimes better) services than those currently available from on-campus systems, and it can permit extending those services to segments of the campus community (especially alumni) not served by existing systems.

- **Cost-sharing by clients**
  Computing services, like library services, are generally not charged back to the segments of the campus community that use them, so there is a limit to the number of new services that can be introduced. Outsourcing remote access establishes or extends the precedent of cost-sharing with the college or university community so that scarce institutional resources can be used for other priorities.

---


---

**Guidelines for Outsourcing Remote Access**

by Ardoth Hassler and Michael Neuman

As demand for Internet resources explodes on campus, faculty and students increasingly want network access from off-campus locations. Soaring demand has led numerous colleges and universities to investigate outsourcing. This article offers a discussion of the advantages and disadvantages of outsourcing remote access, including a sample checklist for an RFP, based on the examination of the RFPs for outsourcing remote access of six universities and a follow-up survey to determine their outcomes.

---

**Ardoth Hassler** (hasslera@guvax.georgetown.edu) is Executive Director of Academic Computing and Information Technology and CIO for the main campus at Georgetown University. She has served as chair of the CAUSE Nomination and Election Committee, is a member of the CAUSE Recognition Committee, and is serving as program chair for EDUCOM’97. She has made numerous presentations at CAUSE, Educom, ACUTA, Southern Directors, and other professional organization conferences.

**Michael Neuman** (neuman@guvax.georgetown.edu) is Director of the Research, Curriculum, and Development Group within Academic Computing Services at Georgetown University. In that capacity he helps faculty integrate computing into their research, teaching, and developmental projects. Currently Dr. Neuman is president of the Association for Computers and the Humanities, and he has recently published articles on developing electronic texts of standard critical editions, and maintaining humanities resources on the Internet.
Partnerships with vendors

While many institutions are simply seeking to add such basic services as PPP (Point-to-Point Protocol), TCP/IP (Transmission Control Protocol/Internet Protocol), and asynchronous access, contracts with vendors (commonly one to two years with the possibility of a one-year extension) may soon extend to an array of other protocols and information resources.

These advantages for outsourcing are compelling, but drawbacks become apparent when the remote access is viewed in relation to the current institution-based services and systems. This article draws upon experience at the authors’ university, Requests for Proposals (RFPs) for remote access obtained from five other universities, and a follow-up survey conducted by the authors to determine outcomes of those RFPs (see sidebar for details). The article describes the key technical and customer-support services that must be provided by the vendor, then describes ways to avoid the potential institutional problems of decreased control of systems and services, and concludes with a checklist of factors to consider when creating an RFP for remote access.

Outsourcing and Improved Service

Outsourcing, in conjunction with passing along the costs to the consumer, can expand services and extend them to a broader segment of the institution without significantly increasing charges incurred by computing services departments. Many such departments are under increasing pressure to extend service beyond the traditional client base to include alumni, patrons of the institution, and the community at large. Offering an array of network services to this extended community is good for public relations, but expanding the client base will inevitably impose peripheral demands on an infrastructure already overtaxed. Consequently, identifying in detail the vendor’s services—both technical and customer-support—will help to clarify both the extent to which outsourcing can extend campus services as well as the peripheral demands likely to be placed on the system.

Technical services

For what problems is the vendor’s service a solution? Circumventing a busy modem pool, extending Internet access to alumni, providing students with remote access to the Web, expanding access to the institution’s high-speed network—whatever the problems, the following five technical components of the vendor’s service are likely to require careful consideration, and information about them must be sought in the RFP for a remote-access vendor partnership.

Supported protocols

Should the vendor provide merely dial-up Internet access or should it supply access to campus servers as well? For the former, TCP/IP through SLIP (Serial Line Internet Protocol) and PPP are given; for the latter, other protocols such as IPX (Internet Packet Exchange) or AppleTalk may be necessary and will entail more serious considerations of security measures and policy issues. Once the Internet is available by remote access, members of the community are likely to want remote access to the resources of the institution’s high-speed network as well. Cur-

Five universities contributing RFPs to author Ardoth Hassler’s study were Florida Atlantic University, Florida State University, North Carolina State University, University of Alabama/Birmingham, and University System of Georgia. Georgetown University’s own “Memorandum of Understanding” was also used in the study. The RFPs were obtained through the electronic discussion list of the Southern Computer Center Directors. (This directors’ group, with participating institutions from Texas to Washington, D.C., has held an annual meeting each spring for more than twenty years.)

In October 1996, a follow-up survey to determine outcomes of RFP processes for outsourcing remote access was distributed to the Southern Directors’ discussion list and to the CAUSE CIO electronic discussion list. All five of the institutions that originally submitted RFPs completed the survey, with two indicating that they are still negotiating agreements with a provider. In addition, twelve other institutions that have chosen to outsource remote access responded to the survey: Brigham Young University, George Mason University, Georgia State University, Hamilton College, Lewis and Clark College, Pepperdine University, Rice University, University of Georgia, the University of Montana, University of Puget Sound, University of Tennessee/Chattanooga, and University of Tennessee/Martin.

Of the seventeen institutions responding, seven have contracted (and one is in process) with MCI, one has contracted with Sprint, one has contracted with IBM Advantis, one has contracted with BellSouth, and six use local providers. The average length of the agreement is two-plus years. Most institutions signed on for only one or two years; three signed on for five years. As this article goes to press, Georgetown University’s own service contract is in the process of being awarded.

Georgetown’s Memorandum of Understanding is accessible through the CAUSE Information Resources Library at http://www.cause.org/information-resources/ir-library/text/csl1099.txt; Florida Atlantic University’s RFP is available at http://www.fau.edu/irm/css/modem-rfp.html; and a copy of the author’s follow-up survey is available at http://www.georgetown.edu/acs/people/hassler/.

Winter 1996 15
rently, the majority of vendors are only able to support PPP. Only one institution responding to our survey reported a local provider offering IPX and Appletalk. Many indicated that supporting such protocols as IPX and Appletalk is under consideration.

- **Client software**
  Because the RFP should itemize the software that the vendor will supply, it is necessary to specify what the campus community will need in order to operate in a stable, familiar, and cost-effective environment. For stability, the vendor’s software must function on a full range of client operating systems, including DOS, Windows 3.11 or 95, and Mac OS. For familiarity, the vendor’s software should include common Internet utilities. For economy, the vendor’s pricing mechanisms should be noted carefully; for example, Netscape provides free licenses to its Navigator browser for the Web, so the RFP should seek to avoid charges for this utility. In our survey results, as specified by the institutions, the provider and/or institution are providing Trumpet Winsock (for Windows 3.1 clients), Netscape, Telnet, FTP, MAC dialer, terminal emulation (TN3270 and Telnet), and POP (Point of Presence) mailer client software.

- **Bandwidth**
  Access speeds/bandwidths determine the response time needed for downloading image files or large text files over the Internet, so the RFP should specify such standards as 28.8 kbps (or greater) and V.34 for dial-in ports. In the RFPs, as specified by the institutions, the provider and/or institution are providing Trumpet Winsock (for Windows 3.1 clients), Netscape, Telnet, FTP, MAC dialer, terminal emulation (TN3270 and Telnet), and POP (Point of Presence) mailer client software.

- **Absence of busy signals**
  The users’ tolerance for busy signals (as a percentage of calls to the vendor’s host computer) is generally known to the CIO or computing services director on the basis of previous complaints. The vendor of remote access, therefore, should be expected to match or exceed the current on-campus standards for minimizing busy signals. The RFPs generally specify the grade of service between P.00 (no busy signals) and P.05 (busy signals occurring on five percent of the calls). The majority of agreements examined in our study accepted P.05.

- **Scope of access**
  An increasing number of faculty members want remote access to the Internet not only from home but from a “home away from home,” when traveling for a conference or a vacation. Some vendors provide such “remote remote access” by means of an 800/888 phone number. The charges per minute should be negligible (either free or no more than $.10). Other vendors can provide local access numbers in all major cities, a service that can reduce the difficulties from dropped modem connections associated with cross-country dial-in on a toll-free (800) line. As would be expected, the larger, national vendors are better able to provide 800/888 access and/or local points of presence in major metropolitan areas. There is often an extra charge for this feature.

**Customer services**

The vendor’s success in providing customer services will be even more obvious to the campus community than its success with technical services. And the vendor’s success in easing the faculty, staff, and students past obstacles—especially in the following four areas—will reflect well on the computing services department for brokering the contract.

- **Rapid implementation**
  Once the contract is signed, the campus community will be eager to take advantage of the service; consequently, a minimal implementation period is recommended. In the RFPs examined, the institutions typically expected implementation within sixty to ninety days of signing the contract. By contrast, survey respondents reported that implementation ranged from two days to four months. Those institutions in major metropolitan areas obtained connectivity more quickly.

- **Installation and trouble-shooting**
  Easily installed software is essential. It is important to consider setting a requirement that the client software will “plug and play” for 90 percent of the users, and to determine if the vendor offers installation assistance at a fee. Good documentation is also essential in order to minimize the impact on the computing services help desk. Even so, the help desk must be prepared for questions about the vendor’s service and will need its own special access to the vendor’s support mechanisms.

- **Scope of support**
  The RFP should specify expectations for service from the vendor’s help desk. Is coverage required twenty-four hours a day, seven days a week, 365 days a year? What are the minimum requirements for access to the vendor’s customer
service organization for order processing, billing information, etc.? The RFPs in our study typically called for toll-free services extending Monday through Friday from 7:00 a.m. to 10:00 p.m., and Saturday and Sunday from 7:00 a.m. to 8:00 p.m.

✓ Pricing

Considerations here include start-up, usage time, and tiering. If there is a start-up fee, what services will it cover? Will the vendor incur a new start-up fee if he or she leaves home for the summer, or will the vendor permit a “stop out” fee that would keep the user’s account open but inactive? Will the vendor provide unlimited access? If not, what is an acceptable level of service? Typically, the study RFPs requested that “N” hours be included in the base rate with an hourly charge for anything over an N of about fifteen hours.

Can the vendor support tiering, that is, lower rates for off-peak usage? For example, usage might be unlimited between 1:00 a.m. and 6:00 a.m. or summer usage may be available at a lower rate. Most importantly, the cost of the remote access must be competitive. On the basis of the completed surveys, those institutions using local providers have typically been able to obtain flat fees for unlimited access. Those using a national provider typically have a base rate averaging around $12–13/month for sixty hours with a $.95/hour charge after that. Some have an option of a higher rate for unlimited use. One vendor offers unlimited use in off-peak hours, which vary from agreement to agreement. The majority have a $10–25 start-up fee.

Relationship to current institution-based services

Consideration of the scope of the vendor’s technical and customer services naturally raises the issue of the relationship of the outsourced services to the institution’s own. At one end of the outsourcing continuum, the vendor could be asked to provide all Internet services for the institution, though in the RFPs examined all preferred to maintain the relationships with their current providers of campus-to-Internet connections, while reserving the option to transfer to the dial-up vendor in the future. More frequently at issue is the question of modem pools, which many institutions maintain simply for access to their mainframes and minicomputers. Should these be dismantled in favor of support from the vendor? If so, restricted-use pools may be desirable to allow institution staff access to these systems in an emergency. These “backdoor” pools may present a security threat if not closely monitored, so a backdoor pool with specified maximum size should be included in the RFP to ensure that this resource does not appear to “compete” with the vendor’s resources. Only one of the institutions surveyed is not continuing to maintain a modem pool. The majority have no plans to stop maintaining their modem pools because they support different services from those provided by the vendors.

Electronic mail and personal Web space constitute another issue, since some vendors will offer to provide them on their servers as part of the base offering. Vendor-supplied electronic mailboxes may not integrate well if the college or university system is attempting to standardize on one on-campus system for all users. The RFP should specify whether or not these services are available to subscribers who are funded from the institution. On the other hand, if alumni or other “friends” of the institution pay their own way under this plan, it may be desirable to allow them to select electronic mail and Web pages as an option, particularly if the institution does not provide this service for them. All of the institutions surveyed continue to provide e-mail to their users; however, eleven institutions permit the vendors to offer additional e-mail services. In some cases, there is an added fee for this service.

Finally, it is important to determine whether “downstream” connections through the institution will be blocked from off campus. Institutions are sensitive to having people from off campus access the Internet through their connection. Further, it is important not to impact the institution’s bandwidth to the Internet. By requiring the vendor to provide direct Internet service to those who dial in, the institution can filter traffic at the router level to ensure that dial-in users cannot leave the campus backbone by way of the institution’s Internet connection. This would allow the institution to use a separate provider for Internet service for the campus backbone. However, vendors generally assign users an IP number from a block of their own. This may prevent off-campus users from accessing some online services, such as Encyclopedia Britannica, since they must be accessed from an IP number with the institution’s domain. As for campus users of the Internet, a “non-circuitous” routing should be specified, since institutions will not want their clients routed “across town” or across campus via distant nodes.

Because the vendor’s technical and customer services will have an impact on so many corresponding systems on campus, the institution ought to conduct a pre-test of the remote access. Prior to signing the contract, the institution should obtain five to ten demonstration accounts, encourage faculty and computing per-

“Only one of the institutions surveyed is not continuing to maintain a modem pool.”
sonnel to experiment with them for at least a month, and gauge the effect on the institution’s systems.

**Outsourcing and Decreased Control of Systems and Services**

In ways even more important than modem pools and mailboxes, outsourcing remote access must be carefully coordinated with the institution’s existing computing services and systems. At the most basic level, directors of academic computing frequently must balance the conflicting goods of responding to requests for new services while managing the limited resources of a complex system. The new services available by remote access, even though provided by a vendor and billed directly to the customer, nevertheless come at a cost of decreased control over systems and services, especially in such areas as security and management. In preparing their RFPs, CIOs and computing services directors can minimize the complications of decreased control.

**Security and authentication**

As faculty experience network access from home, their list of requested resources has grown beyond e-mail and discussion groups to include the World Wide Web and, more recently, the resources of the campus high-speed network. Protecting the institution’s Internet connection and the campus LAN infrastructure will become increasingly difficult as remote users press for more complete access to files and servers. Systems that had not been previously exposed outside the campus backbone, such as Novell file servers running IPX, may suddenly be open to attack if IPX is specified as a protocol requirement. These dial-in ports may need to be classed as on-campus resources in order for legitimate users to have complete access.

If alumni or other “friends” of the institution are permitted access to the modem pool, the vendor may be exposing the campus network and its resources to outsiders who would otherwise be considered unauthorized. Access to this pool should be restricted to faculty, staff, and students in order to reduce security risks. Consequently, the institution’s needs for security must be carefully spelled out in the RFP in four distinct areas.

- **Global network security**
  Teamwork with the vendor is essential. All of the RFPs in our study articulated general responsibilities for security, including working closely with one another, with the campus Internet provider, with the Computer Emergency Response Team (CERT), and with organizations such as College and University Information Security Professionals (CUISP).

- **Authentication**
  The conditions under which the vendor seeks authentication from legitimate users at remote sites must strike a balance between maintaining security of campus systems and avoiding inconvenience to the campus community. For example, while it is appropriate to permit only one session per username, it may be helpful to achieve consistency between the vendor’s policies and the institution’s on such matters as length of usernames and passwords so that the user need not learn two different sets of rules.

- **Audits**
  The vendor should be required to provide complete auditing of every user given access to the system. The institution may also require the vendor to accept requests for new accounts only from an on-campus service provider who can screen the applications. Or the vendor may need access to the student information system and lists of faculty and staff in order to validate requests to sign up for the service.

- **Non-disclosure**
  Because the vendor is likely to learn a great deal about the security systems that the institution has in place, the contract must contain a non-disclosure clause about security and privacy. The good news from the completed surveys in our study is that most respondents who have had sufficient time to evaluate security and procedures report that the vendor’s security provisions meet or exceed their expectations.

**Management and marketing**

Campus computing organizations are continually engaged in the effort to establish control over an array of constantly growing and changing systems; consequently, the decreased control of systems and services that accompanies outsourcing must be managed satisfactorily within the terms of the contract.

- **Location of equipment and maintenance**
  If the servers and other equipment necessary for remote access are located at the vendor’s site, the institution must determine (and express in the RFP) its tolerance for outages. If the equipment is to be located on campus, the vendor is likely to request conditioned space and utilities. The vendor may also expect the institution staff to monitor the equipment and swap “hot spares,” return-
Checklist for an RFP on Outsourcing Internet Access

Services from the Vendor’s Server

**SUPPORTED PROTOCOLS**
- __TCP/IP
- __SLIP, PPP
- __IPX
- __Appletalk
- __Others:

**CLIENT SOFTWARE PROVIDED**

<table>
<thead>
<tr>
<th>Software</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>__Trumpet Winsock</td>
<td>_____</td>
</tr>
<tr>
<td>__Netscape Navigator</td>
<td>_____</td>
</tr>
<tr>
<td>__TN3270</td>
<td>_____</td>
</tr>
<tr>
<td>__VTxxx emulation</td>
<td>_____</td>
</tr>
<tr>
<td>__MAC dialer</td>
<td>_____</td>
</tr>
<tr>
<td>__FTP</td>
<td>_____</td>
</tr>
<tr>
<td>__Telnet</td>
<td>_____</td>
</tr>
<tr>
<td>__Others:</td>
<td>_____</td>
</tr>
</tbody>
</table>

**SPEED/BANDWIDTH**

Specify the modem speed capable of being supported by the host:
- __28.8 Kbps
- __14.4 Kbps
- __9600 baud
- __V.34 protocols for dial-in ports

**BUSY SIGNALS**

Specify the grade of service desired (and cost):

<table>
<thead>
<tr>
<th>Response</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>__P.00 (no busy signals)</td>
<td>_____</td>
</tr>
<tr>
<td>__P.05 (busy signals on 5 percent of calls)</td>
<td>_____</td>
</tr>
<tr>
<td>__Other:</td>
<td>_____</td>
</tr>
</tbody>
</table>

**SCOPE OF ACCESS**

Specify the telephone charges required for the following connections:

<table>
<thead>
<tr>
<th>Point of Call</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>From institution city or town</td>
<td>_____</td>
</tr>
<tr>
<td>From surrounding metropolitan area</td>
<td>_____</td>
</tr>
<tr>
<td>U.S. connections from beyond current area code</td>
<td>_____</td>
</tr>
<tr>
<td>International connections</td>
<td>_____</td>
</tr>
</tbody>
</table>

**Vendor’s Customer Services**

**IMPLEMENTATION PERIOD FOR CONTRACT**
- __30 days
- __45 days
- __60 days
- __Other:

**GUARANTEED SUCCESS RATE FOR SOFTWARE INSTALLATION**
- __N.A.
- __75 percent
- __90 percent
- __Other:
VENDOR’S DOCUMENTATION
Content. Check all that apply:
- Software installation guide
- Trouble-shooting guide
- Vendor help-desk information
Availability. Check all that apply:
- from vendor by surface mail
- from institution
- via World Wide Web

VENDOR’S HELP-DESK COVERAGE
Hours per day Specified days per week Weeks per year

PRICING OPTIONS
Start-up: Specify any costs and conditions.
Stop out: Specify any costs and conditions.
Usage time and costs per month
Unlimited use:
Base costs: (number of hours) (incremental costs per hour)
Tiering options for off-peak use: Specify options and prices.

Institution Systems and Services

CURRENT SYSTEMS
Modem pool:
- Retain
- Discontinue
Electronic mail and Internet access:
- Retain
- Discontinue

SECURITY
- Collaboration with security professionals: Specify.
- Consistency with institution structures and policies:
  - simultaneous logins
  - passwords
  - other:
  - Auditing of access privileges and user transactions
  - Non-disclosure clause about institutional security and privacy procedures

MANAGEMENT
Location of vendor’s servers and maintenance
- on campus
- off campus
Reports requested of vendor:
Kinds Frequency Format
- Utilization reports
- Sign-up rates
- Time-of-day usage statistics
- Lists of complaints and resolutions
- Statistics on blocked calls
- Other:

MARKETING
Access to addresses:
- students
- faculty
- administrators
- staff
Permissions/safeguards regarding institutional logos and trademarks. Specify.
Billing mechanisms. Check all that apply:
- Direct billing to customers only
- Full and partial billing to institutional departments
ing the bad parts by mail for repair. If such “pair-of-hands” maintenance is considered acceptable, the institution should have exclusive use of the equipment and could expect a per-user rebate as well. In either case, it is necessary to specify how much notification must be given for maintenance and upgrades (typically, forty-eight hours). Given the likelihood that computing services staff will become engaged in on-campus support of the vendor’s equipment, it may be advisable to reject that option. Indeed, the majority of institutions responding to the survey report that the equipment is located off campus. Of the four institutions in our study who have the equipment located on campus, the vendor is performing monitoring and maintenance.

✔ Management reports

It is important to specify the types and frequency of reports required—including utilization reports, sign-up rates, time-of-day usage statistics, lists of complaints and their resolutions, and statistics on blocked calls—and to determine the frequency of the reports—either monthly or quarterly—and specify that they be delivered in machine-readable format as well as hard copy.

✔ Marketing

Even though the vendor will be providing services to the campus community and charging individuals directly, the institution must still have the final word on how, when, and where the remote access is marketed. Because faculty and students are likely to argue that Internet access has always been free on campus and should be free from off campus as well, a careful job of publicizing and “selling” the service will be necessary. Consequently, while information from the vendor can facilitate the process of education, it will be the task of the computing services department to muster the fiscal arguments for remote access in order to win the endorsement of relevant advisory committees and constituencies. For this purpose computing services will need data on the costs of maintaining and upgrading modem pools and of adding new SLIP/PPP services, and then will need to weigh these services against enhancing and upgrading modem pools and of Internet access. In addition, the RFP should attempt to ensure high standards of security and authentication, marketing and management, and use of the institution’s name and insignia.

“Because faculty and students are likely to argue that Internet access has always been free on campus and should be free from off campus as well, a careful job of publicizing and ‘selling’ the service will be necessary.”

Summary

Information Week reports that by 1997, corporate spending for remote access will average $8.5 million per company, up 81 percent from 1995. Hardware and software acquisition costs for remote access will be about 23 percent of the $8.5 million, meaning that about 77 percent of the costs will be for sustaining an installed base.3 While we have not found data specific to higher education, similar trends must be occurring in colleges and universities as the demand for remote access increases. For many institutions, outsourcing remote access is proving to be a viable option for providing service. Nevertheless, the institution’s request for proposals from vendors must carefully spell out the technical services to be provided and acceptable levels of performance, the customer services ranging from implementation to pricing, and the relationship of the new service to such current services as modem pools and Internet access. In addition, the RFP should attempt to ensure high standards of security and authentication, marketing and management, and use of the institution’s name and insignia.