

Library Public Access Workstation Authentication

SPEC KITS

Supporting Effective Library Management for Over Twenty Years

Committed to assisting research and academic libraries in the continuous improvement of management systems, OLMS has worked since 1970 to gather and disseminate the best practices for library needs. As part of its commitment, OLMS maintains an active publications program best known for its SPEC Kits. Through the OLMS Collaborative Research/Writing Program, librarians work with ARL staff to design SPEC surveys and write publications. Originally established as an information source for ARL member libraries, the SPEC series has grown to serve the needs of the library community worldwide.

What are SPEC Kits?

Published six times per year, SPEC Kits contain the most valuable, up-to-date information on the latest issues of concern to libraries and librarians today. They are the result of a systematic survey of ARL member libraries on a particular topic related to current practice in the field. Each SPEC Kit contains an executive summary of the survey results (previously printed as the SPEC Flyer); survey questions with tallies and selected comments; the best representative documents from survey participants, such as policies, procedures, handbooks, guidelines, websites, records, brochures, and statements; and a selected reading list—both in print and online sources—containing the most current literature available on the topic for further study.

Subscribe to SPEC Kits

Subscribers tell us that the information contained in SPEC Kits is valuable to a variety of users, both inside and outside the library. SPEC Kit purchasers use the documentation found in SPEC Kits as a point of departure for research and problem solving because they lend immediate authority to proposals and set standards for designing programs or writing procedure statements. SPEC Kits also function as an important reference tool for library administrators, staff, students, and professionals in allied disciplines who may not have access to this kind of information.

SPEC Kits can be ordered directly from the ARL Publications Distribution Center. To order, call (301) 362-8196, fax (301) 206-9789, email <pubs@arl.org>, or go to <<http://www.arl.org/pubscat/index.html>>.

Information on SPEC Kits and other OLMS products and services can be found on the ARL Web site at <<http://www.arl.org/olms/infosvcs.html>>. The Web site for the SPEC survey program is <<http://www.arl.org/spec/index.html>>. The executive summary or flyer for each kit after December 1993 can be accessed free of charge at the SPEC survey Web site.



SPEC Kit 277

Library Public Access Workstation Authentication

October 2003

Lori Driscoll

Associate University Librarian and Chair of Access Services
University of Florida



Series Editor: Lee Anne George

SPEC Kits are published by the

Association of Research Libraries
OFFICE OF LEADERSHIP AND MANAGEMENT SERVICES
21 Dupont Circle, NW, Suite 800
Washington, D.C. 20036-1118
(202) 296-2296 Fax (202) 872-0884
<<http://www.arl.org/olms/infosvcs.html>>
<pubs@arl.org>

ISSN 0160 3582

ISBN 1-59407-609-X

Copyright © 2003

This compilation is copyrighted by the Association of Research Libraries. ARL grants blanket permission to reproduce and distribute copies of this work for nonprofit, educational, or library purposes, provided that copies are distributed at or below cost and that ARL, the source, and copyright notice are included on each copy. This permission is in addition to rights of reproduction granted under Sections 107, 108, and other provisions of the U.S. Copyright Act.



The paper used in this publication meets the requirements of ANSI/NISO Z39.48-1992 (R1997) Permanence of Paper for Publications and Documents in Libraries and Archives.

SPEC Kit 277

Library Public Access Workstation Authentication

October 2003

SURVEY RESULTS

Executive Summary.....	11
Survey Questions and Responses.....	15
Responding Institutions	30

REPRESENTATIVE DOCUMENTS

Public Access Workstation Authentication Policies

Brown University	
Brown University Library Policy for Access to Computing and Network Services.....	34
University of California, Santa Barbara	
UCSB Libraries Public Access Computer Use Policy.....	36
University of Florida	
Privacy Policy & Use of Public Workstations	37
University of Hawaii at Manoa	
Library Public Computer Use Policy.....	38
University at Buffalo, SUNY	
Policy on University Libraries Public Access to Electronic Information Resources.....	40
Workstation Help	41
University of Texas at Austin	
UTOL Station Use Policy	42
Wayne State University	
Community Access Terminals.....	43
Yale University	
Policies Governing Use of and Access to Yale University Library Public Workstations.....	45

Library Computer Use Policies

University of Florida	
Use of Library Systems. Acceptable Use, Copyright.....	48

Computer Use Policy	49
Privacy Policy.....	51
Oklahoma State University	
OSU Library Internet Access	53
University of Pennsylvania	
Restrictions on the Use of "Penn Only" Networked Resources	55
Wayne State University	
Community Access Terminals (CATs) Use Policy	56
University of Western Ontario	
Western Libraries' Computer and Internet Acceptable Use Policy	58

Parent Institution Computer Use Policies

Arizona State University	
ASU's Privacy Statement	62
University of Florida	
University of Florida Office of Information Technology. Acceptable Use	65
McMaster University	
Request for Access to External Networks (including the Internet).....	69
University of Minnesota	
User Authentication for Access to University Computer Resources.....	72
Smithsonian Institution	
Smithsonian Directive 931. Use of Computers & Networks.....	78

Security Unit Descriptions

Brown University	
CIRT Charge/Mission	88
University of Chicago	
NSC: What We Do	89
University of Waterloo	
Statement on Security of UW Computing and Network Resources	91
University of Western Ontario	
What is the SUIIS Committee?	93

Security Incident Response Procedures

University of Oklahoma	
Computer Security Incident Report.....	96
Rutgers University	
Computing Incident Response Team.....	101

Wayne State University
Computer Support Team. Guidelines for Library Staff on Illegal Computer Activities 102

SELECTED RESOURCES

Books and Journal Articles..... 107
Web Sites 109



SURVEY RESULTS

EXECUTIVE SUMMARY

Introduction

In reaction to the events of September 11, 2001, as well as several widely reported misuses of campus computer networks, computer systems administrators have re-examined network access policies. While systems administrators have moved to restrict access to information assets, librarians have worked to support barrier-free access that protects users' privacy.

This survey was distributed to the 124 ARL member libraries in May 2003 to gather data on how users at public access workstations are authenticated; what is driving IT policy changes in libraries; who is involved in policy decision-making; how access controls have affected services; how, with tighter campus IT security, Federal Depository libraries are meeting the information needs of the public; and other questions. Sixty-seven libraries (54%) responded to the survey.

Authentication

The majority of respondents to this survey (67%) do not require user authentication at public access workstations in the library. Of those remaining, 11% require authentication at all terminals and 22% require it only at selected terminals. While some institutions implemented authentication on public access workstations more than ten years ago, the majority of respondents began requiring authentication as recently as 2001-2003. Ten percent of the respondents who do not currently authenticate

have plans to do so within the next year.

Libraries that authenticate are using various methods. Many respondents referred to campus Lightweight Directory Access Protocol (LDAP) servers. An LDAP server allows a network administrator to set permissions for access to a variety of applications and databases through a single list of authorized users and passwords. Most use some form of university-wide identifier. Non-affiliated users are either limited to workstations with minimal access or are assigned guest login accounts. One library that isn't authenticating admits to using signup sheets for Internet use; the patron provides a first name and the library staff enforces a half-hour time limit if someone else is waiting. The signup sheets are not retained. Most of the responding institutions are in the Federal Depository Library Program (91%), but this did not seem to affect authentication policy.

Institutional technology units, as well as state governments, have issued mandates for certain levels of IT security measures. One library acknowledged that

We are very aware that our "guest" public workstations are in a grey area, especially in the context of Internet service provider agreements that often require that all workstations/users be authenticated. However, as a library that also is accessible by our larger public community, we think it is important that any member of the public can use our online resources in the same manner

they have always been able to print materials, i.e., no requirement to have a library borrower card. We have been careful in determining the location of “guest” workstations and as all of our public workstations are “locked down” in various ways, they limit the manner in which they can be used. If inappropriate use incidents persist at a specific “guest” public workstation, we will change it [to] one that requires authentication.

Another federal institution’s library responded that the parent institution “has also begun a yearly mandate for all ... staff to take a security course.”

Generally, there were different services available to authenticated and non-authenticated users, primarily by limiting access to different workstations. As might be expected, non-authenticated users could access the OPAC, government documents, and stand-alone CDs, and often did not have access to circulation services, e-reserves, and specific software. Surprisingly, non-authenticated users often had access to the WWW, licensed electronic resources, ILL, e-mail, and chat reference. Comments indicated that access to licensed electronic resources is allowed only when the license agreements permit such use and that e-mail access is provided through Web-based accounts.

For institutions that managed access to public workstations, user privacy was handled either through anonymous access or identified access in which actual identities can be associated only with sessions. A few respondents indicated that pseudonymous access with or without demographic information was used. Half of the respondents indicated that users were informed of the authentication policy either electronically on the workstation or with signage on and near the computers. Users were also informed about the policies when they were assigned accounts. A few institutions posted the policy on their Web sites. However, seven institutions stated that users are not informed.

Authentication Logs

The majority of respondents (65%) indicated that authentication activity at public access workstations

was not logged because most respondents do not require authentication. Of the institutions that required workstation authentication, most kept logs of the user ID and workstation ID that corresponded to the date/time of logon/logoff. Some reviewed the logs and others did not. Review was prompted by a security incident for the few respondents that looked at the data.

The primary data analyzed include search patterns, system usage, workstation usage, and unauthorized login attempts. Most respondents do not maintain logs or were uncertain of the period of time that logs are maintained. Retention periods range from one week to indefinitely.

Public Workstation Access Policy

After examining the responses, it is clear that there are several different policy approaches taken toward network security and patron privacy in ARL libraries. Many policies were created by a representative group of administrators, information technology managers, and librarians. Some groups also included students. There were a variety of other representatives including the Acquisitions Department Chair and Director of Research Services.

Thirty-five percent (35%) of respondents received a mandate from the parent institution to authenticate at library public access workstations. Another 20% stated the driving factor behind authentication was a decision by library administration. However, a full 35% indicated other factors drove the decision to authenticate at public access workstations. In one case, the institution received the mandate from state government. Other institutions wanted to ensure access to resources by primary clientele and to prevent misuse. Still others listed software licenses and wireless access as reasons to begin authentication.

Security incidents in general are requiring more time and attention by campus and library staff. A full 95% stated that library IT staff were responsible for investigating suspected misuse of library public access workstations. Institutional IT staff, library administration, and campus police are also often involved. Most respondents report that additional staff and resources have been assigned to IT security

tasks during the past year. The USA PATRIOT Act and other post-9/11 developments, along with the growth of Internet use, contribute to this increased emphasis.

Conclusion

The intent of computer use policies and procedures is to protect against security incidents that originate from within the library computer network. Issues of privacy and security must be carefully balanced in the management of library networks. The best security procedures preserve the privacy of users and do not interfere with user access to library resources. The balancing act is becoming more difficult with software and database licenses that require user authentication.

ARL libraries are handling public workstation access to computer networks in a variety of ways. Although the majority of libraries do not currently authenticate users at all of their public workstations, most are reviewing security policies and procedures. IT policy changes in libraries are being driven by institutional initiatives, and more resources are being dedicated to controlling network access to prevent cyberattacks, identify theft, illegal file sharing, and other unauthorized uses. Policy decisions are a result of informal groups consisting of institutional IT units, library administrators, and library IT units. The results confirm that ARL libraries remain committed to providing information access to users with minimum disruption in services.

