

TECHNICAL REQUIREMENTS
FOR LICENSED RESOURCES

Revised 3/8/2011

CALIFORNIA DIGITAL LIBRARY
UNIVERSITY OF CALIFORNIA

1 Contents

1	CONTENTS	1
2	CDL CONTACT INFORMATION	1
3	OVERVIEW.....	2
4	ACCESS REQUIREMENTS	3
4.1	SYSTEM INTEGRITY	3
4.1.1	<i>High Availability Services.....</i>	<i>3</i>
4.1.2	<i>System Security Threat Resolution.....</i>	<i>3</i>
4.1.3	<i>Information Security.....</i>	<i>3</i>
4.1.4	<i>User Privacy</i>	<i>4</i>
4.1.5	<i>Usage Load.....</i>	<i>4</i>
4.2	SIMULTANEOUS USERS	5
4.3	AUTHORIZATION AND AUTHENTICATION	5
4.3.1	<i>Institutional Authentication</i>	<i>5</i>
4.3.2	<i>IP-based Authentication</i>	<i>5</i>
4.3.3	<i>Shibboleth.....</i>	<i>5</i>
4.3.4	<i>Remote Access.....</i>	<i>6</i>
4.4	ADDITIONAL TERMS AND CONDITIONS	7
4.4.1	<i>Click-through Licenses</i>	<i>7</i>
4.4.2	<i>Online Terms and Conditions.....</i>	<i>7</i>
4.5	PERPETUAL ACCESS AND PRESERVATION	7
4.5.1	<i>Perpetual Access</i>	<i>7</i>
4.5.2	<i>Preservation Responsibility</i>	<i>8</i>
4.6	DISCOVERABILITY	8
4.6.1	<i>Accommodation for Integrated Discovery: Federation and Aggregation.....</i>	<i>8</i>
4.6.2	<i>Vendor Records.....</i>	<i>9</i>
4.6.3	<i>Resource URL Verification</i>	<i>9</i>
4.6.4	<i>Inbound Linking to Full text Content.....</i>	<i>9</i>
4.7	OUTBOUND LINKING	10
4.7.1	<i>Metadata Requirements for OpenURL</i>	<i>10</i>
4.8	DOWNLOADING AND CITATION MANAGEMENT SOFTWARE.....	12
5	INTERFACE REQUIREMENTS	13
5.1	ADHERENCE TO PREVAILING STANDARDS	13
5.2	PLATFORM AND BROWSER SUPPORT	13
5.3	CLIENT SOFTWARE.....	13
5.4	MOBILE COMPUTING	13
5.5	SEARCH WIDGETS	14
5.6	AVAILABILITY OF CONTENT.....	14
5.7	OPEN ACCESS	15
5.8	USABILITY	15
5.8.1	<i>Consistency and Clarity</i>	<i>15</i>
5.8.2	<i>Context and Navigation</i>	<i>15</i>
5.8.3	<i>Search.....</i>	<i>16</i>
5.8.4	<i>“Learnability” and Flexibility.....</i>	<i>16</i>
5.9	INSTITUTIONAL CUSTOMIZABILITY	16
5.9.1	<i>OpenURL.....</i>	<i>16</i>
5.9.2	<i>Institutional Branding.....</i>	<i>17</i>
5.10	ONLINE HELP	17
5.11	COMPLIANCE WITH THE AMERICANS WITH DISABILITIES ACT (ADA).....	18

5.12	PERSONALIZED FUNCTIONALITY.....	19
5.12.1	<i>Interface Customization</i>	19
5.12.2	<i>Current Awareness</i>	19
5.12.3	<i>User Self-Registration</i>	20
5.13	STREAMING MEDIA.....	21
5.14	DIGITAL RIGHTS MANAGEMENT.....	21
5.14.1	<i>Watermarks</i>	21
5.14.2	<i>Restricted Functionality</i>	22
6	VENDOR COMMUNICATION AND SUPPORT	23
6.1	DOCUMENTATION TO BE PROVIDED TO CDL STAFF.....	23
6.1.1	<i>All Resources</i>	23
6.1.2	<i>Ejournals</i>	23
6.1.3	<i>Ebooks</i>	23
6.2	EXPECTATIONS FOR PROBLEM RESOLUTION.....	24
6.2.1	<i>Access Problems Reported to the Vendor by the CDL or UC Campus Staff</i>	24
6.2.2	<i>Use of Vendor Web Forms for Reporting Problems</i>	24
6.3	NOTIFICATIONS FROM VENDORS.....	24
6.3.1	<i>Downtime</i>	24
6.3.2	<i>Breach Resolution</i>	24
6.3.3	<i>Notification of Changes to the Resource</i>	25
6.4	ADMINISTRATIVE MODULE ACCOUNT.....	26
6.5	IP ADDRESS LIST UPDATES.....	26
6.6	USAGE STATISTICS.....	26
7	CONTENT	28
7.1	DATA INTEGRITY.....	28
7.2	COVERAGE.....	28
7.3	FREE TRIALS AND NON-SUBSCRIBED CONTENT.....	28
7.4	CURRENCY.....	28
7.5	COMPLETENESS.....	28
7.6	CORRECTIONS.....	29
7.7	BACKFILES.....	29
7.8	QUALITY OF CONTENT.....	29
7.9	RETRACTED/DISPUTED ITEMS.....	29

2 CDL Contact Information

CDL Helpline – 510.987.0555

CDL Support Team list email address – cdlsupport-l@ucop.edu

For questions about this document, contact cdlsupport-l@ucop.edu.

3 Overview

When selecting vendors for licensed electronic resources, the CDL aims not only to maintain existing standards for access and service, but also to improve, whenever possible, on existing arrangements. Moreover, by choosing our technologies and vendor relationships carefully now, we hope to lay the groundwork for future improvements. To that end, the following document sums up the major technical issues considered by the CDL during our decision-making process, and offers vendors insight into our preferred solutions, why they're important to the University of California, and what their implications are for prospective vendors.

Preferred vendors will provide the CDL opportunities for input on development priorities. The CDL sets a high standard for vendors that ultimately benefits all academic customers and leads to more competitive products for the publisher or vendor. The CDL is willing to work closely in the development and implementation of new features and functionality for existing products as well as co-development on new, cutting edge products that fit CDL's own strategic plans. These opportunities could take place via a users group, focus groups, working with the vendor's director of development, or discussions with the development planning team.

As part of the negotiation and evaluation process, a version of this document with explicit test cases (*Selection/Evaluation Criteria*) will be distributed to the vendor, along with similar documents regarding expected terms for licensing and requirements for cataloging, metadata and support. As part of this exchange, we expect that vendors will respond to these documents with information about how their product and platform does or does not adhere to these standards.

Where descriptions of licensing and other non-technical requirements are included in this document, they are provided in order to give context to the technologies needed to support these requirements and this document should not be considered a substitute for other requirements documents that may be included as part of a negotiation.

4 Access Requirements

4.1 SYSTEM INTEGRITY

4.1.1 High Availability Services

Delivery mechanisms must have high availability:

- Resources must be available on stable sites.
- Resources should be served by high-speed machines on networks with large bandwidths.
- Resources should be accessible 24 hours a day, 7 days a week, with 99% end-user availability outside of scheduled maintenance and 98% total availability including scheduled maintenance.
- Vendors should notify the CDL of any unexpected outages via email to the CDL Support Team list or by phoning the CDL Helpline as soon as possible after the outage occurs.
- Scheduled downtime should not occur during “prime time” hours for our users. Prime time for the University of California is 7am to midnight Monday through Friday, 8am to midnight on Saturday and 10am to midnight on Sunday. All times are in Pacific Standard/Daylight Time. All other times are referred to as “non-prime time.” UC holidays are considered non-prime time for the entire day.

REFERENCES

CDL Support Team list email address: cdlsupport-l@ucop.edu

CDL Support Team Helpline: (510) 987-0555

Sample vendor status page: <http://www.oclc.org/support/systemalerts/>

4.1.2 System Security Threat Resolution

Preferred vendors should provide assurance that they will work swiftly to resolve security threats when they arise. When the software requires access via third party software or plugins, the vendor should ensure prompt compatibility with the updated version of the supporting software. (For instance, as security threats are discovered in Adobe Reader and updates are provided, the resource should be made compatible with these updates in a timely manner.)

4.1.3 Information Security

The University of California maintains policies regarding the protection of electronic information, notably through *UC Business and Finance Bulletin IS-3 Electronic Information Security*. That policy includes clauses for “Third-party agreements” which shall “include satisfactory assurances that the contracting third party will appropriately safeguard information in accordance with federal and state laws and regulations and University policies.”

Safeguards are particularly important for what the University defines as restricted information (and elsewhere is often referred to as personally identifiable information). Restricted information is defined in *IS-3* as “any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security

protection, whether in storage or in transit." Further, Personally Identifiable Information (PII) is defined in the *CDL Privacy Policy* as "any information that can be directly or indirectly associated with a known individual." In a library context, "this information includes, but is not limited to, address and other registration information, informational questions asked, and searches, displays, and downloads of content."

Vendors are strongly discouraged from collecting restricted information as defined by UC, must inform the CDL if they do collect restricted information, must provide assurances that they safeguard any restricted information and/or personally identifiable information, and are requested to provide documentation about all of the personal information they do collect. Any personally-identifiable information that is collected must protect user privacy as described in section 4.1.4.

The CDL encourages vendors to create information security programs with elements parallel with and equal to *UC's IS-3 policy* and to provide a description of information security elements upon request.

REFERENCES

UCOP Business and Finance Bulletin: IS-3: Electronic Information Security:
<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>

CDL Privacy Policy: <http://www.cdlib.org/about/policies.html>

4.1.4 User Privacy

Confidentiality of individual users must be maintained. User data should not be reused, shared or sold to third parties without permission. Vendors should have a formal policy addressing user privacy that is readily discoverable on their website. At minimum, the vendor's policy should conform to the *ICOLC Privacy Guidelines for Electronic Resources Vendors*.

Elements that should be addressed in the vendor's privacy policy include:

- who collects user information and who has access to it
- what information is collected
- why the information is collected
- the duration for which the information is retained
- to what level the data can be correlated to individual user activity and for how long
- when the policy was last revised
- who is responsible for the privacy policy and how to contact the responsible party

REFERENCES

ICOLC Privacy Guidelines For Electronic Resource Vendors:
<http://www.library.yale.edu/consortia/2002privacyguidelines.html>

CDL Privacy Policy: <http://www.cdlib.org/about/policies.html>

4.1.5 Usage Load

Systems must be capable of handling typical UC usage. If possible, the CDL will provide average user statistics for a comparable resource.

4.2 SIMULTANEOUS USERS

The CDL prefers that there are no port limitations on our licensed electronic resources. However, systems that impose simultaneous user limits must provide a mechanism for the user to explicitly logoff from the resource and free the resource for other UC users. It is unacceptable for vendors to rely solely on a passive time-out action to free up restricted ports; however, automatic time-out functionality should be present to prevent a locked seat within a reasonable time period.

4.3 AUTHORIZATION AND AUTHENTICATION

Access controls should be designed to allow the UC's licensed user community to get to the resource from anywhere with a minimum of effort on the part of the University of California or that of the user, and with minimal disclosure of identity information.

4.3.1 Institutional Authentication

Users should not be presented with a personal login/password screen when access is controlled by other means, e.g., IP address or when trusted authentication has taken place and can be passed on in a trusted authentication federation such as InCommon via Shibboleth.

4.3.2 IP-based Authentication

IP addresses remain the most common means of user authorization at the University of California. Vendor systems should be able to accommodate IP-based access via campus proxy servers or VPN. Special requirements for access via campus proxy servers should be well documented.

The CDL will provide an initial list of IP addresses for the UC community, with quarterly updates. The list indicates which addresses represent proxy servers.

We require that vendors notify the CDL via the CDL Support team when the IP addresses list has been activated or updated so that we can begin testing to ensure that access is working. We do not announce a new resource to our user community until this testing is complete. Delays and problems in activation or updates will be taken into account when UC makes decisions on new products or renewals.

Because the IP-based access method is labor intensive, error prone, and often frustrating for our users, the University of California Libraries is actively investigating new solutions, particularly those that stress federated identity management and privacy protection such as Shibboleth.

REFERENCES

CDL Support Team list email address: cdlsupport-l@ucop.edu

4.3.3 Shibboleth

Recent trends in telecommuting, distance education, and the globalization of scholarship suggest that the university's need to accommodate remote users will grow exponentially in the coming years. The early adoption of Shibboleth may very well preempt large-scale access problems as the sophistication of user access needs grows. Going forward, the University of California libraries have adopted Shibboleth as the primary authentication standard for access to our research resources and services.

In addition to providing a better experience for our users through the user of a single username and password, Shibboleth simplifies secure authentication management and builds stronger partnerships between UC, its vendors and the wider academic community. Shibboleth allows currently valid users to access licensed electronic resources regardless of their physical location. At the same time, the protocol provides vendors with a more authoritative and up-to-date assurance that the user is a verified member of the UC community, which in turn makes it easier to identify and exclude users whose affiliation status has lapsed. Once it becomes ubiquitous, the use of Shibboleth is expected to prove a more cost-effective and efficient means of validating users' status, and will relieve both parties of the need to maintain extensive IP address tables.

The University of California Identity Management Federation (UCTrust), is currently working on issues related to systemwide implementation of Shibboleth. UTrust, in conjunction with the InCommon Library Shibboleth project, is investigating best practices for using Shibboleth to enable a seamless user experience when accessing library resources. Additional vendor implementation recommendations are being formulated by NISO's Establishing Suggested Practices Regarding Single Sign-On (ESPreSSO) working group.

Vendors are strongly urged to implement Shibboleth in order to enable a timely transition away from IP-authenticated access. The University of California campuses are members of the InCommon Federation and prefer to work with vendors that are also members of InCommon.

REFERENCES

Shibboleth: <http://shibboleth.internet2.edu/>

UCTrust: The University of California Identity Management Federation:
<http://www.ucop.edu/irc/itlc/uctrust/>

Library Shibboleth Project: <https://spaces.internet2.edu/display/inclibrary/InC-Library>

InCommon Federation: <http://www.incommonfederation.org/>

NISO ESPReSSO Working Group: <http://www.niso.org/workrooms/sso>

The UK Access Management Foundation (JISC): <http://www.ukfederation.org.uk/>

4.3.4 Remote Access

Vendor systems should be able to accommodate IP-access authentication via campus proxy servers or VPN client software. Special requirements for access via campus proxy servers and other supported remote authentication methods should be well documented by the vendor.

REFERENCES

Off-Campus Access FAQ:
http://www.cdlib.org/services/info_services/guides/off_campus_access.html

4.3.4.1 REWRITE PROXIES

EZProxy and WebVPN are two examples of rewrite proxies. Rewrite proxies have gained a substantial following as a way to provide off-campus access to licensed electronic resources without requiring the user to install client software or make configuration changes. This makes rewrite proxies ideal for use in environments where the user has no authority to make configuration changes to the machine, and also reduces the likelihood of user errors made during configuration.

Rewrite proxies route activity through the proxy server by appending or prepending additional information to the default URL. For most resources, this works well; however, resources that are heavily reliant on scripted functionality, contain a large number of separate objects per page, or require installation of client software on the user's machine will have problems when used through a rewrite proxy, as the rewrite process also affects all individual elements on the page.

At the University of California in 2011, 7 of the 10 UC campuses use some form of rewrite proxy as a remote authorization mechanism, and one campus uses it as their sole method for providing access to off-campus users. This primary access, along with the central use of link resolver software to move between different resources necessitates that ensuring licensed resource functionality within this configuration is essential.

At a minimum, vendors should test their products to ensure compatibility with the EZProxy software and with Cisco and Juniper WebVPN.

REFERENCES

EZProxy: <http://www.oclc.org/ezproxy/>

OCLC overview of rewrite proxies:

<http://www.oclc.org/support/documentation/ezproxy/rewrite.htm>

InCommon Library Best Practices:

http://www.incommon.org/library/docs/Best_Practices.pdf

4.4 ADDITIONAL TERMS AND CONDITIONS

4.4.1 Click-through Licenses

Click-through agreements are not allowed. The publisher/vendor will not require authorized users to enter into a potentially binding agreement with the publisher (e.g., a "click-through" license) independent of the institutional agreement with the University as a condition of use of its product.

4.4.2 Online Terms and Conditions

Where the online terms and conditions differ from the signed license, the signed license shall prevail.

4.5 PERPETUAL ACCESS AND PRESERVATION

4.5.1 Perpetual Access

Vendors should provide perpetual online access to licensed electronic content, meaning that UC has use of the materials to which it previously subscribed, in a manner that allows authorized users to continued access to that data in the event the subscription is cancelled. The vendor should be able to tailor access rights to purchased materials by IP address or other preferred authentication mechanisms, as well as by title, and year. Electronic works should have a permanent identifier for citation and linking purposes.

As an alternative to vendor-hosted perpetual access, a vendor can partner with a trusted digital preservation repository. Portico is the University of California's preferred archival partner. The CDL Standard License Agreement delineates UC's need for the right to obtain archival copies on request for local storage and hosting at UC's discretion.

REFERENCES

Portico: <http://www.portico.org>

CDL Standard License Agreement / California Digital Library Licensing Toolkit:
<http://www.cdlib.org/services/collections/toolkit/>

4.5.2 Preservation Responsibility

Preservation is not the same as perpetual access. For preservation, the content should be archived in a secure manner so that it remains usable and faithful to the creators' original intention and permanently available. It should not be isolated in an obsolete format. Vendors should implement a trusted digital preservation repository to safeguard the long-term integrity of the content. The preservation repository should comply with the emerging standards for digital preservation such as the *Open Archival Information System (OAIS) Reference Model*. In addition, vendors should be familiar and comply with *Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist*. The Checklist serves to identify digital repositories capable of reliably storing, migrating, and providing access to digital collections. Print is not an acceptable archival format for electronic content.

REFERENCES

Open Archival Information System (OAIS) Reference Model:
http://nost.gsfc.nasa.gov/isoas/ref_model.html

Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist:
http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

4.6 DISCOVERABILITY

4.6.1 Accommodation for Integrated Discovery: Federation and Aggregation

The trend in bibliographic discovery is to move away from visiting each separate vendor interface and move toward the use of a single search environment. This requires vendors to make their content and metadata discoverable through a variety of means. The CDL believes it is in the vendor's interest to expose content in as many places as possible, since vendors:

- retain all their existing revenue streams; and
- continue to safeguard access to the full text, since vendors still control authentication/authorization/delivery

As a benefit, users enjoy increased findability and vendors enjoy increased promotion and use of their content.

Integrated discovery can be achieved in one of two ways: aggregation or federation.

4.6.1.1 AGGREGATION

Scholarly content is aggregated into a single index that is made available in centralized services such as Google, Google Scholar, and WorldCat Local. In this approach, a centralized service (e.g., Google Scholar) obtains permission from the content provider to index the content locally, either by harvesting metadata or by crawling the full text content.

The CDL strongly encourages content providers to allow their content to be included in these services, which are taking an increasingly prominent role in the searching behavior of users. Exclusive arrangements with aggregated search providers are strongly discouraged and will be considered in licensing decisions if the library's service of choice is not supported.

4.6.1.2 FEDERATION

Some individual University of California campuses are investigating the use of federated search portals that search multiple remote databases with a single query. Vendors should be aware of the *NISO MetaSearch Initiative* and the following protocols:

1. Z39.50
2. SRU (preferred) or SRW
3. NISO Metasearch XML Gateway (MXG) protocol (based on the NISO-registered SRU protocol)
4. Proprietary XML gateway

REFERENCES

NISO MetaSearch Initiative: <http://www.niso.org/workrooms/mi>

NISO Metasearch XML Gateway (MXG) protocol: <http://www.niso.org/publications/rp/RP-2006-02.pdf>

4.6.2 Vendor Records

The University of California is investigating web-based next generation discovery services. In order for UC patrons to have access to our complete holdings, it is important that licensed vendor records be fully represented in these services. The CDL requests that vendors make their record sets available for loading into web-based discovery services, so that UC patrons have centralized access to a broad range of materials. The CDL prefers vendor records to be provided in MARC format.

4.6.3 Resource URL Verification

The CDL maintains a local persistent identifier (PID) service to manage access and changes to vendor resource URLs. The CDL will periodically validate these persistent identifiers (PIDs) to assure that they still resolve to the correct URLs. If the licensor's site maintains a robots.txt entry indicating that it does not permit programmatic access to the site, the CDL will assume permission to run its validation tool for the PIDs that the CDL has assigned to the licensed content. No reconfiguration of the licensor's robots.txt file is needed.

4.6.4 Inbound Linking to Full text Content

All documents contained in the electronic resource should be easily discovered and located from any licensed resource held by the CDL or UC campuses when in electronic form, or in print form from any of the UC campuses.

4.6.4.1 CONSTRUCTION OF INBOUND URLS

URLs for linking to content on the vendors site can be formatted according to either the OpenURL standard or a well documented proprietary format. The elements used in constructing the URL must be common citation data elements and cannot be tied to an identifier specific to the vendor such as a unique article ID number.

Linking to articles: the CDL's preferred method is a computable, dynamic link to the publisher's site that will take the user directly to the article. We should be able to create this link using the metadata commonly found in an OpenURL, i.e.

- ISSN or ISBN
- Volume
- Issue
- Page
- Date

REFERENCES

NISO OpenURL standard Z39.88-2004: <http://www.niso.org/standards/z39.88-2004>

4.6.4.2 CROSSREF

The CDL can also use CrossRef to discover Digital Object Identifiers (DOIs), a unique identifying string which can be used to link to content on the publisher's site. The CDL needs a commitment from publishers that are CrossRef members that all of the full text that is available on their web sites has a corresponding metadata record in the CrossRef database.

REFERENCES

CrossRef: <http://www.crossref.org/>

International DOI Foundation: <http://www.doi.org/>

4.7 OUTBOUND LINKING

The CDL requires that OpenURLs be present on all records in the database, and when possible, the references associated with the articles. The OpenURLs should be formatted according to the NISO OpenURL standard, Z39.88-2004 and contain as much metadata as possible.

The CDL's link resolver presents additional service options, such as the CDL's Request service (ILL) and links to citation management databases such as RefWorks and EndNote which work best with a high level of quality metadata. The CDL Request service allows users to initiate an Interlibrary Loan request from citation(s) found in the database search result. To fully support Request and other OpenURL based services implemented for the UC community, the CDL has established the following set of metadata requirements.

4.7.1 Metadata Requirements for OpenURL

While we recognize there are no minimum data element requirements by default in the OpenURL standard, the CDL prefers that vendors use as complete an OpenURL as possible.

To support CDL's Request service (automatic generation of ISO Interlibrary Loan requests), the capture of article citations for use in bibliographies, and e-content links at the article level, the CDL SFX server needs to receive a comprehensive set of metadata data in the OpenURL from the source service (electronic resources vendor).

1. The Origin-Description needs to contain a database specific sid value.
2. In the Object-Metadata zone the elements are:
 - issn; isbn
 - DOI
 - aulast
 - aulast; auinit; auinit1; auinitm

- title;
 - atitle
 - volume
 - issue
 - pages; spage; epage
 - date
 - genre
3. In the Local-Identifier zone the elements are:
- publisher
 - placeOfPublication
 - edition
 - seriesTitle
 - conferenceTitle
 - conferenceDate
 - reportNumber
 - dissertationNumber

EXAMPLE 1. BOOK RECORD

Barry, B. T. K. Tin and its alloys and compounds/B.T.K. Barry and C.J. Thwaites

Chichester: Ellis Horwood; New York: Halsted Press, 1983.

Series title: Ellis Horwood series in industrial metals.

The OpenURL for this book would be:

OpenURL version 1.0 :

```
<sid>;genre=book;isbn=0470274808;title=Tin%20and%20its%20alloys%20and%20compounds%20%20;date=1983;aulast=Barry;aufirst=B;aunitm=T;rft_id=info%3Aoclcnum%2F9756612;rft_id=urn%3AISBN%3A0470274808;rft.aulast=Barry;rft.aufirst=B;rft.aunitm=T;rft.btitle=Tin%20and%20its%20alloys%20and%20compounds%20%20;rft.date=1983;rft.isbn=0470274808;rft.place=Chichester%20%20%3BNew%20York;rft.pub=Ellis%20Horwood%20%3B%3BHalsted%20Press;rft.genre=book
```

OpenURL version 0.1 (before percent encoding):

```
<sid>?isbn=0470274808&aulast=barry&aunit=BTK&title=Tin and its alloys and compounds&date=1983&pid=publisher=Ellis Horwood:placeOfPublication=Chichester:seriesTitle=Ellis Horwood series in industrial metals
```

EXAMPLE 2. ARTICLE RECORD

Hall M; Thwaites R; Gompels MJ. Census of availability of neonatal intensive care should have used different denominator. BMJ (Clinical Research Ed.), 2001 Mar 17,322(7287):675

The OpenURL for this article would be:

OpenURL version 1.0:

```
<sid>;rft.atitle=Census%20of%20availability%20of%20neonatal%20intensive%20care%20should%20have%20used%20different%20denominator;rft.aunit=M;rft.aulast=Hall;rft.date=2001;rft.epage=675;rft.genre=article;rft.issn=0959-535X;rft.issue=7287;rft.spage=675;rft.stitle=BRIT%20MED%20J;rft.title=BRITISH%20MEDICAL%20JOURNAL;rft.volume=322;rft.au=Thwaites%2C%20R;rft.au=Gompels%2C%20MJ
```

OpenURL version 0.1 (before percent encoding): <host>?issn=0959-8138&title=Bmj (Clinical Research Ed.)&aulast=Hall&aunit1=M&atitle=Census of availability of neonatal

intensive care should have used different denominator&date=2001-03-17&volume=322&issue=7287&spage=675

4.8 DOWNLOADING AND CITATION MANAGEMENT SOFTWARE

The direct interchange of information between abstracting and indexing services and our users' citation management software is critical for today's scholar. Proprietary vendor data export that does not function efficiently with citation management software creates a barrier for our users. The CDL prefers to contract with vendors who are willing to provide record export formatting that is compatible with the citation management products in general use by UC faculty, students and staff, for example, RefWorks and Endnote.

5 Interface Requirements

5.1 ADHERENCE TO PREVAILING STANDARDS

Access to the resource must be simple for the user, and should use standard formats, protocols, codecs, and applications already in widespread use (e.g., HTTP, HTML, PDF, GIF, XML, MP3, MPEG, etc.).

5.2 PLATFORM AND BROWSER SUPPORT

Many UC users access licensed electronic resources from different platforms, including those available on the Windows, Macintosh, and Linux operating systems. In order to reach all University of California users, vendors should offer file formats and interface functionality that is accessible on all major browsers regardless of platform. In addition, vendors should be compatible with third-party applications (such as Adobe Reader) that are supported for the most current and recent previous major releases of each Windows and Macintosh operating system release. The same support level should be maintained for vendor created client applications.

Compatible – Resources should be tested and compatible with all major authentication methods, platforms, major browsers and recent versions of this and supporting software. As of May 2010, this is defined as:

- Platforms and OS Versions: Macintosh OS X 10.4 and above, 64 and 32 bit; Windows 7, Vista, XP; Linux. Browsers: Internet Explorer 7 and above, Firefox 3.0 and above, Safari 3.2 and above, Google Chrome 4 and above.
- Supporting software: Java, Adobe Reader, Adobe Flash.

REFERENCES

Browser Support Matrix for University of California Web Content Providers:

<https://spaces.ais.ucla.edu/display/ucitag/UCBrowserSupportMatrix>

Browser Related Recommendations for Developing and Procuring Web Services at the University of California:

<https://spaces.ais.ucla.edu/display/ucitag/UCWebStandardsSupportStrategy>

5.3 CLIENT SOFTWARE

The CDL highly discourages requiring the installation and use of specialized client applications to access licensed content, as this requires a substantial time investment to distribute to library and staff machines, has restricted compatibility with remote access authentication methods, and often poses problems for users who are on restricted-access workstations. If client software is required, the software should be available at no charge, tested on multiple platforms, should not require administrative permissions on the local machine, and should be easily acquired and implemented.

5.4 MOBILE COMPUTING

Mobile computing is becoming more ubiquitous, and for some users it is their primary method of access to the Internet. Many vendors are providing mobile functionality, ranging from mobile-specific web pages to custom client applications. Issues of authentication are crucial for accessing licensed resources, and the authentication methods of these features are as varied as the interfaces themselves.

As of August 2010, the CDL's support policy for mobile access to licensed resources is limited to mobile-optimized web pages (the "mini-browser" experience), and access to the current web interface to the degree that behavior can be duplicated on a desktop machine. Applications are not supported by the CDL at this time.

Recommendations:

- Vendors should prioritize development of mobile web sites over client applications.
- Web pages should be tested and compatible with the primary browsers available on the Apple, Blackberry and Android platforms.
- Testing should be performed on the devices and not rely solely on emulators.
- Access to the licensed resource should match the method used for desktop access and should not require additional accounts or authentication methods.
- Accessing the platform from a mobile device should default to the mobile web interface, if available.
- Users should have the ability to "force" mobile or conventional web site display regardless of platform they are currently using (desktop or mobile).
- PDFs displayed on mobile platforms should have one column and/or be compatible with epub format for resizing.

REFERENCES

CDL Mobile Support Policy for CDL Licensed Resources:

<http://www.cdlib.org/services/collections/mobile.html>

CDL Mobile Device User Research Wiki: <https://wiki.ucop.edu/display/CMDUR/>

The Morgan Stanley Mobile Internet Report:

http://www.morganstanley.com/institutional/techresearch/mobile_internet_report122009.html

5.5 SEARCH WIDGETS

Search widgets provide an external search point for a licensed resource. Widgets can take three different forms:

- Web page/build your own/JavaScript (EBSCOhost, ProQuest)
- API (for direct and programmatic access)
- Browser Plugin (LibX)

Any widget functionality should be tested and compatible with all major platforms and browsers and recent legacy versions as listed under Platform and Browser Support.

5.6 AVAILABILITY OF CONTENT

- When the electronic resource interface includes both licensed and non-licensed content (e.g. some online journal or e-book sites), the availability of the licensed content should be unambiguous to the user.
- If icons or other identifiers are used to indicate availability, these must be kept up-to-date and should be displayed at all levels of access, e.g., title level, volume level, issue, chapter, etc.
- Users must be able to readily identify full-text access options such as PDF or HTML. In databases that contain multiple types of resources there should be a way to readily identify the item type and format.
- Pay-Per View and print on demand options should never obscure or override library-provided access to content. For licensed materials, content access should be easily seen. For non-licensed content, if a purchase option is present, a link to UC-eLinks,

UC's link resolver, should be the dominant one on the page, in addition to customizable text reflecting alternative access. If customizable text is not available, the print on demand option should not be present.

5.7 OPEN ACCESS

Vendors that offer a combination of open access and subscribed content should indicate the journal's access status both through the interface at the title level as well as including open access markers at the article level.

5.8 USABILITY

When selecting information services vendors on behalf of the entire University of California, the CDL prefers vendors who meet our standards of usability. We use the following principles when evaluating a user interface.

5.8.1 Consistency and Clarity

- The interface should use consistent language and tone throughout, with words, phrases and concepts familiar to users, rather than system-oriented terms. It should follow real-world conventions, and information should appear in a natural and logical order. Example: Use "Subject" as the label for Subject searching rather than "Descriptors."
- Users should not be presented with irrelevant or rarely needed information and/or graphics. Every extra unit of information in a dialog box competes with the relevant units of information and diminishes their relative visibility. Example: The interface should not contain distracting graphic icons.
- The same words/commands should perform the same functions throughout the interface. Users should not have to wonder if different words, situations, or actions mean the same thing. Example: Clicking on a "modify search" link from any point in the search results display should take the user back to the same menu of search modification choices.
- Functions of words/commands should be consistent with widely accepted standards. Example: Search options (such as Keyword, Boolean, etc.) should function as expected.
- If used, icons or words/commands indicating actions and options should be clearly differentiated so that users can readily tell them apart. Example: Labels for items such as Full Text and Citation should appear with the icon.

5.8.2 Context and Navigation

- The interface should be structured so that, at any given point, users can identify where they are in relation to the supported options and functions. Users should not have to remember information from one part of the dialogue to another. Supporting tools and search features should be incorporated into the most common user task sequences. Example: Tabbed search screens where a tab's label and emphasis indicates the search type being used, or an on-screen display of the status, e.g., "Advanced Search."
- Links should clearly indicate to users where they will end up, preventing errors. Example: A link to details on how to use a thesaurus should be labeled "Go to Thesaurus Help" rather than "More Info."
- Instructions for use of the system should be visible or easily retrievable whenever appropriate. Example: The options for features such as Search or Help should be readily available so the user does not have to remember how to navigate to them.
- It should be clear how to exit or back up from an activity at any point in the process. Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an

extended dialogue. Examples: Functions such as Undo and Redo should be clearly marked; for functions that open new browser windows, the procedure for closing the window should be obvious.

5.8.3 Search

- The interface should aid in the process of creating a search statement, and should provide multiple ways for users to intuitively refine a query by grouping, sorting, and limiting from the results page. Examples: Suggestions for broadening or narrowing a search by language, format, etc. should be made; users should be able to select options from a list of controlled vocabulary.
- The system should offer choices from a menu of pre-defined syntaxes, for both searching and navigating thesauri. Users should not have to guess at syntaxes. Example: Multiple pull-down menus with the choices AND, OR, NOT etc. should be offered to combine search terms.
- Documentation of the range and scope of searchable materials must be easy accessible. Example: Providing a link to the list of Journal Titles indexed in the database directly from the search interface.

5.8.4 “Learnability” and Flexibility

- There must be a minimal learning curve for first time users, as well as provisions for more advanced users to learn features as they become appropriate. Example: Both simple and advanced search modes should be available.
- Mechanisms should be available to speed up the interaction for expert users; the system should cater to both inexperienced and experienced users. Example: A Command line interface that allows advanced users to accomplish their searches more quickly and concisely than is possible via the graphic user interface.
- Help and documentation should be easy to search, focused on the user’s task, list concrete steps to be carried out, and should not be unwieldy. Examples: Documentation should be readily available on each page or just a click/page away; definitions of terms should be provided.
- The system should always keep users informed about the status of reported problems through appropriate feedback within a reasonable time. Example: If a patron cannot access a particular database because of a licensing agreement condition, this should be clearly stated instead of simply denying access without an explanation.
- Error messages should be expressed in plain language, precisely indicate the problem, and constructively suggest a solution. Example: The system should suggest search strategies when it retrieves too few or too many search results.

5.9 INSTITUTIONAL CUSTOMIZABILITY

5.9.1 OpenURL

Vendors should provide the option for a customizable icon for OpenURL. The OpenURL icon should appear for all appropriate display formats, e.g., for each occurrence of the cited reference/bibliography for an article.

5.9.2 Institutional Branding

Users often cannot tell the difference between freely available and subscribed content. To increase awareness of library-provided materials, vendors should support institutional branding, using a text string, graphics, or both.

For CDL licensed electronic resources, branding should be customizable at the campus-level and the branding text needs to be on all web pages to capture user attention regardless of the user's access path.

Branding settings should be configurable through the institutional administrative interface.

Requirements such as text length, graphics dimensions, graphics size, etc. should be documented and easily available.

The ability to preview settings is preferred.

REFERENCES

UC Libraries Interface Branding: <http://www.cdlib.org/services/collections/branding.html>

5.9.2.2 CAMPUS NAMING CONVENTION

Users should be presented with the message "Access paid by [campus library name]".

5.9.2.3 BRANDING WITH GRAPHICS

Graphics should be clickable to go to a specified URL.

5.9.2.4 ASK A LIBRARIAN

"Ask a Librarian" is a web page hosted by each campus and/or campus library containing reference librarian information, phone number, hours, email, and an option to initiate a live chat session. Similar to branding, this option should be customizable for each campus.

5.10 ONLINE HELP

Online help is increasingly important as many users work off-campus. All aspects of the resource and access to it should be well documented. There should be online help functions and a prominently placed link to the vendor's technical assistance/user support resources. Good online help also aids librarians in training and assisting users in person. Based on experience with many vendor help systems, the CDL has developed a checklist of desirable characteristics.

Many of the UC's users access databases from remote locations, 24 hours a day. In such circumstances, in-person help may not be available or convenient. Vendor online help, then, becomes increasingly important to our users. Vendor online help is most effective for users when it is:

1. Organized and accessible in several ways: Help should be organized by task or function, by index or glossary, be searchable, and be context sensitive.
2. Context sensitive: Help should be specific to the situation or action just taken.
3. Easy to navigate between Help and previous activity: Help should appear in a new, smaller window that "stays on top" so that users may consult help while working on the search form, display options, etc.
4. Database specific: Help should describe options that apply only to the selected database or it should be clear when a feature is generic to the platform vs. specific to a database. Features unique to a database should be easily discovered.

5. Searchable: For example, if users want to know how to rank results in the database, it is most useful if, in the help system, users can type in the term rank results and be guided as to how do this in the database.
6. Glossary: The user should be able to locate the definition of a specific term; the glossary should be easy to discover.
7. Built in "how-to" tutorials: Tutorials, available from the search screen, that guide the user through the system, allow for searching specific terms, and provide some indication of how long each section of the tutorial is (e.g., 3 screens, five minutes) are extremely useful.
8. Error messages: Messages should be comprehensible and helpful; for example, zero results prompts for a display of search tips.
9. Self-instructing: The help interface should guide the user by providing sample searches shown on the initial and following search screens, if appropriate, as well as in help text.
10. Adaptable training materials: The vendor should provide materials such as online user guides that are adaptable by the home institution.
11. Feedback: The option for the user to provide feedback should be highly visible, with the ability to send online comments both to the home campus and to the vendor. It is also desirable to provide a link to a designated page on a library's web site (at least one per campus) which offers the user choices for getting help via live reference chat, email, phone, or in person.
12. For each index in the database there should be database-specific
 - a. Explanations of what is searched, e.g., "The keyword index looks for terms from the Title, Abstract and Subject fields";
 - b. Indication of the portion of the database searched by the index, e.g., 1994-present, if the index does not search all years of the database. This should also appear with the index name in any search forms or menus, e.g., Subject (1967-);
 - c. Examples of the syntax to be used for the index, e.g., "When searching for the author Andrea P. Anderson, format your search as Anderson, A P";
 - d. Links from the index description to any controlled vocabulary used by the index.

5.11 COMPLIANCE WITH THE AMERICANS WITH DISABILITIES ACT (ADA)

The CDL is committed to providing resource access to members of the UC community with disabilities. Preferred vendors will comply with World Wide Web Consortium (W3C) "Web Content Accessibility Guidelines" and Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). As part of the Selection/Evaluation document submitted to the vendor, vendors should submit proposals that include a reasonable response to applicable sections of the Voluntary Product Accessibility Template (VPAT), particularly sections 1194.21 - Software Applications and Operating Systems; 1194.22 - Web-based Internet Information and Applications; 1194.31 - Functional Performance Criteria; and 1194.41 - Information, Documentation and Support, in order to describe product accessibility compliance. Disclosure of noncompliance as well as a clear timeframe for compliance should be included in the Remarks and Explanations column.

The CDL reserves the right to conduct real-world testing of a vendor's product or services to validate claims regarding Section 508 compliance. Information about the University's electronic accessibility initiative and information about the VPAT and the Information Technology Industry Council are referenced below.

REFERENCES

Web Content Accessibility Guidelines (WCAG) 2.0: <http://www.w3.org/TR/WCAG20/>

Section 508 Standards: <http://section508.gov/>

Voluntary Product Accessibility Template: <http://www.itic.org/clientuploads/resources/ITI-VPAT-v1.3.doc>

VPAT Information:

http://www.itic.org/archives/articles/20040506/faq_voluntary_product_accessibility_template_vpattm.php

UC Information Technology Leadership Council: <http://www.ucop.edu/irc/itlc/welcome.html>

Electronic Accessibility at the University of California Work Group:

<http://www.ucop.edu/irc/itaccessibility/>

5.12 PERSONALIZED FUNCTIONALITY

5.12.1 Interface Customization

User defined display options should be available. Example: Users should be able to change the size of icons, or choose a certain number of results to display.

5.12.2 Current Awareness

UC users rely on current awareness services (a.k.a. AutoAlerts, Search Alerts, RSS feeds) to keep up with the literature in their field. These services allow users to submit scripts of one or more searches that run at pre-selected intervals in the ejournal system or selected database and retrieve records added to the corpus since the last run of the script. Results from these searches are automatically mailed to the user's email address.

The vendor system should:

1. Support user self-registration for current awareness service and not require the CDL to assign specific user accounts for access to this service.
2. Support the creation of a script of one or more searches that can be scheduled to run without user intervention.
3. Run search scripts automatically against the specified ejournal system(s)/database(s) at a specified interval.
4. Mail the results of automatic searches to one or more user-defined electronic mailboxes or via RSS feeds.
5. Support all display options that are supported for search results in the vendor web interface. This should include a tagged data format so that a user may export the data into citation management software.
6. Make it possible for users to designate an existing search (e.g., the current search or a search available in the Previous Searches) to be executed as an automatic "update" search.

7. Allow the user to edit the search scripts once submitted.
8. Allow the user to delete a script and its associated search results at any time.
9. Have search scripts run for a specified time period, preferably one year, with an option for the user to renew them. Scripts should not expire during June, July, August, or September. Scripts that would normally expire during these months should expire in October so that users who are away during the summer do not return to find that their scripts have expired.
10. Alert the user via email that an update is about to expire. If the system supports storage of personal information between sessions, it is desirable that a notification also be placed in the profiled user's work area.
11. Include URLs that accompany records in an update.

The following items are desirable, but not required.

1. Ability to disable the "update" feature for certain public locations and/or for certain databases.
2. Option for user to assign an email subject line to the automatic "update" search.
3. Option for user to assign a name to the automatic "update" search.
4. Option for user to supply an email annotation that would be attached to each delivery of search results.
5. Option to select whether or not to receive reports of searches that retrieve zero results.
6. Possibility for search results to remain accessible for at least 4 weeks after the weekly search has completed. Users should be able to access the results via the same identification mechanism used to edit existing "update" searches.
7. Option for the profiled user to be notified that an automatic search has completed at the time of logon to the database.
8. Option for user to select whether to receive the update results by email, by RSS feeds, and/or by notification at logon (for profiled users).
9. Ability to send the results of an "update" search to a user work area to be accessed by the profiled user who submitted the search.

5.12.3 User Self-Registration

This function allows users to set various preferences on the vendor site, for example, to create a set of favorite journals, save search results, store their email address, set default preferences such as preferred display format, etc. It enables users to easily identify themselves in order to create, view and modify their preferences.

Where single sign-on is implemented, personalization features should be integrated with single sign-on authentication. If not, or if single sign-on is not implemented, then personalized account access should be provided via username and password, as well as requiring separate IP validation. These user accounts should not provide access to the resource comparable to IP access. Accounts used for accessing personalized functionality should not require librarian intervention to implement or maintain - UC is not responsible for verifying the authorization status of an account's user.

The specifications below are those used for this function in CDL's Melvyl Catalog. Methods for allowing users to self-register may vary as long as they generally conform to the

method described below. The “forgot password” routine is optional but experience has shown that users will need and appreciate this capability.

1. To create a profile, the user must establish a User ID and Password. These may consist of 3 to 12 alphanumeric characters. The user is asked to enter the password twice to confirm.
2. On the same page, the user may enter an email address if they want to use the Update (current awareness) service.
3. On the same page, the user is presented the option of answering one of three possible “password bypass” questions. User's answer to the question may be up to 15 alpha characters long, is not case sensitive, and is stored in the administrative database.
4. On Sign In page, user is required to enter User ID and Password. Sign In page contains the “Forgot Password?” link.
5. If user selects the “Forgot Password?” link from Sign In page, the user is taken to a page that includes the password bypass question, as well as the opportunity to enter their User ID and a new password.
6. If user's answer to password bypass question is positively matched against the stored answer, user receives confirmation that a new password has been established. User is signed in and is granted access to previously established profile. If password bypass question is not answered correctly, system returns message that a match could not be made and that user must establish a new profile.

5.13 STREAMING MEDIA

Many of our users access electronic resources from remote locations, 24 hours a day. In order to provide streaming media databases to our remote users, vendors should utilize streaming media protocols that are supported on a wide variety of proxy servers and VPN software. Any special instructions, such as port opening or tunneling protocols, should be communicated explicitly in advance of launching the service for implementation by remote access administrators.

5.14 DIGITAL RIGHTS MANAGEMENT

Digital Rights Management includes protocols and functionality to limit use and functionality of content for the purpose of inhibiting unauthorized use and distribution.

REFERENCES

Wikipedia -Digital Rights Management:

http://en.wikipedia.org/wiki/Digital_rights_management

5.14.1 Watermarks

Implementation of watermarks for digital images, text, audio or video should be invisible to human senses, and should not degrade the quality of the content. Watermarks (either embedded or as accompanying metadata) is intended to protect the owner's rights and must not contain any user- or account-related information, for example, a UC account number or the user's IP address.

5.14.2 **Restricted Functionality**

In addition to watermarks, any limitations to use and functionality should not create an undue burden on the user and should not infringe on permitted use as defined in the signed license.

- Text and images should have no restrictions on printing.
- The file itself should be easy to use and access – each page should not be a separate file, for instance.
- Navigation between chapters should be easy.

For audio and video, offering materials via web streaming addresses many vendor concerns that are present with downloaded files.

In general, selected functionality should not be restricted to subgroups of users (as an example, only permitting faculty to use personalized list creation and sharing features). In the case that such restrictions are implemented, all responsibility for identifying permitted users lies with the vendor and is not the responsibility of the institution.

6 Vendor Communication and Support

6.1 DOCUMENTATION TO BE PROVIDED TO CDL STAFF

To set up a new account the vendor should provide the following information as soon as the resources and/or journal titles are agreed upon:

6.1.1 All Resources

- Date access is scheduled to begin
- Any high level network configuration requirements (port settings, etc.)
- Technical contact (including email address and phone number) for problems, questions, etc.
- Account number and administrative username and password where applicable
- URL for access to a menu of all UC licensed databases on the platform
- URL(s) for access to each database licensed; if the URLs are campus specific, the campus specific URLs should be supplied
- If client-side software or plugins are required, the plugin version supported, link to installation instructions, documentation for functionality and limitations should be supplied

6.1.2 Ejournals

- If back years are still being loaded, the date when content is scheduled to be complete
- Underlying platform used (for example, Highwire, Atypon, Metapress, Ingenta, etc.)
- For each title, we need to know the following:
 - ISSNs
 - Coverage details: initial volume/issue with full-text, including month/year (YYYYMM)
 - For closed titles, ending volume/issue, including month/year (YYYYMM)
 - Title level URLs for each journal, or instructions for creating
 - List should include titles no longer actively published, that are linked to currently published titles (i.e., prior titles)
 - Any gaps in coverage should be fully documented for both current and backfile content

6.1.3 Ebooks

- Title list with publication dates and ISBNs
- Title level URLs for each book or instructions for creating
- Whether we have rights to future or past editions
- Material excluded from the digitized version: missing content, illustrations, et al.

6.2 EXPECTATIONS FOR PROBLEM RESOLUTION

6.2.1 Access Problems Reported to the Vendor by the CDL or UC Campus Staff

Once an issue is reported, the vendor should reply back to confirm receipt, and include the text of the original problem. Access problems should be resolved as soon as possible. The vendor must clearly indicate the mechanism for reporting and resolving problems that occur outside normal business hours. If issues, such as problems with access, become complex and/or difficult to resolve, the vendor will keep the CDL apprised daily of possible solutions and a timeline for resolution of the problems. Once the issue is resolved, the vendor will notify CDL as to the resolution.

6.2.2 Use of Vendor Web Forms for Reporting Problems

With increased use of web forms by vendors for submitting incidents, a submitted incident needs to have an immediate copy of the web form text emailed to the reporting person.

In addition, it is desirable to include an incident code for future inclusion in the subject line (so that it can immediately hook into the ticketing system) and an option to include the ticketing software email address in the report.

6.3 NOTIFICATIONS FROM VENDORS

6.3.1 Downtime

Notification must be provided to the CDL Support Team list preferably two weeks in advance of scheduled downtimes during prime time, or no less than 48 hours for a scheduled outage during non-prime time. Outage notification should include the expected time of the outage, the probable length of the outage, the systems or resources affected and the impact of the outage on the licensed systems. Placing a notice of scheduled maintenance on the product home page is not sufficient; we require proactive notification of anticipated downtime.

In addition, vendors should provide a system status page that is hosted on a server not used to provide access to content. See the OCLC Support home page "System Alerts" page for an example. The vendor system status page should report both planned and unexpected outages.

REFERENCES

OCLC Support System Alerts: <http://www.oclc.org/support/systemalerts/>

6.3.2 Breach Resolution

CDL has established procedures for immediate investigation of access or downloading violations. CDL technical staff will work with the appropriate campus and the vendor to identify source, remedy any problem, educate campus users, and document activities.

The vendor should immediately report any suspected irregularity to CDL's License Manager, Curtis Lavery (curtis.lavery@ucop.edu or 510-987-9262) and to CDL's technical contact, Margery Tibbetts (margery.tibbetts@ucop.edu or 510-987-0581). In the event that these staff members are unavailable, please contact the CDL Helpline (510-987-0555).

REFERENCES

CDL Breach Process documentation: <http://www.cdlib.org/contact/BreachAllegation.html>

6.3.3 Notification of Changes to the Resource

Major changes to the resource should be fully documented and announced at least three months in advance via email to the CDL Support Team list and the appropriate Resource Liaison. Ideally, such changes should occur in the summer, so that notification to users and instructional and publicity materials can be prepared in advance, as well as causing minimal disruption to the academic calendar.

- Changes in delivery, including access mechanism, platform, article, journal or resource URLs, require advance notification.
 - For global changes, such as changing the database platform, the CDL requires a minimum of six months notice. Notification should be sent via email to the CDL Support Team list and Resource Liaison.
 - When migrating to a new site, dual access must be maintained for a minimum of three months.
 - The full extent of the changes should be documented and announced at least three months in advance.
 - Vendor technical staff must be available for consultation and problem resolution.
 - Any aspect that impacts service to users, e.g. OpenURL service, should be included in the notification.
 - Redirect services should be provided.
- User interface changes: This includes changes in format, display and indexing of the content and adding new features and functionality.
- Changes in content coverage: The full extent of the changes should be documented and notification sent to the CDL Support Team list at least six weeks in advance regarding:

For Ejournals, Ebooks and other resources licensed per-title:

- If not all titles are available on day one, an automatic notification procedure is needed when new titles are added to the site
- Title changes, including new title details and last volume/issue of prior title
- Newly published, transferred and newly online titles available for addition to agreement
- Titles to be dropped, including details of the publisher picking up the journal (if applicable) and the effective date
- Titles ceasing publication, including last expected issue

For Databases:

- Titles to be dropped from indexing and/or full-text coverage
- Titles ceasing publication and date of last indexed issue
- Titles added to the indexing stream and level of coverage, e.g., cover-to-cover or selective indexing

- Changes in content loading schedule: The CDL should be notified via email to the CDL Support Team list as soon as it is established that there are problems with content loading that may result in delays of one week or more for addition of new content.
- OpenURL support: Changes in the level of OpenURL support, including data added or dropped from the OpenURL, e.g., moving from version 0.1 to version 1.0 of the OpenURL standard. Notification of major changes, e.g., new syntax, should be sent to the CDL Support Team list as soon as the final specifications have been established.
- Functionality: Notification should be sent to the CDL Support Team list at least three months in advance of the addition of new functions and of functions that are removed, substantially changed and/or impact platform compatibility.
- Problems with statistics reports: Vendors should inform customers of any issues related to usage statistics in a timely manner, for instance, incorrect data or delays in posting data.

REFERENCES

CDL Support Team list email address: cdlsupport-l@ucop.edu

CDL Resource Liaison roster: <http://www.cdlib.org/inside/rl/rosters.html>

6.4 ADMINISTRATIVE MODULE ACCOUNT

The CDL prefers one systemwide login that provides full access to all related subaccounts (providing the ability to move quickly between campuses when updating options). Administrative logins should use a user name and password, and not be authenticated via IP address.

6.5 IP ADDRESS LIST UPDATES

The CDL will provide an initial list of IP addresses for the UC community, with subsequent updates. The list indicates which addresses represent proxy servers and VPNs. The UC Office of the President [UCOP] is an administrative unit for the system as a whole and must have access to CDL-licensed material. CDL requires that vendors notify us via the CDL Support Team list when the IP addresses list has been activated or updated so that CDL staff can begin testing to ensure that access is working. The CDL does not announce a new resource to our user community until this testing is complete. Delays and problems in activation or updates will be taken into account when UC makes decisions on new products or renewals, and vendors may be asked for a pro-ration or credit if activation is not handled in a timely manner.

The CDL makes a conscious effort to update the IP lists on a regular basis. We prefer that the vendor can take a formatted file and update the local IP tables. If IPs are maintained through the administrative interface, an import mechanism should be available to batch upload the IP list.

6.6 USAGE STATISTICS

Vendors should provide regular monthly statistics that conform to the COUNTER Code of Practice for Journals and Databases . Vendors should conform to the most current required release of the code. For further information, see COUNTER (Counting Online Usage of NeTworked Electronic Resources).

The CDL cannot license electronic products for which no usage statistics are provided. Statistics should include searches, sessions (optional), turn-aways (where applicable), and article downloads (e.g., PDF, HTML accesses) broken down by site (institutionally-defined set of IP addresses) and journal and/or database title.

Statistics should be reported separately for each UC campus and the Office of the President, as well as our two associated laboratories (Ernest Orlando Lawrence Berkeley National Laboratory [LBNL or LBL] and Lawrence Livermore National Laboratory [LLNL] where applicable).

Access to statistical reports should be available for download via a web-based reporting system that is updated in a timely manner. In addition, these data should be available in flat files containing specified data elements that can be downloaded and manipulated locally (e.g., Excel spreadsheets). Effective with Release 3 of the COUNTER Code of Practice (published August 2008), support for statistics harvesting via the NISO Standardized Usage Statistics Harvesting Initiative (SUSHI) is required.

REFERENCES

COUNTER: http://www.projectcounter.org/code_practice.html

CDL's Vendors and Content Providers: <http://www.cdlib.org/vendors/>

UC Campus sites with FTE: <http://www.cdlib.org/gateways/vendors/enrollment.html>

NISO Standardized Usage Statistics Harvesting Initiative (SUSHI):
http://www.niso.org/committees/SUSHI/SUSHI_comm.html

7 Content

7.1 DATA INTEGRITY

Data should be as accurate and up-to-date as possible and appropriate for the resource.

7.2 COVERAGE

CDL's expectation is that content availability is consistent and continuous for the date ranges provided for the licensed resource. Any variations in content and coverage (coverage gaps, embargoes) need to be communicated by the vendor in a clear and timely manner, preferably on a website.

7.3 FREE TRIALS AND NON-SUBSCRIBED CONTENT

No "free trials" of non-subscribed journal titles or databases should be added to the CDL package without express approval from the CDL.

7.4 CURRENCY

Abstracting and indexing databases should be updated within a week of receiving the new data from the provider. If that database also contains full text articles, that information should be current. If electronic content has print counterparts, electronic content including supplements should be available before, or no later than, the print equivalent. If the vendor provides the data in multiple formats, e.g., HTML and PDF, all formats should be available when the item is added to the site.

7.5 COMPLETENESS

Indexing should adhere to documented editorial guidelines that clearly state whether any parts of publications will not be indexed or whether certain titles will be selectively indexed based on subject. Missing material (e.g., articles and images) that should have been included should be added in a timely fashion at no additional cost.

For materials with a corresponding print version: Content that appears in the print version, which cannot appear online due to lack of electronic publication rights, must be acknowledged in the electronic version with a statement of why the material is unavailable online.

Electronic content should be cover-to-cover and include all content found in the print equivalent as well as all content issued as supplements or special issues in print or in other formats such as CD-ROM. Supplements should be made available online at the same time as the main issue. Cover-to-cover content includes, but is not limited to:

Abstracts, Addendums, Advertisements, Announcements, Author Biographies, Award Announcements, Book Reviews, Books Received, Brief Communications, Calendars, Cartoons, Case Reports, Classic Papers, Clinical Practice Reports, Conference Contents Lists, Correspondence, Cover Art, Debates, Directories, Discussions, Editorial Board Members, Editorials, Education Notes, Errata/Erratum, Forewords, Forthcoming Articles, Forum Articles, Full Length Articles, In Memoriam/Memorials, Indexes, Instructions To Authors, Introductions, Legal Notes, Letters To The Editor And Replies, Literature Alerts, Masthead Information, Miscellaneous, News/News Items, Obituaries, Other Contents, Papers Accepted for Publication, Patent Abstracts, Patent Reports, Personal Reports, Previews, Product News/Reviews, Publisher's Notes, Requests For Assistance, Research Notes, Research Papers, Review Articles, Schedule of Issues, Sequencing Reports, Short

Communications, Short Surveys, Software Reviews, Supplementary Materials, Tables Of Contents, Test Reviews.

7.6 CORRECTIONS

Vendors should supply a mechanism for reporting errors in the data to the publisher, and provide a documented policy for how often and by what mechanism errors will be corrected.

7.7 BACKFILES

Corrections or changes made to backfiles should be documented and communicated as performed.

7.8 QUALITY OF CONTENT

Digital reproductions of data, text, images, or media files should be of comparable quality to the original item. Vendors are expected to provide color digitization of images when a color image is used in the print version. Images of low quality that do not contain the details in the original image, scanned text that is done at too low of a resolution to be legible, or OCR created text that does not accurately reproduce the original prose are not of use to the academic community as teaching or research tools. Preferred vendors will meet or exceed the requirements as set forth in the "CDL Guidelines for Digital Images," the Digital Library Federation's "Benchmark for Faithful Digital Reproductions of Monographs and Serials," and BCR's Collaborative Digitization Program's "Digital Audio Best Practices."

REFERENCES

CDL Guidelines for Digital Images: <http://www.cdlib.org/inside/diglib/guidelines/GDO.pdf>

Digital Library Federation's Benchmark for Faithful Digital Reproductions of Monographs and Serials: <http://www.diglib.org/standards/bmarkfin.htm>

BCR's Collaborative Digitization Program's Digital Audio Best Practices: <http://www.bcr.org/dps/cdp/best/digital-audio-bp.pdf>

7.9 RETRACTED/DISPUTED ITEMS

Items under dispute must not be removed from the system, but should be clearly identified as disputed items and provide an explanation of the dispute. Retracted items must remain online and be clearly labeled as retracted. Errata should be linked to the original item and a link should appear for the Errata statement on the original item.