TECHNICAL REQUIREMENTS FOR LICENSED RESOURCES

Revised 5/08/2015

CALIFORNIA DIGITAL LIBRARY
UNIVERSITY OF CALIFORNIA

http://www.cdlib.org/gateways/vendors/guidelines_technical.html

1 Contents

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 the University of California (UC) libraries select a particular vendor for a systemwide licensed electronic resource, we aim not only to encourage maintenance of 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 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 opportunities for input on development priorities. The California Digital Library (CDL) sets a high standard for vendors that ultimately benefits all academic customers and leads to more competitive products for the publisher or vendor. We are 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 the University's own strategic plans. These opportunities could take place via a vendor user group, focus groups, working with the vendor's director of development, or discussions with the development planning team.

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. This document should not be considered a substitute for other requirements documents that may be included as part of a negotiation.

The expectations and behaviors described in this document should be considered broadly applicable to both existing features of UC licensed resources and newer capabilities that may emerge. They are meant to serve as guidelines and principles that are applicable to any functionality provided by the vendor.

Last but not least, despite the explicit mention of "Licensed Resources" in the document title, these guidelines and principles are relevant to any resource that the University of California promotes to its users, including those resources containing open access and freely available content.

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 an average of 98% end-user availability per month. The 2% unavailability includes both scheduled maintenance and unanticipated failures.
- 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.
- Systems must be capable of handling typical UC usage. If possible, the CDL will provide average user statistics for a comparable resource.

REFERENCES

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

CDL Support Team Helpline: (510) 987-0555

4.1.2 Information Security

The University of California maintains policies regarding the protection of electronic information, notably through *UC Business and Finance Bulleting BFB 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.”

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, “User Privacy”.

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

REFERENCES

UCOP Business and Finance Bulletin: BFB IS-3: Electronic Information Security: http://policy.ucop.edu/doc/7000543

4.1.3 User Privacy

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."

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 the data is retained.
- when the policy was last revised
- who is responsible for the privacy policy and how to contact the responsible party

REFERENCES

UCOP Business and Finance Bulletin: BFB IS-3: Electronic Information Security: http://policy.ucop.edu/doc/7000543

ICOLC Privacy Guidelines For Electronic Resource Vendors: http://icolc.net/statement/privacy-guidelines-electronic-resources-vendors

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

4.1.4 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.)

4.2 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.

Where a resource is subject to limited simultaneous users, the vendor should provide corresponding turnaway statistics.

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.

The University of California Libraries are actively investigating new solutions, particularly those that stress federated identity management and privacy protection such as Shibboleth.

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. Individual logins should only be used to support personalization features and not required for authentication.(see section 5.12, "Personalized Functionality".)

4.3.2 IP-based Authentication

IP addresses remain the most commonly implemented and supported means of user authorization at the University of California

At initial licensing, the CDL will provide an initial list of IP addresses for the UC community, with updates as needed. The list indicates which addresses represent proxy servers and VPNs.

We require that vendors notify the CDL via the CDL Support team when the IP addresses list has been activated 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.

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 in the coming years. The adoption of Shibboleth may very well preempt large-scale access problems as the sophistication of user access needs grows. In addition to providing a better experience for our users through the use 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 an 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.

However, large-scale implementation of Shibboleth requires careful planning to ensure a positive user experience across a broad range of resources. UC will be exploring Shibboleth implementation for licensed resources over the next several years.

Vendors are strongly urged to implement Shibboleth in order to enable a timely transition away from IP-authenticated access and facilitate strategies that UC may plan for in the next several years. The University of California campuses are members of the InCommon Federation and prefer to work with vendors that are also members of InCommon. Additional vendor implementation recommendations were issued in 2011 by NISO's Establishing Suggested Practices Regarding Single Sign-On (ESPReSSO) working group.

REFERENCES

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

UCTrust: The University of California Identity Management Federation: http://www.ucop.edu/information-technology-services//initiatives/uctrust-the-university-of-california-identity.html

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

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

InCommon Library Best Practices: http://www.incommon.org/library/docs/Best_Practices.pdf

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 IP-based 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 2015, 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. Therefore, 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 the Cisco and Juniper WebVPNs.

REFERENCES

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

OCLC overview of rewrite proxies:
http://www.oclc.org/support/documentation/ezproxy/rewrite.htm

4.3.5 Vendor Managed Authentication

It is CDL's preference that all access options to a licensed resource use access methods that are under the control of the subscribing institution.

Some vendors are providing alternative authentication methods directly to end users to permit off-campus user access to an institution's licensed content. This can happen in one of two ways: affiliation of a user name and login with an institution's subscription, e.g. by allowing users to establish a personal login from an on-campus IP address (thereby enabling access via username and password when logging in to a vendor website) or device authentication, which affiliates the device or application by use of a token, cookie, or vendor-managed proxy prefix.

In most cases, this functionality is intended for access via mobile devices or applications, although often the authentication also permits access by users via desktop or laptop computers.

Because the vendor-managed authentication process is completely outside of the control of the institution, and has the ability to provide access to individuals who are not authorized users, (such as remote access by walkin users and recent graduates), the University of California cannot accept responsibility for unauthorized use resulting from vendor-managed accounts.

Additional considerations for implementation:

- The institution should have an option to disable this functionality in the administrative module.
- The vendor is wholly responsible for verifying the user's institutional affiliation both when the user account or functionality is initially activated and when accounts or devices are "re-affiliated."
- Affiliations should regularly expire and require periodic user re-affiliation with the vendor. Users should be notified of upcoming expirations.
- The expiration and validation process and durations should be clearly documented on the vendor's web site.
- Vendors should disclose whether usage activity occurring through these vendor managed authentication methods is included with the regular usage statistics.

- This functionality should not be promoted by the vendor on their interface if the functionality has been disabled by the institution.

REFERENCES

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

4.4 ADDITIONAL TERMS AND CONDITIONS

4.4.1 Click-through Licenses

Click-through agreements are not allowed. The publisher/vendor may 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 institution's 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 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.

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 standards for digital preservation such as the *Open Archival Information System (OAIS) Reference Model*. In addition, the preservation repository vendor should be familiar and comply with *Audit and Certification of Trustworthy Digital Repositories* (ISO 16363). The Standard defines a

recommended practice for assessing the trustworthiness of digital repositories, and can be used either in a self-assessment or as the basis for a formal audit.

REFERENCES

CCSDS Open Archival Information System (OAIS) Reference Model:
http://public.ccsds.org/publications/archive/650x0m2.pdf

CCSDS Audit and Certification of Trustworthy Digital Repositories
http://public.ccsds.org/publications/archive/652x0m1.pdf

Center for Research Libraries. Certification and Assessment of Digital Repositories.
http://www.crl.edu/archiving-preservation/digital-archives/certification-assessment

4.5.3 Archival Format

- Print is not an acceptable archival format for electronic content.
- Archival content should be provided by the vendor in a format appropriate for the content and accessible using commonly available software.
- Files provided for archival purposes should not use commercial identifiers (such as DOIs) for internal navigation.

4.6 DISCOVERABILITY

4.6.1 Accommodation for Integrated Discovery: Federation and Aggregation

The trend in bibliographic discovery is the use of a single search environment. This requires vendors to make their content and metadata discoverable to the providers of the single search discovery tools. It is in the vendor's interest to expose content in as many places as possible.

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 EBSCO EDS, ExLibris PRIMO, Google Scholar, and ProQuest Summon and OCLC WorldCat Discovery. In this approach, a centralized service (e.g. OCLC WorldCat Discovery) obtains permission from the content provider to index the content locally. Article-level content sharing should adhere to the NISO Open Discovery Initiative best practices, and as applicable, follow the NISO Access and License indicators Recommended Practice which defines metadata indicators to be used to indicate free-to-read content and a link to license terms for the use/re-use of that 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

Vendors should be aware of the following protocols related to federated search and retrieval:

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

NISO Open Discovery Initiative (ODI): http://www.niso.org/workrooms/odi/

NISO Access and License Indicators (ALI): http://www.niso.org/workrooms/ali/

4.6.2 Vendor Records

The University of California has web-based next generation discovery services. In order for UC patrons to have access to our complete holdings, it is important that licensed vendor content be fully represented in these services. The CDL requests that vendors make their records available for loading into web-based discovery services, so that UC patrons have centralized access to a broad range of materials. Sharing of records should follow the NISO ODI and NISO metadata best practices, and CDL prefers that records be made available in MARC 21 format.

4.6.3 Resource URL Verification

The CDL will periodically validate URLs used to assure that they resolve correctly. 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 validation 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 items contained in the electronic resource should be easily discovered via an inbound link.

CDL use the ExLibris SFX link resolver software (UC e-Links) to support inbound linking to content. Vendors are encouraged to work with all major link resolver vendors to provide linking at the article level.

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.

REFERENCES

NISO OpenURL standard Z39.88-2004:
http://www.niso.org/apps/group_public/project/details.php?project_id=82

4.6.4.2 LINKING WITHIN A FRAME

In an endeavor to get user to content in one click, CDL is currently linking within a frame to display licensed full-text content along with navigation and library access information. Vendor content and display functionality should work within a framed environment.

4.6.4.3 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. Publishers that are CrossRef members should ensure 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 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.

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 (reference OpenURL profiles for metadata list).

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. Vendors should provide record export formatting that is compatible with the citation management products in general use by UC faculty, students and staff, for example, RefWorks, Endnote, Zotero and Mendeley.

4.9 TEXT AND DATA MINING (OR NON-CONSUMPTIVE USE)

Data mining, meta-analysis and other "non-consumptive" use are increasingly important activities engaged in by UC scholars. A concise explanation of non-consumptive use and the importance of supportive licensing terms is located in the ARL Fair Use Guidelines, Principle 7.

Expectations for text mining functionality include:

- It should be possible for the user to perform text and data mining against the resource natively through the default UI.

- If an API is offered:
    - the API should not be the sole way for a user to gather this data.
    - there should be no restrictions/limits to the amount of content that can be downloaded for non-consumptive use.
    - Usage statistics for API activity should be provided and identified.
- As non-consumptive use is permitted under the terms of the license, users should not need to get additional permissions or to pre-register with the vendor.
- Vendors should be willing to provide customized data sets upon user request.

REFERENCES

ARL Fair Use Guidelines, Principle 7 (page 28-30): http://www.arl.org/storage/documents/publications/code-of-best-practices-fair-use.pdf

LIBLICENSE Model License: http://liblicense.crl.edu/licensing-information/model-license/

5 Interface Requirements

Access to the resource must be simple for the user, and should use standard formats, protocols, codecs, and applications already in widespread use.

5.1 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 (Internet Explorer, Firefox, Safari and Google Chrome) regardless of platform. In addition, vendors should be compatible with third-party applications (Java, Adobe Reader, and Adobe Flash) 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.

5.2 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.

5.3 MOBILE DEVICE COMPUTING

Many vendors provide mobile access to their content, ranging from mobile-specific web pages to custom client applications.

For vendors who implement mobile access functionality, the CDL suggests the following to ensure that the mobile access methods are promotable and supportable by campuses:

General 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 iOS, and Android platforms.
- CDL prefers that access to licensed resources be authenticated via methods under the subscribing institution's control (such as IP address or Shibboleth). Access via methods not under the subscribing institutions' control has additional legal and contractual implications. More information is available at 4.3.5 "Vendor Managed Authentication".
- General standards regarding UI, content, access and support described in this document also apply to mobile access interface functionality.

Recommendations for Browser Based Web Access

- If a mobile-optimized web page is available, accessing the resource's web page from a mobile device should default to the mobile web page.
    - Mobile display should be available at all levels of the website, top level, title landing and article/chapter.

- Responsive design (same URL) is preferred over mobile-specific page (different URL).
- The mobile-optimized web display should have a link to display the full site.
- The mobile optimized web display should have basic institutional branding.
- Article displays for the mobile device should be optimized for the format/screen site.

Recommendations for Mobile Apps

- Mobile apps providing access to institutional content should not incur additional cost to the user.
- Apps should be available for both phone and tablet devices.
- Apps providing access to a subset of institutionally licensed content, or that only provide access to personally subscribed content should clearly indicate these limitations.

REFERENCES

CDL Mobile Support Policy for Systemwide Licensed Resources:
http://www.cdlib.org/services/collections/mobile.html

5.4 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

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.

5.5 PRESENTATION OF ACCESS ENTITLEMENTS

- The vendor should provide the ability to limit visibility of content to subscribed/available content only.
- 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 or chapter.
- Users must be able to easily 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.
- Where multiple entitlement types exist (OA, Free, Subscribed), the highest level indicator should reflect the highest privilege of access – for example, in the case above where a user has access to both subscribed and unsubscribed content, the top level link should indicate that the item contains subscribed content.
- Pay-Per View and paid print on demand options should never obscure or override library-provided access to content.

- For licensed materials, the path to access the content should be the default path.
- For non-licensed content, a link to UC-eLinks, UC's link resolver, should be dominant on the page.

5.6 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.

5.7 USABILITY

When selecting information services vendors on behalf of the entire University of California, the CDL prefers vendors who follow good UI design practice.

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.

REFERENCES

U.S. Dept. of Health and Human Services, The Research-Based Web Design & Usability Guidelines: http://guidelines.usability.gov/

5.8 INSTITUTIONAL CUSTOMIZATION

5.8.1 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.

5.8.2 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.
- Branding should be customizable at the campus-level.
- Branding text and graphics should 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

Preferred campus names and graphics for Interface Branding:
http://www.cdlib.org/services/collections/branding.html

5.8.2.2 CAMPUS NAMING CONVENTION

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

5.8.2.3 BRANDING WITH GRAPHICS

Graphics should be clickable to go to a specified URL.

5.8.2.4 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, a mechanism for displaying this functionality should be customizable for each campus and easily accessible from all pages.

5.9 ONLINE HELP

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 (i.e., specific to the situation or action just taken).
2. Easy to navigate between Help and previous activity.
3. Database specific: Help should only describe options that apply to the selected database. It should be clear when a feature is generic to the platform vs. specific to a database.
4. 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.
5. Glossary: The user should be able to locate the definition of a specific term; the glossary should be easy to discover.
6. Error messages: Messages should be comprehensible and helpful; for example, a search that returns zero results should include display of search tips.
7. 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.
8. Feedback: The option for the user to provide feedback should be highly visible.

5.10 LIBRARIAN MATERIALS

1. A section for institutional subscriber / librarian information should be clearly available from the top level landing page.
2. Adaptable training materials: The vendor should provide materials such as online user guides that are adaptable by the home institution.

5.11 COMPLIANCE WITH THE AMERICANS WITH DISABILITIES ACT (ADA)

The University of California is committed to supporting an information technology environment that is accessible to all, and in particular to individuals with disabilities. To this end, the University seeks to deploy information technology that has been designed, developed, or procured to be accessible to people with disabilities, including those who use assistive technologies. A UC systemwide UC Information Technology Accessibility Policy was approved and is effective as of August 27, 2013.

Preferred vendors will comply with the Americans with Disabilities Act (ADA) in a manner consistent with the WCAG 2.0 level AA for products/services with Web or Internet access and Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) for telecommunications products; video and multi-media products; self-contained, closed products.

Vendors will affirm their compliance via inclusion of the Disability Compliance clause in the signed license. Vendors should provide a current completed Voluntary Product Accessibility Template (VPAT) to demonstrate compliance with the federal Section 508 standards. Disclosure of noncompliance as well as a clear timeframe for compliance should be included.

The CDL reserves the right to conduct real-world testing of a vendor's product or services to validate claims regarding compliance to affirmed standards and guidelines. If the product does not comply, the CDL and the campuses will have the right to adapt the Licensed Materials in order to comply with federal and state law and University of California policy.

Information about the University's electronic accessibility initiative and information about the VPAT, WCAG 2.0 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/

VPAT Information and Voluntary Product Accessibility Template: http://www.itic.org/public-policy/accessibility

UC Information Technology Leadership Council: http://www.ucop.edu/information-technology-services/initiatives/information-technology-leadership-council.html

Electronic Accessibility at the University of California: http://www.ucop.edu/electronic-accessibility/

UCOP Procurement: http://www.ucop.edu/procurement-services/policies-forms/index.html (UC Terms & Conditions for Goods and Services)

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 (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 resource(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.

If the vendor has made the decision to enable resource access via a vendor-maintained and authorized user account, this should be implemented, managed, and subject to the licensing exceptions as listed in section 4.3.5 “Vendor Managed Authentication”.

In all cases, accounts used for accessing personalized functionality should not require librarian intervention to implement or maintain.

Methods for allowing users to self-register may vary as long as they generally conform to current secure user name and password standards and provide a mechanism for users to retrieve/reset both forgotten passwords and user names.

5.13 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

5.13.1 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) are 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.

5.13.2 **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 FOR NEWLY ACTIVATED RESOURCES

To set up a new account, the vendor should provide the following information. This is a minimal list of the information needed to begin evaluation testing and activation confirmation.

- Date access is scheduled to begin.
- Any high level network configuration requirements (port settings, proxy configuration requirements.)
- Vendor technical contact (including email address and phone number) for problems and questions.
- The account number and administrative username and password. If no institutional administrative interface is supported, provide a vendor contact for platform configuration.
- URL for access to a menu of all UC licensed databases on the platform, if applicable.
- URL(s) for access to each database licensed; if the URLs are campus specific, the campus specific URLs should be supplied.
- For title or item-level content, provide a full title list as compliant with the KBART standard, including
    - Title Name
    - ISSN / ISBN
    - Coverage Details (if applicable):
        - Initial volume/issue with full-text, including month/year (YYYYMM)
        - For closed titles, ending volume/issue, including month/year (YYYYMM)
    - 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
    - Title level URLs for each journal, or instructions for creating them
- If the full set of content is not accessible (not yet published or back years are still being loaded), the date when content is scheduled to be complete.
- Underlying platform used in the case of full text providers (for example, Highwire, Atypon, Metapress, Ingenta.)
- Information about any material excluded from the digitized version such as missing content, illustrations.
- If client-side software or plugins are required, information on the plugin version supported, and a link to installation instructions or documentation for functionality and limitations should be supplied.

Additional questions to inform the negotiation, licensing and lifecycle management processes are requested separately by the negotiator(s) at negotiation time.

REFERENCES

KBART: http://www.niso.org/workrooms/kbart

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 to a vendor, 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

If a web form is used for submitting incidents to the vendor, a copy of the web form text should be emailed to the reporting person upon submission.

In addition, it is desirable to include a ticketing system incident code for future inclusion in the subject line and an option to include the ticketing software email address in the report.

6.3 NOTIFICATIONS FROM VENDORS

6.3.1 Downtime

Notification shall be provided to the CDL Support Team list preferably two weeks in advance of any downtime that is scheduled 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.

For additional information expected uptime obligations, please see High Availability Services (4.1.1).

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.

In addition to the official breach contact in the license, the vendor should immediately report any suspected irregularity to cdlsupport-l@ucop.edu or 510-987-0555.

REFERENCES

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

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 of the academic year, as well as causing minimal disruption to the academic calendar.

- 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.

  For Ejournals, Ebooks and other resources licensed per-title, the following notifications should be provided:

  - If not all titles are available on initial activation, automatic notification 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

- Transitions: Changes in delivery, including access mechanism, platform, 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 at all entry points of the website, top level URL, resource landing, title landing and article/chapter (if applicable).

- User interface changes: This includes changes in format, display and indexing of the content and adding new features and functionality.
- 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.
- Changes affecting user account data: Any changes that incur potential user data loss such as non-migration of user accounts that contain annotations, saved searches or individually purchased content.
- 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.
- 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/services/collections/rl/roster.html

6.4 ADMINISTRATIVE MODULE ACCOUNT

The CDL prefers one systemwide login that provides full access to all related campus-level subaccounts. This provides the ability to move quickly between campuses when updating settings.

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 the vendor with 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 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 most current release of the COUNTER Code of Practice for journals, databases and books, as well as multimedia content after December 31, 2013.

CDL principles strongly advise against licensing electronic products for which no usage statistics are provided.

Statistics should be reported separately for each UC campus and the Office of the President, as well as our two associated national laboratories (Ernest Orlando Lawrence Berkeley National Laboratory [LBNL or LBL] and Lawrence Livermore National Laboratory [LLNL] where applicable). Consortium-wide statistics should be provided in addition to campus-level statistics.

Reports should be made available on a monthly basis via a password-controlled website. The consortium administrator account must be able to access both the consolidated consortium level usage statistics and the usage statistics for individual campuses, from a single login (using the same user id and password). In addition, these data should be available as a text or comma separated flat file, or as an Excel spreadsheet. COUNTER usage reports must also be provided in XML format in accordance with the COUNTER XML schema specified by SUSHI and documented on the NISO/SUSHI website.

Where vendors discover (or independent audit reveals) errors in vendor-provided usage reports, such errors must be corrected within three months of their discovery, and customers informed of the corrections.

REFERENCES

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

NISO Standardized Usage Statistics Harvesting Initiative (SUSHI): http://www.niso.org/workrooms/sushi

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) must 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.

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. Supplements should be made available online at the same time as the main issue. 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.

For all media, we expect complete content. If the content has been altered from the original recording, it needs to be clearly indicated.

Missing material (e.g., articles and images) that should have been included should be added in a timely fashion at no additional cost.

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.

7.6.1 Backfiles

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

7.7 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.

7.8 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.

The page containing the errata should have a link back to the original item and a link to the errata page should be available from the original item.