Draft Script / API Approval policy

Summary: SCLS would like to support the development of scripts, browser extensions, APIs, etc. to improve certain aspects of the SCLS shared ILS. SCLS has the responsibility to protect the data in the shared ILS (particularly patron data), though SCLS shall have no responsibility or liability for or arising from any loss of data or by Library or arising from any Library equipment, network, or system (per the Agreement to Participate in Technology Services). If a library writes a browser extension, script or API or contracts with a third party vendor outside of SCLS for such a product, it must be shared with SCLS for review. The following procedure must be followed for all types of scripts, browser extensions, APIs, non-SCLS supported third party products, etc. that access Koha.

The term script in this document refers to scripts, browser extensions, APIs, database connections, etc.

1. Library has idea for script (etc.) they would like to develop and maintain.
2. Once script is written SCLS staff will do a preliminary review, with assistance from the creator, to identify what we would see as potential security issues such as automatically logging in to the shared ILS; where the script is hosted; who is accessing it (patrons or staff), etc. If no such issues are identified, the library may move forward.
3. If SCLS staff determines there is an area of concern in the script, it will be submitted to a third party vendor selected by SCLS for review of potential security issues. The library will be responsible for the costs incurred by the review.
4. Once the script is vetted and approved by the third party vendor, the library may move forward or not. If the vendor does not approve, the library may take steps to rectify the security issue(s).
5. SCLS will not be responsible for supporting any script (etc.) if it is not integrated into the main shared ILS software solution.

Draft Policy for Accessing the SCLS Shared ILS

1. SCLS is not liable for security breaches related to a member-library's unauthorized access and/or use of data in the SCLS shared ILS.
2. Libraries are responsible for establishing a method of distributing login information to staff and for changing passwords on a regular basis and after a staff member leaves employment at the library.
3. Libraries should establish their own policies and procedures for preventing their staff from having unauthorized access and/or use of data in the SCLS shared ILS.