SCKLS Wireless Printing Policy

Wireless printing to a wireless printer or utilizing WiFi printing to a wired network printer carries inherent risks. Without adequate network security measures in place, your library may be exposed to potential vulnerabilities.

1. Any WiFi connected user has access to print freely, at any hour of the day, which could result in:
    a. Hundreds of unwanted/unclaimed print jobs that consume paper and toner.
    b. Print jobs depicting undesired or illegal images or text.

2. Potential network security vulnerabilities may arise from the rules implemented for WiFi printing, which could jeopardize the integrity of the network.

After evaluating the risk versus benefit factors, SCKLS will not support or configure wireless printing using the aforementioned methods and will be removing these firewall rules from all SCKLS supported networks. If your library considers wireless printing to be essential, we recommend:

a. Exploring more secure subscription solutions for wireless printing, such as those offered by *Cybrarian, EnvisionWare, LibData, Princh*, and other wireless printing vendors (SCKLS may assist)

b. Managing library network in-house

c. Migrating to a third-party managed solution provider that offers alternative solutions

Services and support provided by SCKLS for any software or hardware product should not be interpreted as an endorsement of either the vendor or the product.

Questions regarding this policy should be directed to one of the following SCKLS staff:

a. SCKLS Director of Information Technology
b. SCKLS Automation and Technology Services Coordinator
c. SCKLS Network Services Coordinator