Best Practice for at Home Network security and Printing Sensitive Data on Non-COSA owned printers

The purpose of this document is to provide best practice network security and guidance for COSA employees and non-employees who engage in remote work that require printing of Agency-Sensitive data or Sensitive Personally Identifiable Information (PII) on non-City owned printers. Definitions and examples are in AD 7.3a Data Security. Many of the recommendations provided here are taken from NIST SP 800-114 Rev. 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security.

Health Care and Criminal Justice Data is regulated and cannot be stored or printed on personal computers or printers. For other types of data, consider foregoing printing to hard copy in favor of saving to PDF output for sharing or later printing on a COSA device if printing is necessary.

Best Practices for Securing Home Network and Devices

- Remove or shutdown all connections and devices from your home network when not in use.
    - Out of sight out of mind, if hackers were to access your home network and there are no active devices, they will just leave.
    - Turn on your devices only when needed. Saves electricity and prevents hackers from getting into your systems that are on/activated.
    - Disconnect personal and City devices used to access COSA network from your home network and only connect them when Internet is required.
- Router and Wi-Fi Network passwords
    - Ensure you use strong passwords (upper and lower case, numbers, special characters, at the very minimum 8 characters, 12 is preferred).
    - Change passwords every 3-4 months.
- Routinely update your personal device firmware, systems, Microsoft, Apple and other software send out regular updates/patches.
    - These are likely to fix vulnerabilities in your Operating Systems and various supporting software such as Acrobat, Flash, and others.
    - Maintain up-to-date anti-virus and malware protection applications.
    - Keep up with your knowledge of what you have. News come out all the time about systems that may have been manufactured with vulnerabilities.
- Insure that your City Device has been connected to the COSA network to receive updated patches and security tools.

Home printers/Personal printers connected directly to computer

1. Disconnect your printer USB cable from your computer. This simple technique will isolate your printer from being searched in case your computer is compromised.
2. Shut down your printer and clear its volatile memory. Most home or personal printers have only volatile memory which means turning it off will clear its memory. Following the practices below will help to avoid compromising your system. (flushing the memory)
3. Secondary flushing of the printer memory by printing non-sensitive documents until your printer memory does not contain the job that contained sensitive protected data.

For Bluetooth connected printer:

Disconnect the printer from Bluetooth, disable Bluetooth function and follow the procedures above.

For Wi-Fi Connected Printer:

Follow the above procedure and turn off your printer to disconnect from the Wi-Fi.
If you wish to leave your Printer connected to your Wi-Fi for availability you need to "flush" the memory using printing other unclassified documents or maintenance memory flush.
General at home Wi-Fi connection precautions

- It is BEST to only allow KNOWN devices to connect to your home Wi-Fi.
- Limit the number of connections to the devices you have. For example, you know you have 12 known devices that connect to your network, so limit your router to only 12 device connections.
- Ensure that your printer setting is in energy safe mode, so it is turned off and do not allow remote waking function. Only allow turning back on using on/off button.