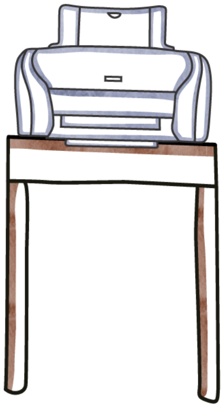
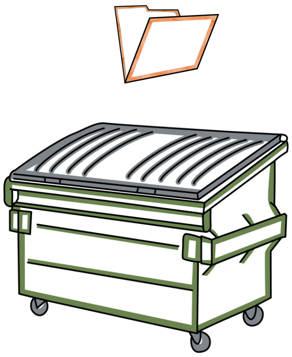
Office of the Chief Information Security Officer
Risk Advisory: Multifunction Devices

BEST PRACTICES

If you lease or manage a copy machine, printer, fax or other multi-function device for your department, the Office of the Chief Information Security Officer (CISO) encourages you consider the following:

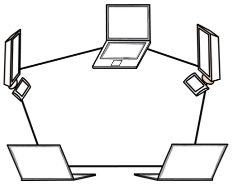
- **Passwords:** Passwords should be changed from default manufacturer or contractor default to something unique that is not used for any other equipment.
- **Physical Access:** Multifunction devices should be protected from unauthorized access and only used by authorized personnel. Closely monitor and promptly remove documents, especially those that contain confidential data.
- **Paper Jams:** Remove all documents when clearing a paper jam. For added security, run a blank copy after a paper jam, to ensure that no confidential data is left in the machine.
- **System Access:** Limit the number of people who have access to make configuration changes.
- **Secure Data:** If the device is able to store information and is used to copy confidential data, configure it to securely erase the data after a document is copied.
- **Patching:** Apply manufacturer patches or updates in a timely manner.
- **Lease:** If the device will be used for confidential data, include data security terms and conditions.
- **Disposal/Surplus:** Securely erase or remove the hard drive when the machine is surplussed or returned to the lessor.



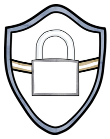


Office of the Chief Information Security Officer
Risk Advisory: Multifunction Devices

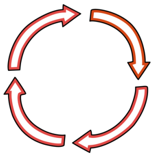
If the device has networking capability, then there are additional risks entailed. Network connectivity provides a remote attack vector to potential malicious actors. If you have a network connected device we encourage you to consider the following:



- **Remote Access:** A firewall should be used to limit both inbound and outbound network traffic to authorized and intended users only.
- **Web Console:** Many devices come with a web console for remote management; login and password should be changed from the default settings to something unique that is not used on any other device.
- **Private IP:** Use a private IP address, not internet-routable or discoverable from outside of the UW network.



- **Secure channels:** Encryption or other secure transmission channel should be used for sending and receiving data on multifunction devices.
- **Auditing and monitoring:** Review device logs and monitor network traffic as part of the operational administration of multifunction devices, especially for devices that send and receive confidential information.



- **Short retention cycle:** Do not let multifunction devices turn into unintended unmanaged file servers. Consider configuring the device (if possible) to delete stored after a few hours and limit the duration of deferred printing.

This list is not exhaustive. Other information security configurations and recommendations may apply to the particular device that you manage.

For additional information, consult with your department IT support person. For instructions on how to implement the above recommendations, please refer to the user manual for the device or consult with the device provider or manufacturer.

RESOURCES

Private Network Addressing

help@uw.edu

Office of the CISO, March 2016