OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

Information Security Risk Advisory
Multi-Function Devices (Copier, Printers, Faxes)

Copy machines, printers, and faxes have evolved from mechanized tools to digital combined multi-function devices with storage that may retain confidential data - such as payroll information, student information, or protected health information - that warrants careful protection by law or UW Policies. Modern multi-function devices may be vulnerable to some of the same data security breaches as other computing technology.

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: multi-function devices should only be used by authorized personnel and protected from unauthorized access. 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 sent to surplus or returned to the lessor.

If the device has networking capability, confidential data may be exposed to additional risks. Network connectivity increases the potential of malicious actors gaining unauthorized access to confidential data. If you have a network connected device we encourage you to consider the following:

- Malware: To reduce the risk of exploit and compromise to a multi-function device all of the below recommendations should be followed.
- Remote Access: A firewall should be used to limit remote access if the machine needs to be accessed outside of the UW's network.
- Web Console: Many devices come configured with default passwords for services, such as web or console management; these should be changed to something unique that is not used on any other device.
- Private IP: Consider using a private IP address in order to protect from unauthorized access and/or configuration.

- Sending Data To: Confidential data should be sent over secure channels in order to reduce the risk of unauthorized third parties gaining access it.
- Sending Data From: Data sent from the device should only go to intended parties, and, if confidential, should be sent over secure channels.

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:

Data Security Agreement
help@uw.edu