The IT Security Office has monitored an increase in attacks that exploit printer technologies and the tendency for printing devices to be kept less secure than other IT components. The recommendations found below will help achieve compliance with Policy 7010 - Policy for Securing Technology Resources and Services and should be considered for any networked printing device. Without proper configuration, the following attacks and misuse are possible:

- Sensitive data loss and theft through printer memory access and print job capture,
- Device availability and uptime,
- Data integrity,
- Printer toner consumption rate,
- User impersonation,
- Targeted phishing attacks augmented by background information gained from printer meta and log data or its embedded web interface,
- Device misuse as a file server or remote storage device.

# Security Recommendations

- IP Filtering is Paramount
    - If IP filtering is in place, either on the device itself or provided by an external, in-line component, almost all of the security threats mentioned above are thwarted if originated from external actors.
    - The ITSO recommends IPv4 filter restrictions to *at least* the ranges shown below. Both CIDR notation and the corresponding IP ranges will be listed below for ease of configuration. If IPv6 is not used but the printer has an IPv6 filter, it should be *ENABLED* and configured to *DENY ALL* traffic.

| CIDR Notation | IPv4 Start | IPv4 End |
|---|---|---|
| 128.173.0.0/16 | 128.173.0.0 | 128.173.255.255 |
| 198.82.0.0/16 | 198.82.0.0 | 198.82.255.255 |
| 172.16.0.0/12 | 172.16.0.0 | 172.31.255.255 |

This will restrict IPv4 communication with your printer to any on-campus source, including VT wireless and VPN connections.

| CIDR Notation | IPv6 Start | IPv6 End |
|---|---|---|
| 2607:b400:20::/44 | 2607:b400:20:0:0:0:0:0 | 2607:b400:2f:ffff:ffff:ffff:ffff:ffff |
| 2001:468:c80::/48 | 2001:468:c80:0:0:0:0:0 | 2001:468:c80:ffff:ffff:ffff:ffff:ffff |
| 2607:b400::/40 | 2607:b400:0:0:0:0:0:0 | 2607:b400:ff:ffff:ffff:ffff:ffff:ffff |

This will restrict IPv6 communication with your printer to any on-campus source, including VT wireless and VPN connections.

- PCL is Recommended and PS and PJL should be *disabled* if not explicitly needed.
    - Data gathered from vulnerability tests shows that the PCL is the least-vulnerable printer interpreter language. When possible, PCL should be used and PS and PJL should be disabled.
- Printer Web Service Access should be Restricted and Secured
    - An unsecured web service on a printer allows extensive information to be gathered by an attacker, even without administrative access to the device. Web access should require an encrypted connection and secured with strong administrative credentials.
    - Confirm that the IP filtering on the device also applies to the Web Service. If not, the printer should be treated as though it does not have any built-in IP filtering. In this case, see the response to "What if my printer doesn't have any built-in IP Filtering?" below for alternatives and configuration details.
- Simple Network Management Protocol (SNMP) should be Restricted or Disabled
    - Older versions of SNMP are vulnerable. SNMP should either be disabled or restricted to SNMPv3, and the credentials should be explicitly configured.

## What if my printer doesn't have any built-in IP Filtering?

The ITSO currently recommends an in-line external device solution similar to one developed by Dominik Borkowski. This is a low-cost (~$50) option. Details on implementation can be found here:

https://devlab.vbi.vt.edu/dom/edgeos_printer

## What if I need to use PostScript (PS) or Printer Job Language (PJL)?

If you have an explicit need to run PS or PJL, be aware that anyone who has access through the printer's IP filtering can potentially exploit vulnerabilities in those printer interpreter languages that may allow them to print, change device settings, use the printer for file storage, add unwanted content (graffiti and overlays) to print jobs, or send unwanted print jobs to the device without creating an event in the printer's logs. In this case, it is recommended to use a print server or implement print job tracking as potential mitigating security controls.