Archdiocese of Seattle

October 26, 2026

Lock Down Access: Advisory for Parishes and Schools

Oct 24, 2026 · @Kevin F. Benz

Summary

Every parish and school must follow two rules for its network-connected equipment:

1. **No login page on the public internet.** The setup or login page of a router, firewall, camera recorder, printer, door controller or similar device must not be reachable from outside your building.
2. **Older equipment on its own network.** Devices that no longer receive security updates, and devices such as cameras and building controls, must sit on a separate, secured part of the network, apart from staff and student computers.

Attackers run automated scans of the whole internet, looking for exactly these login pages. Many of them still use the factory password, or run software with known flaws that will never be fixed. One exposed device can let an attacker into the rest of the network.

As with the earlier advisories in this series, you do not need to do the technical work yourself. Your job is to send the request, ask the questions below, and keep a written answer.

Rule 1: Keep Login Pages Off the Public Internet

Most exposed login pages were opened on purpose, usually so a vendor or staff member could reach a device from home. The convenience is real, but the same page is open to everyone else on the internet.

Device	How it is often exposed	Why it matters
Router or firewall	"Remote management" turned on	Whoever controls it controls the whole network

Device	How it is often exposed	Why it matters
Camera recorder (NVR or DVR) and cameras	Port forwarding so staff can watch from a phone	Recorders are among the most attacked devices online, and many run old software
Door access and alarm panels	Vendor remote access left open	Physical security of the building
Printers and copiers	Web page or scan-to-email reachable from outside	Stored documents, address books and email passwords
Thermostats, HVAC, bell and PA systems	Installed by a contractor with remote access	Often never updated after installation
Network storage (NAS) and servers	Remote file access turned on	Records, backups and a common target for ransomware
Wireless access points and switches	Management page opened to the internet	A path to every device on the network

The safe way to reach equipment from outside:

- Use a VPN, the device maker's cloud management service with two-step sign-in, or a remote-support tool that the vendor starts only while you are watching.
- Turn off port forwarding and remote management on the router for every device that does not need it.
- Change every factory password, and use a different password for each device.

Rule 2: Put Older Equipment on Separate Networks

A single flat network lets any device talk to every other device. If an old camera recorder is compromised, the attacker can then reach the bookkeeper's computer. Separate networks, often called VLANs or sub-networks, stop that spread.

Your technical help can set these up on most business-grade routers, firewalls and wireless systems. A typical arrangement for a parish or school:

Network	What goes on it	What it may reach
Staff	Office computers, the finance computer, staff laptops	The internet and shared printers
Students (schools)	Student Chromebooks, tablets and lab computers	The internet only, through the school's content filter
Guest Wi-Fi	Visitors, parishioners, personal phones	The internet only
Building and security devices	Cameras, recorders, door access, HVAC, bell and PA systems	Only the vendor services they need; nothing on staff or student networks
Older equipment	Devices past their end-of-support date that cannot be replaced yet	Nothing beyond what the device strictly requires; no internet if possible
Network management	Router, switch and access point management pages	Reachable only from a named staff computer or the VPN

Older equipment means any device whose maker no longer releases security updates. Your equipment inventory should list its end-of-support date. Isolation buys time; it is not a permanent fix. Put each such device on a replacement plan with a target year.

Who Does What

Role	Responsibility
Pastor, principal or business manager	Sends the request, approves any equipment purchase, and keeps the written answers

Role	Responsibility
Parish or school technical staff, consultant or volunteer	Closes exposed login pages, sets up the separate networks, and reports back in writing
Security, camera, door access and HVAC vendors	Confirm how they reach their equipment remotely, and change to a safe method where needed
Internet provider	Confirms whether its own modem or router has remote management turned on, when it supplied that equipment
Archdiocese IT	Answers questions, can check your public internet address for exposed login pages, and reviews answers you are unsure about

Vendors who installed equipment often hold the only remote access to it. Ask each of them directly; your general technical help may not know these arrangements exist.

What to Say

Send this message to your technical help, and a shortened version to each equipment vendor. Replace the bracketed parts and ask for a written reply.

> ***Subject: Request: secure remote access and separate networks at [parish or school name]***
>
> *Thank you for supporting our network at [parish or school name].*
>
> *The Archdiocese has asked every parish and school to confirm two things: that no equipment login page is reachable from the public internet, and that older equipment and building devices sit on separate, secured networks.*
>
> *Please reply in writing by [date] with:*

1. A list of every port forward, remote-management setting and vendor remote-access connection on our network, and whether each one is still needed.
2. Confirmation that each one not needed has been turned off, and how the rest are now protected (VPN, cloud management with two-step sign-in, or vendor-started sessions only).
3. Confirmation that the factory password has been changed on every device.

4. A short description of our networks: which devices are on each one and what each network can reach.
5. A list of equipment that no longer receives security updates, where it sits on the network, and a suggested replacement date.

> *If any of this needs equipment we do not have, please tell us what it would cost so we can plan.*
>
> *Thank you, [Your name, title and phone number]*

What to Ask, and What a Good Answer Sounds Like

Question	A good answer	A warning sign
Can anyone on the internet reach a login page on our equipment?	"No. I checked our public address from outside and found nothing open"	"I do not think so" with no check
Which port forwards and remote-management settings are on?	A specific list, each with its purpose, or "none"	"Whatever the installer set up"
How do vendors reach their equipment?	"Through their cloud portal with two-step sign-in" or "Only when we start a session for them"	"They have a permanent connection" or "I do not know"
Have factory passwords been changed?	"Yes, on every device, each with its own password, stored in our password manager"	"On most of them" or "The default is fine because it is inside"
Are cameras and building devices separate from staff computers?	"Yes, they are on their own network and cannot reach staff or student devices"	"Everything is on one network"
Which devices no longer get security updates?	A named list with replacement dates	"Everything still works, so it is fine"
Who else can change the router or firewall?	Named people, each with their own login	A shared login, or former staff or

Question	A good answer	A warning sign
		volunteers who still have access

A device that "still works" can still be unsafe. Age alone is not the problem; the absence of security updates is.

How to Confirm It Is Done

Keep these records with your equipment inventory, in the same secure place:

- The written list of remote-access settings, showing which were turned off and how the rest are protected.
- The description of your networks: which devices are on each one and what each can reach.
- The list of equipment past its end-of-support date, with replacement dates.
- Written confirmation from each equipment vendor about how it reaches its devices.

Two simple checks you can make yourself:

- **From outside the building.** Ask staff how they reach equipment from home, for example a web address the camera installer gave them. On a phone using cellular data, not the building Wi-Fi, enter that address in a web browser. If a login page opens, it is exposed; report it to your technical help. A maker's phone app that connects through the maker's cloud service with two-step sign-in is acceptable.
- **From the guest Wi-Fi.** Join the guest network and try the same pages. They should not open.