

Securely Configuring your PBX

For New Hampshire Schools, PBX security is not just about fraud prevention; it is a critical component of **student safety** and **federal compliance**. Configuring your system correctly ensures you meet legal mandates like **Kari's Law** and the **RAY BAUM'S Act** while protecting sensitive student data.

Securing a **FreePBX** or **VitalPBX** system requires a multi-layered approach centered on strict firewall rules, service isolation, and encrypted communication. The most critical step is ensuring the administration interface is **never exposed to the public internet**.

- ✓ **Enable Direct 911 Dialing (Kari's Law):** Configure the system so anyone can dial **911 directly** from any handset without needing an outside line prefix (like dialing "9" first).
- ✓ **Configure Emergency Notifications:** Set up automated alerts to notify **on-site security** or the front office immediately whenever a 911 call is placed.
- ✓ **Provide Dispatchable Locations (RAY BAUM'S Act):** Ensure every extension transmits precise location data to emergency responders, including the **building name, floor, and room number**.

1 Essential Port Configuration

Service	Default Port(s)	Recommended Action
SIP Signaling (PJSIP)	5060 (UDP/TCP)	Obscure: Change to a non-standard port (e.g., 5454) to reduce bot scanning.
SIP over TLS	5061 (TCP)	Preferred: Use for encrypted signaling instead of port 5060.
RTP (Media)	10000-20000 (UDP)	Limit: Reduce the range based on your maximum concurrent calls (e.g., 100 ports for 10 phones).
HTTP (Admin GUI)	80 (TCP)	Close: Never expose port 80 to the WAN. Use HTTPS (443) only and restrict to trusted IPs.
SSH	22 (TCP)	Change: Move to an obscure high port and whitelist specific administrator IPs.

For both platforms, you should minimize the number of open ports. If a service is not in use (e.g., IAX2), disable its port entirely rather than just changing it.

2 Network Security Best Practices

- **Isolate Voice Traffic:** Place PBX and IP phones on a dedicated **VLAN** to separate voice traffic from standard data, reducing the internal attack surface.
- **Implement Whitelisting:** Configure the built-in firewall (FreePBX Firewall or VitalPBX Firewall) to only allow traffic from **trusted IP addresses** or specific SIP trunk provider IP blocks.
- **Use a VPN:** This is the most recommended method for remote access. Connect remote phones and administrators via **OpenVPN** or **WireGuard** so the PBX remains completely isolated from the public internet.
- **Session Border Controller (SBC):** For public-facing systems, use an external SBC (like Kamailio with dSIPRouter) to filter registration attempts and provide an extra layer of NAT traversal security.

3 System Hardening & Intrusion Prevention

- **Fail2Ban (Intrusion Detection):** Always keep **Fail2Ban** active to automatically jail IP addresses that exhibit malicious behavior, such as multiple failed registration attempts.
- **Geo-Firewall:** Block all traffic from countries where you do not have business operations to eliminate a large percentage of automated attacks.
- **Disable Dangerous Settings:** In Asterisk SIP Settings, ensure **"Allow Anonymous Inbound SIP Calls"** and **"Allow SIP Guests"** are both set to **No**.
- **Encrypted Communication:** Use **TLS** for signaling and **SRTP** for media to ensure end-to-end encryption for calls.
- **Module & OS Updates:** Regularly update the PBX firmware, modules, and the underlying OS (Asterisk, PHP, MariaDB) to patch known vulnerabilities. FreePBX versions 15 and older are now **End of Life** and should be upgraded immediately.

4 Administrative Controls

- **Password Fortification:** Use unique, randomly generated secrets (at least 12+ characters) for every extension and admin user. Never use the extension number as the password.
- **Role-Based Access:** Grant administrative privileges only to essential personnel and use **Multi-Factor Authentication (MFA)** where supported.
- **Outbound Limits:** Implement "Maximum Channels" on trunks and request your SIP provider to disable international calling if it is not required.