# Public Network Risk Mitigation Tips

Use this guide to reduce security risks associated with offering public or employee Wi-Fi access.

## Checklist for Safer Wi-Fi Networks

* ☐ Guest and employee Wi-Fi are on separate VLANs or SSIDs
* ☐ WPA3 or WPA2-Enterprise is enforced for employee Wi-Fi
* ☐ Guest Wi-Fi passwords are rotated regularly or managed with vouchers
* ☐ DNS filtering (e.g., NextDNS or OpenDNS) is enabled for guest traffic
* ☐ Guest access is restricted from local network resources (LAN isolation)
* ☐ Wi-Fi splash pages include disclaimers about usage and monitoring
* ☐ Logs and alerts are monitored for rogue devices or abnormal activity
* ☐ Employee devices on Wi-Fi are covered by endpoint security tools
* ☐ All access points and Wi-Fi controllers have admin credentials secured and updates applied

Tip: Unifi, Aruba, and other business-grade access points typically offer built-in guest isolation and firewall settings. Use them.