

Student Sign-in & Device Security Self-Audit

Accounts

- ☐ Student accounts are in organizational units that match grade or building
- ☐ Departed students' accounts are suspended or archived within a set number of days
- ☐ Staff and student accounts cannot be confused by naming or OU placement
- ☐ Shared or generic logins (kiosks, carts, labs) are inventoried

Devices

- ☐ Managed-device inventory matches what Google Admin reports
- ☐ Unmanaged personal devices cannot sign in to school accounts without review
- ☐ Devices not seen in 30+ days are listed and have an owner
- ☐ Enrollment is forced, so wiped devices come back to your domain

Sign-in and access

- ☐ You can see who signed in from which device, building, and time of day
- ☐ Sign-ins from outside your state or country raise an alert you would actually read
- ☐ Admin and teacher accounts use stronger sign-in than student accounts
- ☐ Unusual access to grade, SIS, or admin tools is reviewed

Response

- ☐ There is a written steps-list for a suspected account takeover
- ☐ There is a written steps-list for a lost or stolen device
- ☐ Someone besides one person can run both steps-lists
- ☐ Incidents are recorded so patterns show up across a school year

Visibility

- ☐ Your team can answer 'which devices are in the building right now?' in minutes

- ☐ Reports exist that a principal or superintendent could read without IT translating
- ☐ You review these checks on a schedule, not only after an incident
- ☐ Everything above is checked automatically or on a calendar, not from memory

Want these checks run for you automatically? Visit userauthguard.com.