

Security system maintenance checklist for Colorado facility managers

Use this checklist quarterly (or after any system incident) to catch maintenance gaps before they become failures. Each item takes minutes to verify. The ones you skip are usually the ones that cause problems later.



Access control

- ☐ **Test card readers at all entry points.** Swipe or tap a credential at every reader and confirm the door unlocks within 2 seconds. Flag any reader that requires multiple attempts.
- ☐ **Check door hardware.** Push and pull each controlled door to confirm the lock engages fully when closed. Listen for grinding or delayed engagement from the mag lock or electric strike.
- ☐ **Verify remote lockdown.** Trigger a lockdown from the management console and confirm every controlled door responds. Time how long full lockdown takes.
- ☐ **Review credential lists.** Pull the active credential report and compare it against your current employee roster. Deactivate any credentials assigned to people no longer with the organization.
- ☐ **Test emergency egress.** Confirm that request-to-exit devices (REX sensors, push bars) release doors immediately. This is a fire code requirement in Colorado, not optional.
- ☐ **Check battery backups on wireless locks.** Battery-powered locks (Salto, wireless ASSA ABLOY) should report battery status in the management software. Replace any batteries below 30%.

Video surveillance

- ☐ **Verify all cameras are online.** Open the video management software (Genetec, Avigilon, or equivalent) and confirm every camera shows a live feed. Check for any “camera offline” alerts that have been ignored or muted.
- ☐ **Review image quality on perimeter cameras.** Pull a still frame from each exterior camera and confirm you can read a license plate or identify a face at the expected distance. Night images degrade faster than daytime, so check after dark.
- ☐ **Confirm recording retention meets your policy.** Verify that your oldest stored footage matches or exceeds your retention requirement (30 days is common for commercial facilities in Colorado). If storage is filling up early, you have a resolution, bitrate, or drive issue.
- ☐ **Clean camera lenses and housings.** Exterior cameras in Northern Colorado collect dust and pollen in spring and summer, salt residue in winter. A dirty lens degrades image quality slowly enough that nobody notices until an incident review.
- ☐ **Test pan-tilt-zoom cameras.** If you have PTZ units, run each one through its full range of motion. Confirm presets return to the correct position. Mechanical wear on PTZ motors causes drift over time.
- ☐ **Check for firmware updates.** Camera firmware updates address security vulnerabilities and stability. Log into the VMS and check each camera's firmware version against the manufacturer's current release. Axis and Avigilon both publish release notes on their support portals.

Intrusion detection

- ☐ **Walk-test every motion sensor.** Put the panel in test mode and walk through every sensor's coverage area. Confirm each sensor triggers. Sensors mounted near HVAC vents or in direct sunlight are the most likely to drift out of alignment.
- ☐ **Test all door and window contacts.** Open and close each protected door and window. Confirm the panel registers the zone change.
- ☐ **Verify central station communication.** Trigger a test signal to your monitoring center and confirm they receive it. If you use both primary and backup communication paths (IP and cellular), test each path individually.
- ☐ **Test the keypad and all user codes.** Every code assigned to a user should arm and disarm the panel. Remove codes for anyone who no longer needs access.
- ☐ **Check backup batteries.** Panel batteries have a 3 to 5 year lifespan. If yours are older than 3 years, test under load. A battery that shows full voltage at rest can fail under load during a power outage.

Fire alarm

- ☐ **Confirm the panel shows no trouble conditions.** A trouble light that has been on for weeks is easy to ignore. Every trouble condition is a potential inspection failure.
- ☐ **Test notification appliances.** Activate a test signal and confirm all horns and strobes in the building respond. Walk the full building during the test.
- ☐ **Verify pull station functionality.** Test at least one pull station per floor to confirm it triggers the alarm and communicates to the monitoring center.
- ☐ **Check sprinkler system tamper switches.** If your fire alarm monitors sprinkler tamper and flow switches, confirm both report correctly to the panel.
- ☐ **Review your inspection schedule.** Colorado requires fire alarm inspections annually at minimum, with some occupancy types requiring semi-annual testing. Confirm your next scheduled inspection date and that your records are current for the fire marshal.

Network and infrastructure

- ☐ **Inspect rack and cable runs.** Check for loose patch cables, overloaded switches, and cables that have been pinched or bent beyond their minimum bend radius. A single bad cable run can take a camera or reader offline intermittently, making it hard to diagnose.
- ☐ **Verify UPS battery health.** Uninterruptible power supplies protecting your head-end equipment have batteries that degrade. Most UPS units display battery health on the front panel. Replace batteries that show less than 80 percent capacity.
- ☐ **Confirm network segmentation.** Security devices should be on their own VLAN, separated from general business traffic. If an IT change merged them onto the shared network, camera bandwidth can cause slowdowns, and the security system is exposed to threats on the business network.
- ☐ **Test remote access.** If facility managers or security staff access the VMS or access control platform remotely, confirm that connection works. Failed VPN certificates and expired remote access credentials are common causes of lost remote visibility.



Documentation and compliance

- ☐ **Update your as-built drawings.** If any devices have been added, moved, or removed since the last update, mark the changes. Accurate as-builts save hours during service calls and are required for some compliance frameworks.
- ☐ **Collect and file all service records.** Every service visit, firmware update, and component replacement should be documented. CJIS-compliant facilities in Colorado are required to maintain these records. Healthcare facilities under Joint Commission review need them as well.
- ☐ **Review user access levels in management software.** Administrative access to the VMS and access control platform should be limited to people who need it. Remove admin rights from anyone who has changed roles or left the organization.

When to call your integrator

Some of these items are facility manager tasks. Others (firmware updates, panel reprogramming, sensor realignment, central station communication troubleshooting) are integrator work. If you're finding problems on this list that you can't resolve in-house, a scheduled maintenance visit from your integrator covers most of them. Facilities with a service agreement get these checks done proactively instead of discovering issues during a self-audit.

ESI Technologies services commercial security systems across Northern Colorado (Fort Collins, Loveland, Greeley, Windsor, Longmont) and Southern Colorado (Colorado Springs, Pueblo, Monument, Castle Rock). Call **(970) 999-1681** (Northern CO) or **(719) 602-7336** (Southern CO) to schedule a service visit or ask about a maintenance agreement.