FREE RESOURCE · VERSION 1.0

The Cannabis IT Readiness Checklist

15 questions every dispensary, cultivator, and processor in a METRC state should be able to answer about their technology and compliance, with a red, yellow, and green rubric and the single next step to take for each one.

~20 minutes
to complete

15 questions
across 5 domains

Scored
so you know what to fix first

HOW THE RUBRIC WORKS

For every question you will see three answer bands. Mark the one that matches your business today.

Green: you are in good shape **Yellow: worth fixing soon** **Red: address this first**

KawaConnect is an IT consulting firm serving Pittsburgh, Cleveland, and the Tri-State area. Questions? Call **(412) 556-7007** or email **support@kawaconnect.com**. No sales pitch inside.

1. Cannabis labeling and compliance

Three questions on the labels, COAs, and per-state rules that we deal with directly through Tagestry. Get these wrong and a routine inspection becomes a hold notice.

Q1. Are METRC labels printed through a validated integration that records who printed what, when, and from which template?

Green Tagestry, with every print logged to a package UID, mislabels are recoverable, and audit trails go back the full retention window.

Yellow Generic label software with manual METRC field entry. Misprints occasionally cause holds.

Red Hand-typed labels or screenshots from METRC pasted into Word.

Next step: Move to Tagestry. METRC-validated, native data sync, audit log per print, and it covers all 28 METRC jurisdictions out of the box.

Q2. Are Certificates of Analysis (COAs) linked to specific METRC packages and to the menu the customer sees?

Green COA PDFs auto-attach to packages on receipt, menu QR codes resolve to the right COA per batch, the linkage survives a label reprint.

Yellow COAs in a Google Drive folder. The right COA per package requires a manager to look it up.

Red Customer asks for a COA, staff guesses.

Next step: Wire COAs to package UIDs, not to SKUs. Tagestry stores the COA reference on the print itself, so a relabel never breaks the link.

Q3. If you operate in more than one state, do you maintain a per-state compliance matrix (tag rules, retention, reporting)?

Green A living document covers the differences across each METRC state you hold a license in. Staff training is state-specific.

Yellow You assume the rules are similar enough. Surprises happen at audits.

Red Multi-state operator running single-state SOPs.

Next step: Build a state-by-state matrix. Tag formats, retention windows, and inspection cadences differ. Tagestry abstracts the label half of this for you.

2. Market intelligence and competitive data

Three questions on what you can see about the market outside your own four walls. These are the questions PryceHawk was built to answer.

Q4. Do you need to view your products (and your competitors' products) across multiple dispensaries, or pull data for an entire state?

Green You query a market data feed (PryceHawk / CannQuest API, BDSA, Headset) by brand, SKU, or product across hundreds of stores in a state, with daily refresh.

Yellow A staffer opens a few competitor menus by hand on Monday and writes notes.

Red You see your own menu only. The market is a black box.

Next step: PryceHawk currently tracks roughly 900 dispensaries across Ohio and Michigan on nine platforms. A read-only API key gives you cross-store visibility without anyone clicking around.

Q5. Do you know when a competitor cuts price or runs a new promo on a product you also carry?

Green Daily undercut and discount alerts on the SKUs that matter to you. The buyer adjusts before the customer notices.

Yellow You find out when a regular tells you "the place down the street is $5 cheaper."

Red No competitor price tracking at all.

Next step: Subscribe to a retail competitor report (PryceHawk emails undercut analysis, discount breakdowns, and THC comparisons by store). Even daily alerts on your top 50 SKUs change buying behavior.

Q6. For your cultivation or wholesale arm, do you track which dispensaries pick up new brands and which let them lapse?

Green Daily wholesale tracker (brand inventory across stores, new-listing and delisting alerts) feeds the rep team's Monday standup.

Yellow Reps ask buyers in person and trust the answers.

Red You learn a chain dropped your brand months later.

Next step: A wholesale presence report (PryceHawk tracks new listings, delistings, and shelf coverage per brand company) catches drift before it becomes a churn problem.

3. Video surveillance and physical security

Q7. Does video retention meet the strictest state rule applicable to any of your licenses?

Green Retention sized for the strictest license: Pennsylvania up to 2 years, Ohio at least 6 months, Oregon 90 days on-site plus 30 off-site, with 1080p+ on regulated areas.

Yellow Retention meets the loose state but you also hold a stricter-state license.

Red Retention is whatever the recorder defaults to.

Next step: Audit retention against every state where you hold a license. Resize storage if any gap exists. NVR storage is cheap; a license suspension is not.

Q8. Are camera outages detected and alerted automatically, with logs retained for inspections?

Green NVR sends health alerts to ops; outages logged with start/end timestamps. Maintenance log goes back at least a year.

Yellow Outages are noticed when someone reviews footage and finds a gap.

Red No monitoring. A regulator notices first.

Next step: Most modern NVRs (Verkada, Eagle Eye, Hanwha Wisenet) have built-in health alerting. Turn it on, route to a monitored inbox.

Q9. Can you produce authenticated video exports for a regulator within their stated deadline?

Green Tested export workflow. Authenticated MP4 with hash, timestamps preserved. Manager has done it for a regulator inquiry without panic.

Yellow Export works in theory, no one has done a real one in a year.

Red You would Google "how to export from this DVR" the day a regulator asks.

Next step: Run a quarterly export drill. Save the runbook to the same folder as the SOPs.

4. Network segmentation and cybersecurity

Q10. Are POS, cameras, compliance machines, and guest Wi-Fi on separate VLANs with ACLs?

Green Layered design: VLAN 10 corporate, 20 POS, 30 METRC/compliance, 40 cameras, 50 guest. Inter-VLAN traffic is denied by default.

Yellow A guest SSID exists, everything else is on one flat LAN.

Red Single flat network. The guest who connects to Wi-Fi can ping the POS.

Next step: Modern firewalls and managed switches (Ubiquiti UDM, pfSense + UniFi, Meraki MX) make this an afternoon project at a single store.

Q11. Is MFA required on POS admin, METRC, banking, email, and every regulator-portal login?

Green MFA enforced. Phishing-resistant on admin and METRC accounts where the platform supports it.

Yellow MFA on email, password-only on POS admin and METRC.

Red Shared budtender logins, password posted on the back-of-house wall.

Next step: Per-employee POS accounts and MFA on every admin role. Cannabis ransomware reports surged in 2024-2025; password-only is the most-targeted gap.

Q12. Are EDR and patching enforced on POS endpoints and the METRC workstation?

Green Managed EDR (Huntress, SentinelOne, Defender for Business with SOC) on every POS terminal. OS and POS-software patches within 14 days of release.

Yellow Antivirus exists, patching is manual, the METRC machine has not been rebooted in months.

Red Built-in AV only. Patches "when the POS vendor pushes them."

Next step: Cannabis POS systems are a known ransomware target. EDR plus a human on the alerts is non-negotiable.

5. Operations, training, and inspection readiness

Q13. Could you produce a complete METRC export, lab COAs, and 30-day camera footage for a regulator within their deadline (often 24-72 hours)?

- **Green** Inspection runbook tested twice a year. The compliance manager has done a mock drill in the last 90 days.
- **Yellow** You could do it but it would consume a full day of the entire ops team.
- **Red** You would call your lawyer and try.

Next step: Run a quarterly mock inspection. The first one is rough; the third is routine. Regulators notice the difference.

Q14. Have budtenders, cultivators, and processors had phishing-awareness training in the last 12 months?

- **Green** Five-minute monthly modules, simulated phish quarterly. Training tracked by employee in HR.
- **Yellow** One-time training at hire.
- **Red** No training. The compliance manager has clicked a real phish in the last year.

Next step: Cannabis is a high-PII, cash-rich target. Phishing-awareness is the cheapest control with measurable ROI.

Q15. Is there a documented offboarding process that revokes POS, METRC, banking, and physical access within one business day?

- **Green** Checklist that covers per-employee POS, METRC user, banking signers, alarm codes, key fobs, M365/Google.
- **Yellow** Email and POS get disabled fast, METRC user lingers for weeks.
- **Red** Former budtenders may still have a working login.

Next step: Build a one-page offboarding checklist this week. METRC user revocation is a regulator-noticed audit item.

Score yourself

Count how many of each color you marked across the 15 questions. Rough interpretation below. It is a starting point, not a verdict.

Green answers	Yellow answers
Red answers	**15** Total questions

13+ Green: you are operating ahead of most of the industry. The risk now is drift; enforce the cadence (quarterly export drill, annual policy review, weekly market data review).

8-12 Green: the basics are mostly there. Your three biggest Yellows are likely your three biggest audit or competitive risks. Close them in 90 days.

Under 8 Green, or any Red on Q1, Q7, Q10, or Q11: you have an exposure that turns a routine inspection into a license-action, or a market shift you will not see in time. Treat these as priority one.

Want a second pair of eyes?

KawaConnect builds IT and data tooling for cannabis operators across multiple states. We run Tagestry (the METRC label platform covering all 28 jurisdictions) and PryceHawk (cannabis market intelligence across roughly 900 Ohio and Michigan dispensaries). The 30-minute readiness call is free and there is no pitch attached. Walk us through your answers, we point out what we would fix first.

Call (412) 556-7007 · **Email** support@kawaconnect.com · **Web** kawaconnect.kawalink.us