IT Support RI
"IT Support Done Right"

FREE RESOURCE FOR MASSACHUSETTS AGENCIES

Is Your Agency WISP-Compliant?

A 10-Point Self-Check for Massachusetts Insurance Offices

If your agency holds the personal information of Massachusetts residents — names paired with Social Security numbers, driver's license numbers, or financial account details — state law **(201 CMR 17.00)** requires you to develop, implement, and maintain a **Written Information Security Program (WISP)**. There is no revenue threshold, no employee minimum, and no industry carve-out, and the requirement is enforced by the Massachusetts Attorney General. Insurance agencies hold exactly the kind of data the law is written to protect — yet most small agencies don't have a compliant program in place.

> **How to use this:** Go down the list and honestly check every box you can answer "yes, and we could show it" to. Your total points you to where the gaps are — and what to fix first.

The 10-Point Check

1. ☐ **You have an actual written WISP document**
   A real, current document — not verbal policy or informal habits. It's the first thing an investigator or auditor asks for.

2. ☐ **One specific person owns the program**
   A named individual (owner, office manager, or your IT provider) is responsible for maintaining the WISP and its safeguards.

3. ☐ **You've done a documented risk assessment**
   You know where client personal information actually lives — AMS, email, cloud, paper files — and the foreseeable risks to it.

4. ☐ **Access to client data is limited and controlled**
   Only staff who need personal information can reach it, with unique logins and multi-factor authentication (MFA) — no shared passwords.

5. ☐ **Data is encrypted on laptops and mobile devices**
   Personal information stored on laptops, phones, and portable or removable drives is encrypted, so a lost device isn't a reportable breach.

The 10-Point Check (continued)

6 ☐ **Data is encrypted when it travels**
Personal information sent over the internet or wirelessly — including email to clients and carriers — is transmitted securely.

7 ☐ **Systems are patched and protected**
Up-to-date firewalls, security patches, and malware/endpoint protection are running on every system connected to the internet.

8 ☐ **The program is monitored and reviewed**
Safeguards are monitored for effectiveness and reviewed at least annually — and whenever your business or systems materially change.

9 ☐ **Your vendors are vetted and under contract**
Third parties that touch client data (AMS, cloud, IT, carriers) are selected for adequate safeguards and contractually required to protect it.

10 ☐ **Staff are trained, with an incident plan ready**
Your team is trained on phishing and wire fraud, and you have a written incident-response and breach-notification plan before you need it.

What your score means

9–10	**Strong footing.** You likely have the bones of a compliant program. Make sure it's documented, dated, and reviewed — an untested WISP still fails under scrutiny.
5–8	**Real gaps.** You have pieces in place, but the missing controls are exactly what an AG inquiry or a cyber-insurance application will surface. Prioritize the unchecked boxes now.
0–4	**Significant exposure.** You most likely don't have a compliant WISP — a legal obligation today, and a breach without one is far harder to defend.

Why it matters for agencies

Regulatory
201 CMR 17.00 is enforced by the MA Attorney General, with civil penalties and mandatory breach notification under Ch. 93H.

E&O & trust
A breach of client data can trigger an E&O claim and erode the client trust your agency is built on.

Insurability
Carriers now require MFA, monitoring, and tested backups before they'll write your cyber policy — the same controls above.

FREE · NO OBLIGATION

Not sure how your agency scored?

If any of these points are hard to answer — or you'd like help building, updating, or reviewing your agency's WISP — we're glad to help. Ask **IT Support RI** for a complimentary **Agency Cyber Risk & Compliance Review** and we'll walk through every point with you. No pressure, no obligation.

Talk to us → ITsupportRI.com/contact-us

Call MA: 508-618-5774 **Main:** 401-522-5200 **Web:** ITsupportRI.com