

How does Cyber Crucible support Massachusetts 201 CMR 17.00 (WISP)?

Short answer: Massachusetts 201 CMR 17.00 requires any organization holding personal information about a Massachusetts resident to maintain a Written Information Security Program with specific safeguards. Cyber Crucible supports a customer's WISP with encryption, access control, and monitoring — and reduces the customer's own exposure because it holds essentially no personal information.

How it aligns

- **Technical safeguards** — encryption in transit and at rest, strong authentication, and access control map to the regulation's computer-system requirements.
- **Endpoint protection and monitoring** support the "reasonably up-to-date" security-software requirement.
- **Minimal data footprint** — the regulation's obligations attach to personal information; Cyber Crucible does not collect it.

Vendor-selection notes

201 CMR 17.00 also requires overseeing third-party service providers by contract. A data processing agreement and control documentation are available on request.

Revision #2

Created 2026-07-23 15:18:41 UTC by Dennis Underwood

Updated 2026-07-23 18:20:07 UTC by Dennis Underwood