IT & Security Requirements

The selected vendor will be responsible for ensuring that all website development and hosting services meet the following Information Technology and Security requirements. Vendors must provide documentation, policies, and certifications to demonstrate compliance.

1. Security & Compliance

- Vendor must maintain a current **SOC 2 Type II certification** (or equivalent such as ISO 27001) and provide certification upon request.
- Vendor must comply with **WCAG 2.1 AA Accessibility Standards**.
- Vendor must comply with applicable **data privacy regulations**, including but not limited to GDPR, CCPA, and HIPAA (if applicable).
- Vendor must implement **controls for Personally Identifiable Information (PII)** to ensure secure handling, transmission, and storage.
- Vendor must maintain a **documented Access Control Policy** with enforcement of role-based access.
- Vendor must have a signed **Acceptable Use Policy** for all personnel with access to systems.
- Vendor must maintain a **Business Continuity and Disaster Recovery (BC/DR) Plan**, reviewed and tested annually.
- Vendor must have an **Incident Response Plan** with breach notification to the client within **24 hours of discovery**.
- Vendor must maintain a **Vulnerability and Patch Management Program**, including:
    - Regular vulnerability scanning.
    - Defined remediation timelines (e.g., critical vulnerabilities remediated within 30 days).

2. Technical & Hosting

- Website must be hosted in a **U.S.-based, Tier 3 or higher data center** or with an equivalent cloud hosting provider.

- Hosting environment must include **firewalls, intrusion detection/prevention systems, and endpoint protection**.
- Data must be encrypted:
    - **At rest:** AES-256 or stronger.
    - **In transit:** TLS 1.2 or higher.
- Vendor must enforce **multi-factor authentication (MFA)** for all administrative and privileged access.
- Vendor must maintain **audit logging and monitoring** of all administrative actions.
- Vendor must conduct **annual penetration testing** and provide an executive summary of results.

3. Operational Requirements

- Vendor must guarantee a **99.9% uptime Service Level Agreement (SLA)** with performance monitoring and reporting.
- Vendor must support **scalability and performance monitoring** to handle traffic spikes.
- Vendor must provide **regular system backups**, including:
    - Daily incremental backups.
    - Weekly full backups.
    - Minimum 30-day retention.
- Vendor must provide defined **support hours and escalation procedures** for critical incidents.

4. Reporting & Oversight

- Vendor must provide **annual security attestations**, including SOC 2 reports, penetration test summaries, and compliance certifications.
- Vendor must disclose and obtain approval for any **material subcontractors** involved in hosting or development.
- Vendor must permit **periodic security audits or questionnaires** as requested by the client.