Information Security Policy

INTERNAL POLICY | Fritz Consulting LLC | fritzconsulting.io | U.S. / Ohio market

1. Purpose, scope, and ownership

This internal Information Security Policy applies to Fritz Consulting LLC personnel and authorized contractors who administer fritzconsulting.io and AccordMint services. It covers customer data, devices, accounts, Wix CMS records, Velo code, project photos, voice recordings, transcripts, payment metadata, and third-party processors.

Policy owner: the managing member of Fritz Consulting LLC. Adopt only after verifying that the listed practices are operational. Review annually and after material changes or incidents.

2. Data classification and handling

Public. Approved website content and published service descriptions; normal publication permitted.

Internal. Business procedures, internal planning, nonpublic operational metrics; business access only.

Confidential. Customer names, contact data, addresses, project descriptions, photos, transcripts, service orders, payment identifiers; least-privilege access and no public links unless explicitly authorized.

Restricted / prohibited collection. Full cardholder data, CVV, passwords, SSNs, medical information, and other highly sensitive data are not to be intentionally collected through project submissions. If received inadvertently, escalate for secure removal.

Data owners must determine whether files can be shared with contractors and remove unnecessary names, contact details, access instructions, or personal imagery wherever possible.

3. Account and access control

Use individual administrator accounts, unique strong passwords, and multifactor authentication where supported. Access to Wix administrative functions, CMS data, payment settings, email systems, and AI provider accounts is limited to personnel who need it. Remove or adjust access promptly when responsibilities change. Review privileged users at least quarterly. Do not share administrator login credentials. Ensure customer/member permissions do not expose another customer's projects.

4. System security: Wix versus business responsibilities

Wix-managed hosting and payment infrastructure may provide network firewalls, monitoring, encryption, and other protections. Fritz Consulting LLC must verify actual product coverage and available evidence before representing that specific IDS, IPS, WAF, DLP, encryption, backup, vulnerability-scanning, or PCI controls are in place.

AccordMint is responsible for safe Velo code, site-role permissions, secure configuration, authorized integrations, API secrets, access hygiene, data minimization, and monitoring unusual use. Do not store card details in CMS, custom forms, or application logs.

Maintain an inventory noting for each control: provider, scope, owner, evidence, verification date, and any gap. Mark unverified controls "not verified," not "implemented."

5. Device and endpoint protections

Use supported operating systems and browsers; apply security updates promptly; enable device lock, antivirus/endpoint protection, and full-disk encryption where available. Protect phones and computers used to access the Wix dashboard. Avoid public/shared computers for administrator access.

Use secure backups of essential internal business records where appropriate. Do not download customer archives to unprotected personal devices or share them through unrestricted cloud folders.

6. Secure development and third-party services

For Velo and custom upload/transcription modules, validate file types and sizes, restrict uploads to authenticated users where appropriate, enforce server-side authorization for every read/write, minimize logs containing personal data, keep secrets server-side, and test permissions with a second customer account.

Before activating a third-party AI, email, analytics, storage, or contractor-access tool, review what customer data it receives, its retention policy, its security commitments, and ability to support deletion or incident response. Keep a vendor register.

7. Retention, deletion, and destruction

Apply the approved Privacy & Data Retention Policy schedule: proposed 30 days for inactive draft projects, 3 days for original audio after successful transcription, 24 months for project records, 7 years for financial metadata, and 90 days for configurable logs, subject to documented exceptions.

Implement automated deletion only after testing. Manual deletion should require authorized personnel and a completion record. Include CMS collections, media library assets, external transcription tools, exports, and any contractor shares. Provider backups may follow provider-specific deletion cycles.

Before disposing of business devices, securely erase storage or use a reputable destruction service and retain a record as warranted.

8. Monitoring, incident handling, and breach reporting

Investigate unexpected logins, bulk downloads, malicious uploads, payment anomalies, unauthorized CMS access, and external complaints. Preserve relevant evidence and avoid deleting logs needed to determine scope.

On suspicion of an incident: (1) contain access; (2) notify the policy owner; (3) preserve evidence; (4) assess the data and persons involved; (5) involve Wix/vendors and cyber insurer promptly; (6) obtain legal advice on notification; (7) document resolution and lessons learned.

Ohio Revised Code §1349.19 imposes notification duties when its definitions and thresholds are met; qualifying notices to residents generally must be made promptly and no later than 45 days after discovery, subject to statutory exceptions. Other states may apply if services expand beyond Ohio.

9. Continuity, education, and periodic review

Keep vendor support details, domain ownership details, incident contacts, and documented recovery steps accessible outside the affected site. Test critical account recovery and project-data restoration where supported.

Review permissions and failed-access concerns quarterly, vendors and retention processes at least annually, and site security after major code/payment changes. Personnel handling customer data should receive basic phishing, sensitive-data handling, and incident reporting instructions.

10. Verification register — for insurance attestation

Firewall / WAF. Provider and coverage: obtain Wix evidence.
IDS / IPS. Provider and coverage: obtain Wix evidence.
DLP. define whether prevention is technical, procedural, or absent.
TLS and encryption at rest. Provider specifics and scope: using current Wix documentation and business settings.
MFA and administrator inventory. current configuration and evidence.
Backups and restore capability. ownership, coverage, and recovery expectations.
Deletion automation. audio, photo, CMS, and third-party workflows.
Cyber-insurance declarations. **a**ctual implemented controls and documented evidence.

References

Ohio Revised Code §1349.19: https://codes.ohio.gov/ohio-revised-code/section-1349.19
Ohio Attorney General consumer information: https://www.ohioattorneygeneral.gov/Business/Services-for-Business/Business-Guide/Personal-Information-for-Consumers
Wix Privacy & Cookies: https://support.wix.com/en/article/about-privacy-cookies
Existing contractual basis: AccordMint Service Agreement, version 2026-10-19.