YBOR CITY SOCIETY WINE BAR MEMBERSHIP APP

DATA PRIVACY & SECURITY POLICY

Effective Date: March 9, 2026 | Version: 1.0 | Status: Demo / Audit In Progress

📋	You are accessing a pre-release demo of this Application. We are actively auditing our systems against the security and privacy standards described in this policy. These standards represent our intended posture — implementation is in progress and will be verified before general release. Your data is private and will not be monetized.

1. Scope & Applicability

This policy applies to all users of the Ybor City Society Wine Bar Membership App ("the Application") during its demo and testing phases, and will remain in effect upon general release. It governs the collection, use, storage, and protection of all personal and non-personal data submitted to or generated by the Application.

🔍	This Application is currently undergoing a formal compliance audit against the standards listed in Section 3. The controls and commitments described in this policy reflect our target security posture. Audit completion is required before the Application will be made publicly available.

2. Our Core Commitments

2.1 Data Privacy

- All user data is treated as private by default and is never publicly accessible.
- Data is not sold, rented, traded, or otherwise transferred to third parties for commercial purposes.
- During the testing phase, data will not be used for advertising, monetization, or any revenue-generating activity.
- You retain ownership of your data at all times.

2.2 Data Minimization

- We collect only the data necessary to operate and improve the Application.
- We do not collect sensitive personal data (e.g., financial information, health records) unless explicitly required and disclosed.
- Aggregate and anonymized analytics may be used internally to understand usage patterns.

2.3 Security Practices

- All data in transit is encrypted using TLS 1.2 or higher.
- All data at rest is encrypted using AES-256 or equivalent standards.
- Access to user data is restricted to authorized personnel on a need-to-know basis.
- We conduct regular security reviews and vulnerability assessments.
- Authentication systems follow OWASP best practices including secure password hashing and support for multi-factor authentication (MFA).

3. Applicable Standards & Frameworks

This policy is designed to align with the following recognized international and industry standards. We are actively working toward full compliance with each, with formal audit procedures underway:

GDPR	EU General Data Protection Regulation — governs data rights for EU/EEA residents including consent, access, and erasure rights.	User rights, lawful basis for processing	**In Progress**
CCPA	California Consumer Privacy Act — grants California residents rights to know, delete, and opt out of data sale.	US user privacy rights	**In Progress**
ISO/IEC 27001	International standard for Information Security Management Systems (ISMS).	Security controls & governance	**In Progress**
SOC 2 Type II	AICPA framework auditing security, availability, processing integrity, confidentiality, and privacy.	Trust & compliance posture	**Planned**

OWASP Top 10	Industry standard for web application security risks and mitigations.	Application-level security	**In Progress**
NIST CSF	NIST Cybersecurity Framework — identify, protect, detect, respond, recover.	Security program structure	**In Progress**

4. Data We Collect

4.1 Data You Provide

- Account information (e.g., name, email address)
- Content or inputs you submit within the Application
- Feedback, bug reports, and support communications

4.2 Data Collected Automatically

- Device type, operating system, and browser information
- IP address (used for security and fraud prevention only)
- Usage logs and interaction data (anonymized where possible)
- Crash reports and error logs

🔍	During this demo phase, additional diagnostic data may be collected to support our compliance audit and identify technical gaps. This data is reviewed only by the engineering and security teams and is deleted or anonymized within 90 days.

5. How We Use Your Data

- To provide, operate, and improve the Application
- To diagnose technical issues and resolve bugs
- To communicate with you about your account or the Application
- To comply with legal obligations

We will NOT use your data for:

- Targeted advertising or marketing to third parties
- Sale or licensing to data brokers

- Profiling for commercial gain
- Any purpose materially different from those listed above without your explicit consent

6. Data Retention

We retain personal data only as long as necessary for the purposes described in this policy. Upon request, or upon the termination of your account, we will delete or anonymize your personal data within 30 days, except where retention is required by law.

7. Your Rights

Depending on your jurisdiction, you may have the right to:

- Access the personal data we hold about you
- Request correction of inaccurate data
- Request deletion of your data ("Right to be Forgotten")
- Opt out of certain data processing activities
- Data portability — receive your data in a machine-readable format
- Lodge a complaint with your local data protection authority

To exercise any of these rights, contact us at: [privacy@yourapp.com]

8. Security Measures

We implement the following technical and organizational measures to protect your data:

Encryption in Transit	TLS 1.2+ for all API and web traffic
Encryption at Rest	AES-256 for all stored data and backups
Authentication	Secure password hashing (bcrypt/Argon2), MFA support
Access Control	Role-based access control (RBAC); least-privilege principle
Infrastructure	Hosted on SOC 2-compliant cloud infrastructure
Vulnerability Management	Regular dependency scanning, penetration testing
Incident Response	Defined breach notification process within 72 hours (per GDPR)

9. Third-Party Services

We may use trusted third-party service providers (e.g., cloud hosting, analytics) solely to operate the Application. These providers are contractually obligated to protect your data and are prohibited from using it for their own purposes.

We do not currently integrate with advertising networks or data brokers.

10. Our Audit Commitment

As a demo user, you should know that we take compliance seriously. Here is where we stand:

- We have engaged an independent security team to audit our infrastructure and application controls against the standards listed in Section 3.
- Findings from the audit are tracked and remediated prior to general release. No known critical vulnerabilities are left unaddressed.
- Our audit process covers: access controls, data handling practices, encryption implementation, incident response readiness, and third-party risk.
- Upon completion of the audit, a compliance summary will be made available to users upon request.

✅	The protections described in this policy are goals we are actively working to certify — not aspirational statements. Demo access is granted with the understanding that we are in a final audit and hardening phase. We appreciate your trust and will not take it for granted.

11. Changes to This Policy

We may update this policy as the Application evolves. Material changes will be communicated via in-app notice or email at least 14 days before taking effect. Continued use of the Application after that period constitutes acceptance of the updated policy.

12. Contact Us

For privacy-related questions, requests, or concerns, please contact:

Ybor City Society Wine Bar Membership App — Privacy Team

Email: info@yborcitywinebar.com
Address: 1600 E 7th Ave, Tampa, FL 33605

⚖️	This document is provided as a policy template and does not constitute legal advice. You should have this reviewed by a qualified attorney before publishing it to users, particularly if operating in regulated industries or serving EU/California residents.