

Security Overview

The standard security practices protecting eMembership and your union's member data.

SOC 1 audited

SOC 2 audited

ISO 27001 certified facility

HIPAA Security Rule compliant

PCI DSS compliant



Data protection

- All data is encrypted in transit, and sensitive member data, including Social Security numbers, is encrypted at rest.
- Nightly backups are encrypted and stored offsite.
- Credit card numbers are never stored; payments are processed exclusively by third-party payment processors.
- Retired data and media are destroyed through secure disposal procedures.



Access control

- Multi-factor authentication is available to every eMembership client.
- Access is granted on a least-privilege basis, with unique user IDs and enforced session timeouts.
- Functional access is granted by role and staff are assigned to roles, making access administration straightforward.



Infrastructure and monitoring

- eMembership runs on infrastructure that Winmill owns and operates, inside a SOC 1 (SSAE 18) and SOC 2 audited, ISO 27001 certified colocation facility.
- Clustered, redundant firewalls protect every connection.
- Managed detection and response covers system logs, endpoint protection includes host-based intrusion prevention, and anti-DDoS protection runs at the network edge.
- Network, database, and application activity is monitored 24/7.
- Layered physical access controls protect the data center, with access reviews every six months.
- Power, networking, and internet connectivity are fully redundant, with no single point of failure.



Security testing

- Winmill's own cybersecurity practice performs penetration testing on the eMembership application and on its networks.
- Static and dynamic code analysis and code reviews are built into the development process.
- Security is overseen by CISSP and CISA certified engineers.



Governance and resilience

- A management-approved information security policy governs operations and is reviewed regularly.
- Formal risk assessments are conducted at least annually.
- A documented incident response program covers security and privacy events.
- Business continuity and disaster recovery plans are tested through regular exercises.
- All employees complete security awareness training at hire and annually thereafter.

Winmill regularly completes formal security audits for clients, and detailed documentation is available upon request. These protections are included for every labor union on the platform as part of the standard eMembership subscription.