# Security at WinAI

How we approach security across websites, automations, AI agents, and client projects.

Last Updated: September 29, 2026

Security is an important part of how WinAI designs, builds, and operates websites, workflow automations, AI agents, integrations, and other technology solutions.

We use reasonable technical, administrative, and organizational measures designed to protect our systems, customer information, and project environments.

Because every client project is different, specific security controls may vary depending on the systems, infrastructure, integrations, data, and requirements involved.

## 1. Our Security Approach

WinAI follows a practical, risk-based approach to security.

Our security practices are designed around several core principles:

- Limit access to systems and data
- Protect credentials and secrets
- Use secure communication channels
- Minimize unnecessary data collection
- Separate development and production environments where appropriate
- Monitor systems for unexpected behavior
- Keep software and dependencies reasonably up to date
- Review security requirements before deploying sensitive workflows
- Use established cloud and technology providers where appropriate

No internet-connected system can be guaranteed to be completely secure, but we work to reduce unnecessary risk throughout the development and deployment process.

## 2. Secure Development Practices

WinAI incorporates security considerations throughout the software development lifecycle.

Depending on the project, our development practices may include:

- Code review
- Input validation
- Authentication controls
- Authorization checks
- Secure API design
- Error handling
- Environment separation
- Dependency management
- Secret management
- Logging and monitoring
- Rate limiting
- Secure configuration
- Production testing

Security controls are selected based on the needs and architecture of each project.

## 3. Access Control

Access to WinAI-managed systems is limited to authorized personnel and systems with a legitimate business need.

Where appropriate, we may use:

- Individual user accounts
- Role-based access
- Multi-factor authentication
- Limited administrative privileges
- Credential rotation
- Session controls
- Access logging

We follow the principle of limiting access to the minimum reasonably required for the task.

## 4. Authentication and Credentials

WinAI does not intentionally store passwords, API keys, authentication tokens, or other sensitive credentials directly in source code.

Sensitive configuration values are generally stored using secure environment variables, secret management systems, or protected platform configuration.

Customers should never send passwords, API keys, authentication codes, private keys, or other sensitive credentials through unsecured communication channels unless specifically instructed to use an approved secure method.

## 5. Data Encryption

Where supported by the applicable infrastructure and service providers, data transmitted between users, WinAI systems, and third-party services is protected using encrypted connections such as HTTPS/TLS.

Data stored by third-party infrastructure providers may also be encrypted at rest according to those providers' security capabilities and configurations.

Encryption practices may vary depending on the architecture of a particular client project.

## 6. Data Minimization

We aim to collect and process only the information reasonably necessary to:

- Respond to inquiries
- Provide consultations
- Deliver customer projects
- Operate integrations
- Provide support
- Maintain security and reliability

We discourage customers from providing sensitive or regulated information unless it is necessary for the project and the appropriate requirements have been reviewed.

## 7. AI Agent Security

WinAI develops AI-powered agents for use cases such as customer service, lead qualification, appointment handling, workflow support, and other business processes.

AI systems may involve multiple technology providers and integrations.

Depending on the solution, we may implement controls designed to:

- Restrict access to approved tools
- Limit available actions
- Validate tool requests
- Protect internal system instructions
- Protect secrets and API credentials
- Restrict sensitive operations
- Require customer confirmation before certain actions
- Log system activity
- Separate internal metadata from customer-facing responses

AI systems are probabilistic and may occasionally produce incorrect or unexpected responses.

For sensitive workflows, human review or additional safeguards may be appropriate.

## 8. Automation Security

Workflow automation can connect multiple systems and perform actions automatically.

WinAI designs automations to limit unnecessary permissions where practical.

Depending on the project, we may use:

- Scoped API permissions
- Authenticated webhooks
- Secret-based authentication
- Request validation
- Idempotency controls
- Audit logging
- Error handling

- Retry controls
- Approval steps for sensitive actions

Customers should grant only the permissions required for the automation to operate.

## 9. API Security

Where WinAI develops or operates APIs, security practices may include:

- Authentication
- Authorization
- Input validation
- Secure headers
- HTTPS
- Request validation
- Rate limiting
- Access logging
- Secret management
- Error handling
- Protection against unauthorized requests

The exact implementation depends on the application's architecture and risk profile.

## 10. Website Security

For websites and web applications built by WinAI, we may implement protections such as:

- HTTPS
- Secure authentication
- Form validation
- Protection against common injection attacks
- Secure cookies
- Access controls
- Dependency updates
- Spam protection

- Rate limiting
- Secure deployment configuration

The security of a deployed website may also depend on hosting providers, plugins, third-party applications, customer configuration, and ongoing maintenance.

## 11. Third-Party Services

WinAI relies on third-party technology providers for certain infrastructure and services.

These may include:

- Cloud hosting
- Database providers
- AI model providers
- Email services
- Telecommunications providers
- CRM platforms
- Calendar services
- Automation platforms
- Analytics providers
- Payment providers

Third-party providers maintain their own security programs, infrastructure, terms, and policies.

WinAI does not control the security practices of independent third-party services.

When selecting third-party services for a project, we consider factors such as functionality, reliability, security features, integration capabilities, and project requirements.

## 12. Customer Data

Customer data may be processed only as necessary to provide requested services.

Depending on the project, this may include data from:

- CRM systems

- Websites
- Contact forms
- Business databases
- Calendars
- Email systems
- Customer support systems
- APIs
- Automation platforms

Customers remain responsible for ensuring that they have appropriate rights and permissions to provide data to WinAI and its authorized service providers.

## 13. Sensitive and Regulated Data

Customers should not provide highly sensitive or regulated information unless WinAI has specifically agreed to process it.

Examples may include:

- Protected health information
- Payment card information
- Government identification numbers
- Authentication credentials
- Highly sensitive financial information
- Confidential legal records

Projects involving regulated data may require additional technical, legal, contractual, and compliance review.

WinAI does not represent that every WinAI service is automatically:

- HIPAA compliant
- SOC 2 compliant
- PCI DSS compliant
- GDPR compliant
- ISO 27001 certified
- or certified under another security framework

Specific compliance requirements must be reviewed for the particular project and environment.

## 14. Infrastructure Security

WinAI may use established cloud and infrastructure providers to host applications, databases, automations, and related systems.

Security controls may include:

- Network protections
- Access controls
- Encrypted communications
- Environment separation
- Backups
- Logging
- Monitoring
- Availability controls

Specific infrastructure depends on the project.

## 15. Environment Separation

Where appropriate, WinAI may maintain separate:

- Development
- Testing
- Staging
- Production

environments.

Production credentials and sensitive configuration should not be committed to public source code repositories.

## 16. Source Code Security

WinAI takes reasonable steps to protect source code and development environments.

Practices may include:

- Private repositories
- Access restrictions
- Branch controls
- Code review
- Secret scanning
- Dependency review
- Environment-based configuration

Customers should also protect any source code, credentials, or repositories transferred to them.

## 17. Logging and Monitoring

Where appropriate, systems may generate logs for:

- Application errors
- API activity
- Authentication activity
- Automation execution
- Webhook requests
- Security events
- Infrastructure health

Logs may be used for troubleshooting, reliability, security monitoring, and incident investigation.

We aim to avoid storing unnecessary sensitive information in logs.

## 18. Vulnerability Management

WinAI may periodically review:

- Software dependencies
- Infrastructure configuration
- Authentication controls
- Application code

- Third-party packages
- Platform updates

When material vulnerabilities are identified, we work to evaluate and address them based on severity, risk, and operational impact.

## 19. Updates and Dependencies

Modern software relies on frameworks, libraries, APIs, and third-party services.

We make reasonable efforts to keep supported systems and dependencies appropriately updated.

However, customers should maintain an active support or maintenance arrangement when ongoing updates are required after project delivery.

## 20. Backup and Recovery

Where backup functionality is part of the selected infrastructure or service scope, backups may be used to help recover from certain failures or data loss events.

Backup capabilities depend on the platform, configuration, retention settings, and project requirements.

Customers should maintain independent backups of important business information when appropriate.

WinAI does not guarantee that every system or data set can always be fully recovered.

## 21. Security Incidents

If WinAI becomes aware of a security incident affecting systems or information under our control, we will evaluate the incident and take reasonable steps to:

- Contain the issue
- Investigate the cause
- Reduce further risk
- Restore affected services where appropriate
- Notify affected parties where required by applicable law or contractual obligation

The specific response will depend on the nature and severity of the incident.

## 22. Employee and Contractor Access

WinAI personnel and authorized contractors may receive access to customer systems only when required to perform their work.

We expect individuals with access to confidential customer information to handle that information appropriately and use it only for legitimate business purposes.

Where appropriate, access may be revoked when it is no longer required.

## 23. Customer Responsibilities

Security is a shared responsibility.

Customers should:

- Use strong passwords
- Enable multi-factor authentication where available
- Limit administrative access
- Protect API keys and credentials
- Keep user accounts current
- Remove access for former employees
- Review permissions regularly
- Maintain backups where appropriate
- Keep software reasonably updated
- Notify WinAI about suspected security incidents
- Avoid sending credentials through insecure channels

WinAI cannot protect systems where customer credentials are compromised or where customers intentionally disable required security controls.

## 24. AI and Human Review

AI agents can automate many tasks, but not every decision should be made automatically.

Customers should consider human review for workflows involving:

- Legal decisions
- Medical decisions

- Financial decisions
- Employment decisions
- High-value transactions
- Sensitive customer data
- Safety-related decisions
- Regulatory obligations

The appropriate level of human oversight depends on the customer's use case.

## 25. No Absolute Security Guarantee

While WinAI uses reasonable measures designed to reduce security risks, no technology platform can guarantee complete security.

We cannot guarantee that:

- Systems will never be compromised
- Software will never contain vulnerabilities
- Third-party services will never experience incidents
- Data transmission will always be uninterrupted
- AI systems will never generate unexpected output

Security is an ongoing process rather than a one-time guarantee.

## 26. Responsible Security Disclosure

If you believe you have discovered a security vulnerability affecting winai.dev or a WinAI-managed system, please report it responsibly.

Please include:

- A description of the issue
- Steps to reproduce it
- The affected URL or system
- Potential impact
- Any relevant screenshots or technical details

Please do not:

- Access data that does not belong to you
- Modify or delete data
- Disrupt production services
- Perform denial-of-service testing
- Use social engineering
- Publicly disclose the issue before WinAI has had reasonable time to investigate

We appreciate responsible security research that is conducted in good faith.

## 27. Security Contact

For security-related questions or responsible vulnerability reports:

Contact Win AI Automation