Smart Aguila Security & Data Protection

Your Security Best Practices

Use Strong Authentication

- Choose a password with at least 12 characters, including letters, numbers, and symbols.
- Enable Two-Factor Authentication (2FA) where available.

Stay Alert to Phishing & Social Engineering

- Smart Aguila will never ask for your password or sensitive information via email or phone.
- Be cautious of unsolicited messages claiming to be from us.

Keep Your Login Credentials Private

- Never share your login details with anyone.
- For support, contact us at hi@smartaguila.com.

Verify Official Website

- Always ensure you are visiting the official Smart Aguila website.
- Our platform uses secure encryption (SSL/TLS) to protect your data.

Watch Out for Suspicious Emails

- Verify sender email addresses before responding.
- Avoid clicking links or downloading attachments from unknown sources.

How Smart Aguila Protects Your Data

Platform Security

- Secure hosting and infrastructure
- Encryption of data in transit (SSL/TLS)
- Regular system monitoring and updates
- Use of trusted third-party services

Internal Security Measures

- Restricted access to sensitive data
- Secure systems and devices
- Regular security reviews and monitoring

Data Protection

- We follow best practices to ensure confidentiality and integrity of your data
- We do not store sensitive payment information

Vulnerability Reporting

If you discover any security vulnerabilities, please report them to us at hi@smartaguila.com. We will investigate and take appropriate action promptly.