Wisdom Born Consulting, LLC
Information Security Policy

Effective Date: August 22, 2025

As a single-member LLC conducting e-commerce business, Wisdom Born Consulting, LLC is committed to maintaining robust information security practices to protect client information and ensure regulatory compliance.

1. Scope

This policy applies to all systems, websites, and data managed by Wisdom Born Consulting, LLC. As a sole proprietorship with no employees, all security responsibilities rest with the owner.

2. Business Model and Payment Processing

Wisdom Born Consulting operates as a service-based business that:

- Sends invoices to client organizations
- Processes payments exclusively through secure third-party platforms (Stripe and QuickBooks)
- Uses secure payment links provided by these platforms
- Does not store, process, or transmit client credit card information

3. Access Control

- Only the owner, has access to all business systems and client information
- Strong passwords and two-factor authentication (2FA) are required for all administrative accounts
- Regular password updates are performed across all platforms
- Administrative sessions are logged out when not in use

4. Third-Party Platform Security

Payment Processing:

- All credit card transactions are processed through Stripe and QuickBooks payment platforms

- These platforms maintain PCI DSS Level 1 compliance
- Secure payment links are generated and provided to clients for invoice payments
- No payment card data is handled directly by company systems

Platform Monitoring:

- Regular review of security notifications from payment platforms
- Prompt application of security updates and patches
- Monitoring of platform compliance certifications

5. Data Handling and Protection

Client Information:

- Invoice data and client contact information are stored securely
- No credit card numbers, CVV codes, or other payment card data are stored
- Client data is accessed only for legitimate business purposes

Data Retention:

- Invoice records are retained for seven years for tax compliance
- Client contact information is maintained only for active business relationships
- Secure deletion procedures are followed when data is no longer needed

6. System Security

Website and E-commerce:

- Company website hosted on WordPress with WooCommerce functionality
- Jetpack security monitoring and scanning enabled
- Regular security updates applied to all website components
- SSL certificates maintained for secure communications

Email and Communications:

- Secure email practices for sensitive communications
- Invoice delivery through encrypted channels when possible
- Verification of recipient identity before sending sensitive information

7. Incident Response

As the sole operator, incident response procedures include:

- Immediate assessment of any suspected security incidents
- Notification of affected clients within 24 hours when applicable
- Documentation of incident details and remediation steps
- Review and improvement of security measures following incidents
- Coordination with third-party platforms if incidents involve their services

8. Physical Security

- Secure storage of any physical documents containing client information
- Immediate shredding of sensitive documents when no longer needed
- Secure workstation practices including screen locks and clean desk procedures
- Protection of devices used for business operations

9. Compliance

PCI DSS Requirements:

- Compliance with PCI DSS SAQ A requirements as a merchant using only third-party payment processors
- No storage of cardholder data on company systems
- Secure transmission of payment information through certified platforms

Business Compliance:

- Annual review and update of this security policy
- Maintenance of current business licenses and certifications
- Adherence to client contractual security requirements

10. Risk Management

Ongoing Assessment:

- Regular evaluation of security risks associated with business operations
- Monitoring of third-party platform security advisories
- Updates to security measures based on emerging threats

Business Continuity:

- Regular backups of essential business data
- Alternative communication methods for client contact during outages
- Documentation of critical business processes

11. Training and Awareness

As the sole proprietor, the owner commits to:

- Staying informed about current cybersecurity threats and best practices
- Participating in relevant security training programs
- Monitoring security publications and advisories
- Implementing new security measures as appropriate

12. Policy Review and Updates

This policy is reviewed annually and updated as needed to reflect:
- Changes in business operations
- New regulatory requirements

Wisdom Born Consulting, LLC
Information Security Policy

Effective Date: August 22, 2025

- Emerging security threats
- Updates to third-party platform security measures

By maintaining this policy, Wisdom Born Consulting, LLC demonstrates its commitment to protecting client information and maintaining the highest standards of information security appropriate for its business model.

Signed,

Natisha S. Jordan

box SIGN   467972WQ-1VRXPYJJ

Natisha S. Jordan
Owner, Wisdom Born Consulting, LLC

Next Review Date: August 22, 2026