Carrington Financials Written Information Security Program (WISP)

Internal use only | Effective date: April 22, 2026

Purpose. This Written Information Security Program ("WISP") establishes the administrative, technical, and physical safeguards Carrington Financials uses to protect client, prospect, applicant, employee, and business information, including nonpublic personal information and other sensitive data handled in connection with insurance and related services.

Scope. This WISP applies to all systems, devices, accounts, software, vendors, websites, forms, records, and business processes used by Carrington Financials to collect, access, store, transmit, use, retain, or dispose of covered information.

1. Governance and Responsibility

Owner / Qualified Individual: Carrington Chatman or designated delegate.

The Qualified Individual is responsible for maintaining this WISP, overseeing safeguards, approving exceptions, coordinating incident response, and documenting annual review activity.

If a managed service provider, website vendor, or IT consultant supports implementation, Carrington Financials retains ultimate responsibility for the program.

2. Information Covered by This Program

Covered information includes contact information, quote details, underwriting data, policy information, payment-related records, driver and property information, health-related data if collected for insurance purposes, internal business records, and credentials that could permit access to covered systems or data.

3. Risk Assessment Process

Carrington Financials will maintain a written risk assessment identifying reasonably foreseeable internal and external risks to covered information.

The risk assessment will identify where covered information is collected, stored, transmitted, and disposed of, including website forms, email, cloud storage, CRM systems, carrier portals, mobile devices, laptops, paper files, and third-party applications.

The risk assessment will be reviewed at least annually and after material changes in systems, vendors, business operations, or threat conditions.

4. Administrative Safeguards

Limit access to covered information to persons with a legitimate business need.

Maintain an inventory of systems, platforms, vendors, and storage locations that handle covered information.

Review user access at least annually and promptly disable access when no longer needed.

Use written onboarding and offboarding steps for any employee, contractor, or vendor with system access.

Provide periodic security awareness training covering phishing, password hygiene, device security, improper disclosure, and incident reporting.

5. Technical Safeguards

Require unique user credentials for business systems and prohibit shared passwords where feasible.

Enable multi-factor authentication for email, website administrator accounts, CRM platforms, cloud storage, password managers, carrier portals, domain registrar accounts, and hosting accounts.

Use encryption where feasible for covered information at rest and in transit. If sensitive information must be sent electronically, use secure portals, encrypted files, or other approved secure methods when feasible.

Keep business devices, browsers, operating systems, plugins, security tools, and website software updated with security patches.

Use reputable endpoint protection, strong passcodes, screen locks, and remote wipe features on business devices where available.

Maintain website security controls such as SSL/TLS, strong admin credentials, limited admin accounts, form-spam protection, security updates, and least-privilege access.

6. Physical Safeguards

Secure paper records in locked cabinets, offices, or other controlled locations.

Do not leave devices or paper files containing covered information unattended in public or unsecured settings.

Use secure destruction methods for paper records and removable media when disposal is authorized.

7. Website and Online Intake Controls

Website forms should collect only the minimum information reasonably necessary for the form's purpose.

Forms should not request Social Security numbers or full payment-card data through standard public website contact forms.

The website should use HTTPS on all pages, current plugins/themes, limited admin privileges, CAPTCHA or anti-bot protection, privacy-policy and terms links in the footer, and consent language near form submission buttons.

Administrative access to the website, domain registrar, DNS, and hosting must be restricted and protected with multi-factor authentication where supported.

8. Vendor and Service Provider Management

Exercise due diligence before using service providers that access or store covered information, including website hosts, form processors, CRMs, quoting platforms, schedulers, cloud-storage providers, e-signature platforms, and IT vendors.

Require service providers, by contract or documented due diligence, to maintain appropriate administrative, technical, and physical safeguards.

Maintain a current vendor list and review high-risk vendors periodically.

9. Retention and Secure Disposal

Carrington Financials will maintain a retention schedule based on legal, licensing, operational, and recordkeeping needs.

When covered information is no longer needed and retention is no longer required, the information will be securely deleted, destroyed, anonymized, or otherwise disposed of in a manner appropriate to the medium and the sensitivity of the information.

10. Monitoring and Testing

Review logs, alerts, backups, website update status, and administrative access periodically, based on available tooling and business size.

Test backups, form delivery, account-recovery methods, and critical security settings on a periodic basis.

Document corrective actions when material weaknesses are identified.

11. Incident Response Plan

Carrington Financials will maintain and follow a written incident response procedure designed to promptly respond to and recover from any event that compromises the confidentiality, integrity, or availability of covered information or business systems.

The incident response procedure will address internal escalation, containment, preservation of evidence, vendor coordination, legal/regulatory assessment, consumer notification where required, regulator notification where required, remediation, and post-incident review.

12. Ohio and Insurance-Specific Compliance Notes

For operations subject to Ohio insurance cybersecurity requirements, Carrington Financials will maintain a comprehensive written information security program based on its risk assessment and a written incident response plan.

If a reportable cybersecurity event occurs, Carrington Financials will assess notification obligations under applicable law, including state insurance and breach-notification requirements.

13. Annual Review and Approval

This WISP will be reviewed at least annually and updated when business practices, legal requirements, technologies, or threat conditions materially change.

Documented review date: [INSERT DATE]
Reviewed by: [INSERT NAME/TITLE]
Next review due: [INSERT DATE]

Appendix A - Minimum Security Checklist

- Use a password manager for all business credentials.
- Turn on MFA for email, CRM, hosting, registrar, cloud storage, and website admin.
- Keep a current vendor list.
- Review website plugins, forms, and admin users monthly.
- Do not collect SSNs through ordinary website contact forms.
- Back up website files and databases on a defined schedule.
- Document annual WISP review and risk assessment update.
- Maintain a simple incident log and remediation log.