SUMMIT LITIGATION SERVICES, LLC

COMPLIANCE POLICY

Effective Date: 11/01/2025
Last Reviewed: 11/01/2025

This Compliance Policy explains how Summit Litigation Services, LLC ("Summit") meets the legal, ethical, and vendor requirements for providing civil-litigation investigative support. All personnel, contractors, and authorized agents must follow this policy without exception.

1. Purpose of the Compliance Program
Summit's compliance program ensures that all research and data handling:

- Supports legitimate civil litigation needs
- Follows attorney direction
- Meets vendor-imposed permissible-use restrictions
- Complies with federal and state privacy laws
- Protects sensitive information through appropriate safeguards

Summit uses data solely to support licensed attorneys in litigation matters. Summit does not perform investigations for personal, commercial, or FCRA-regulated uses.

2. Permissible Use: Civil Litigation Only
Summit performs work exclusively under the direction of:

- A licensed attorney, or
- A legal professional acting under that attorney's authority.

Every request must be tied to a current or reasonably anticipated civil legal matter, including but not limited to:

- Identifying or locating defendants, witnesses, or responsible parties
- Verifying identity before initiating investigative steps
- Preparing for service of process
- Supporting discovery or case strategy
- Due-diligence research to confirm identities, associations, and relevant factual details

Summit does **not** perform:

- Background checks
- Consumer credit checks
- Employment screening
- Tenant screening
- Insurance underwriting or claims investigation
- Personal or non-litigation lookups

Civil litigation is the sole permissible category for Summit's services.

3. Attorney Authorization Requirements

Summit requires that:

- All orders originate from a licensed attorney or an authorized agent acting under that attorney
- The attorney maintains responsibility for the lawful purpose of each request
- All required client authorizations have been obtained before submitting a request
- Summit may rely on the representations made by the requesting party

Summit will request clarification if a request appears outside these guidelines.

4. Identity Verification Requirements

Summit verifies identity before running any substantive investigation.
Verification includes:

- Matching multiple identifiers (e.g., name + DOB + address)
- Comparing attorney-provided information to vendor sources
- Rejecting or returning matters where identity cannot be reasonably confirmed

Summit does **not** conduct searches based solely on a name match or insufficient identifiers.

If identity remains unclear, the request will be returned for clarification.

5. Prohibited Requests

Summit will not:

- Obtain consumer credit reports or financial account data
- Access medical or health records
- Obtain telecommunications or call-detail records
- Access restricted tax or government-benefit information
- Request or use DMV data outside DPPA-permitted purposes
- Conduct surveillance, background investigations, or personal searches
- Perform automated or scripted searches unless explicitly authorized by the vendor

Summit rejects any request that falls outside permissible litigation support.

6. Data Vendors & Permissible Use Rules

Summit complies with all vendor rules, including:

- Permissible use certifications
- Credentialing requirements
- Audit requests
- Documentation retention periods
- Restrictions on sharing, redistributing, or reselling vendor data

Summit's access to vendor platforms is used solely for litigation-support purposes, and only by trained personnel with individual credentials.

7. Information Security Program (WISP)

Summit maintains a Written Information Security Program (WISP) with administrative, technical, and physical safeguards designed to:

- Protect vendor-supplied data
- Meet the GLBA Safeguards Rule (16 C.F.R. § 314.4)
- Prevent unauthorized access, disclosure, or misuse
- Ensure proper handling and storage of sensitive information

Summit's WISP includes procedures for secure access, encryption, credential management, device protection, network security, and secure data disposal.

Access to data is limited to authorized personnel with a legitimate litigation-related need.

8. Confidentiality & Data Handling
Summit protects all data received from clients and vendors.
Summit:

- Keeps all information confidential
- Uses data only to complete authorized investigations
- Restricts access to trained personnel
- Avoids storing vendor data unless required for a deliverable
- Encrypts stored files and protects all devices accessing vendor systems

Client work product and vendor data are never sold, distributed, or used for marketing or non-litigation purposes.

9. Data Retention & Documentation
Summit retains only the records needed to:

- Verify permissible use
- Meet vendor audit requirements
- Document investigative actions
- Satisfy legal or regulatory obligations

Summit does not store unnecessary raw data from vendor platforms.
Documents that are no longer required are securely destroyed.

10. Incident Response & Breach Procedures

A data-security incident includes any unauthorized access, exposure, or compromise of vendor-supplied information.
If a security incident occurs, Summit will:

1. Immediately secure and contain affected systems
2. Investigate the source and scope of the incident
3. Notify affected vendors in line with vendor requirements (including IDI)
4. Cooperate fully with any vendor or legal investigation
5. Comply with applicable breach-notification laws
6. Document the incident and corrective actions

Employees must report any suspected incident immediately to Summit leadership.

11. Employee Responsibilities

Every Summit employee or contractor with access to data must:

- Complete compliance training
- Follow all vendor terms, including IDI, TLO, Delvepoint, Tracers, and others
- Maintain confidentiality of all client and vendor information
- Use only company-approved devices and networks
- Avoid personal, curiosity-based, or non-litigation lookups
- Report compliance issues or concerns promptly

Improper use of data may result in termination and vendor notification.

12. Audit Cooperation
Summit will cooperate with:
- Vendor audits
- Credentialing reviews
- Requests for supporting documentation
- Compliance inquiries
- Reasonable investigations related to permissible use or security

Requested documentation will be provided within reasonable timeframes.

13. Enforcement
Violations of this Compliance Policy may result in:
- Revocation of platform access
- Internal disciplinary action
- Termination
- Reporting to affected vendors
- Legal action if required

Summit enforces this policy consistently to protect access to sensitive vendor data.

14. Oversight & Review
Summit leadership reviews this Compliance Policy:
- Annually
- After any security incident
- When vendor requirements change
- When laws or regulations are updated

Updates are implemented promptly and communicated to affected personnel.

15. Acknowledgment
All personnel must acknowledge that they:
- Have read this Compliance Policy
- Understand their responsibilities
- Agree to follow all procedures and restrictions
- Understand that violations may lead to disciplinary action