LAW OFFICE OF Bradley Gross PA
www.BradleyGross.com

THE IT CHANNEL LEGAL LIFECYCLE PLAN

Legal guidance for MSPs, VARs, and IT resellers at every stage of growth.

Built for companies that strive to keep pace with risk appetites, business strategies, and privacy-related operations.

Your channel business changes every month. Your legal documents should not sit still.

MSPs, VARs, and IT resellers constantly add products, vendors, cloud tools, AI solutions, cybersecurity services, professional services, implementation work, managed services, and new customer expectations. The problem is that most agreements, quote terms, service descriptions, and policies only get attention after a dispute, margin problem, scope-creep issue, vendor conflict, failed project, or customer pushback. **The Legal Lifecycle Plan is designed to prevent that drift by keeping legal strategy connected to daily sales, service, procurement, and delivery operations.**

The IT Channel Legal Lifecycle Plans

Each plan includes one (or more) monthly strategy sessions with one of the most recognized attorneys in the IT channel, focused on helping your business avoid preventable legal problems before they become expensive disputes.

Launching a new service? Use your monthly review hours to make sure your documents, exclusions, and risk allocations are aligned!

Essentials	Plus	Premium
For smaller MSPs, VARs, and IT Resellers	**For growing channel companies**	**For larger MSPs, VARs, Resellers and platform / channel businesses**
• Monthly strategy call • Up to 2 hours (monthly) of conference / review / drafting time[1] • Annual document health check	• Two strategy calls/month • Up to 3 hours (monthly) of conference / review / drafting time[1] • SOW, quote, and customer redline support • Annual document health check	• Expanded strategic access (hotline access) • **Custom playbooks and templates, including AI-related governance, use, and privacy-related templates and data processing agreements.**[2] • Up to 5 hours (monthly) of conference / review/ drafting time[1] • Quarterly executive risk review • Annual document health check
$1,000/month	**$1950/month**	**$3,500/month**

*All plans require a minimum 3-month commitment. After the initial commitment, plans automatically renew for successive 60-day terms unless either party provides at least 60 days' written notice of non-renewal.

[1] Applies to customer agreements, SOWs, proposals, vendor documents, distributor terms, service guides, and policy documents. Unused monthly hours do not roll over to consecutive months. Hours beyond allocated monthly hours will be billed at the following rates (with Client pre-approval): $500/hour for Essentials; $475/hour for Plus; and $425/hour for Premium.

[2] Updated as required to align with best practices.

Because your legal foundation should evolve as fast as your technology business does.

Contact for more information: Bradley Gross, Esq. info@bradleygross.com

RESELLER / SERVICE PROVIDER CHECKLIST

This checklist is not legal advice. This checklist and plan description are for informational purposes only and do not create an attorney-client relationship unless and until a written engagement agreement is signed. Check with counsel before implementing any suggested change, policy, or procedure.

Contracts & Scope

☐ Every customer must accept your master terms/conditions **before** services are rendered.
☐ Your agreement must cover legal liabilities in an enforceable manner, *e.g. avoid heavily one-sided exclusions and limitations that might be deemed unconscionable.*
☐ Your master agreement must:

- cover the realities of your industry and how those realities will be handled;
- (if applicable) discuss third party licensing and non-cancelable upstream licensing obligations;
- clarify the difference between your warranties and those that are provided by third parties;
- provide an unambiguous refund (or "no refund" policy);
- avoid promising, explicitly or implicitly, specific compliance solutions (unless the service CaaS);
- discuss the difference between your pricing, third party pricing (which could change incrementally), and costs related to the economy that could increase (such as shipping/gas costs);
- discuss availability / shipping delays;
- allocate liability of damaged goods during shipping / after delivery;
- addresses pauses for nonpayment or customer delays;
- include a change order framework;
- include common assumptions and exclusions; and,
- require arbitration as the exclusive dispute resolution process.

Data Privacy, Security & Compliance

☐ Identify what types of data you access, process, store, transmit, or support for customers.
☐ Classify customer data by sensitivity: personal data, financial data, health data, credentials, logs, security data, backups, email, regulated data, etc.
☐ Confirm whether you are acting as a service provider, processor, subprocessor, business associate, reseller, referral partner, or independent contractor.
☐ Make sure your contracts describe what customer data you may access and what you are permitted to do with it.
☐ Confirm where customer data is stored, accessed, processed, or supported, including whether data crosses state, provincial, national, or international borders.
☐ Address cross-border transfers and applicable privacy law requirements.
☐ Maintain written policies for data retention, deletion, return of data, and secure disposal.

AI, Automation & Emerging Technology

☐ Identify whether AI tools process customer data, confidential information, tickets, logs, recordings, or emails.
☐ Prohibit entry of sensitive customer data into unapproved AI tools.
☐ Clarify whether AI output is reviewed by humans before being used with customers.
☐ Address AI-related warranties, disclaimers, ownership, confidentiality, and vendor/tool risk.
☐ Avoid promising that AI tools will produce accurate, complete, compliant, or secure results.

Security

☐ Maintain endpoint protection, patch management, logging, alerting, and vulnerability management.
☐ Maintain a written information security program.

- Assign internal responsibility for security oversight.
- Conduct periodic risk assessments.
- Maintain asset inventories for devices, applications, accounts, vendors, and customer-facing tools.
- Require MFA for administrative accounts, remote access, email, cloud platforms, RMM, PSA, backup, and security tools.
- Use role-based access controls and least privilege.

- Disable accounts promptly when employees or contractors leave.
- Encrypt sensitive data at rest and in transit where appropriate.
- Maintain backup, disaster recovery, and business continuity procedures.
- Align your security program with recognized frameworks such as the NIST Cybersecurity Framework (Govern, Identify, Protect, Detect, Respond, and Recover).

Sales, Quotes & Customer Communications

☐ Make sure quotes and proposals clearly incorporate your master terms.
☐ Avoid inconsistent promises between proposals, emails, SOWs, sales decks, and the MSA.
☐ Train sales teams not to promise compliance, security outcomes, uptime, timelines, cost savings, or third-party product performance unless approved.
☐ Include pass-through terms for hardware, software, cloud, vendor, and distributor obligations.
☐ Clarify when pricing, availability, shipping, tariffs, taxes, vendor costs, and third-party fees can change.