

Partner Program

# Partner Code of Conduct

Effective **1 June 2026**. Applies to every Silver, Gold, and Platinum partner of HackFirstAid and to every employee, contractor, or subcontractor acting on a partner's behalf.

*“Calm guidance for the worst morning of a customer's year.” That is the promise of the HackFirstAid brand, and the standard we hold our partners to. This document spells out what that looks like in practice — especially when a deal is contested, a customer is in active distress, or a competitor is in the room.*

## 1. Our shared values

HackFirstAid was built on three commitments. Every partner accepts these as their own when they represent us.

- **Plain language.** No jargon, no acronyms used as gatekeeping, no theatre. If a school superintendent or a town clerk can't follow what you said, rewrite it.
- **No fear marketing.** Cyber incidents are scary enough on their own. We do not manufacture urgency, exaggerate threat actor capability, or use a customer's fear to accelerate a close.
- **No vendor pitch during a crisis.** When a customer is mid-incident, our job is to triage and stabilize. Cross-sell conversations wait until the customer is out of the woods and has explicitly invited the discussion.

## 2. Customer respect

Our customers are school districts, towns, small businesses, and the volunteer trustees who oversee them. Most are under-resourced. Many are in the worst week of their professional life when they reach us. Partners agree to:

DO	DON'T
Lead with the free triage when it fits — even if it means no fee.	Withhold safety-relevant guidance to leverage a sale.
Quote transparently in writing before any work begins.	Use verbal-only pricing, surprise change orders, or hidden retainers.
Honor the customer's chosen IR firm, counsel, or insurer.	Disparage the customer's existing advisors to displace them.
Decline work outside HackFirstAid scope (higher ed, hospitals/health systems, the O/S&A, or security work).	Handle systems, O/S&A, or security work by proxy.
Treat PHI under the Medical vertical as a regulated workload — Backs signed for signed BAs, even “just to look.”	Backs signed for signed BAs, even “just to look.”
Use the customer's data only to deliver what they hired you for.	Reuse customer data, redacted or not, for marketing without written consent.

## 3. Deal registration ethics

Deal registration exists so partners can invest in a deal without fearing it will be taken from them. The rules below apply to every registered opportunity, regardless of tier.

- **One deal, one partner.** The first partner to register a qualified opportunity owns it for the protection window (60 / 90 / 120 days by tier). HackFirstAid will not run a parallel motion on the same buying entity for the same scope during that window.

- **Qualified means qualified.** Registration requires a named contact, a stated need, and evidence of access. "We know someone on the board" is not a registration. Speculative registrations are rejected and may forfeit future protection.
- **Truth in attribution.** Do not register an opportunity HackFirstAid sourced, an opportunity the customer already had under contract elsewhere, or an opportunity you learned about through a confidential channel (board service, advisory role, etc.).
- **No bracketing.** Do not submit multiple competing bids through different entities you control, and do not coordinate pricing with other HackFirstAid partners on the same deal.
- **Conflicts are resolved in writing.** If two partners register overlapping scope, the Partner Operations Lead reviews evidence within 5 business days and issues a written decision. Appeals go to the Founder within 10 business days.

## 4. Conduct during an active customer incident

When a customer is in the middle of an incident, our shared duty of care outranks every commercial consideration. Partners must:

- Stabilize first. Triage, contain, and communicate. Commercial discussions pause until the customer is out of acute response.
- Respect the customer's chosen incident-response firm, breach coach, counsel, and cyber insurer. Do not displace them, disparage them, or work around them.
- Escalate anything outside your competence or capacity to HackFirstAid within 2 hours. "I can figure it out" is not an acceptable answer when a customer's payroll, transcripts, or 911 dispatch is at stake.
- Document what you did and what you saw. Hand the customer a clean record they can give to their insurer, counsel, and regulators.
- Never advise on ransom payment. Refer the customer to counsel and (if applicable) their cyber insurer. Partners are explicitly prohibited from facilitating, brokering, or transacting ransom payments.

## 5. Use of the HackFirstAid brand

Partners may describe themselves as a HackFirstAid *Silver / Gold / Platinum Partner* for the duration of their active agreement. Partners may not (a) describe themselves as HackFirstAid itself, (b) imply that Travis Barlow or AtlSecCon personally endorses a specific engagement unless explicitly arranged in writing, (c) co-mingle the HackFirstAid logo with a competing IR product's logo on the same surface, or (d) use the brand in fear-based advertising (e.g., "you'll get hacked without us").

Full brand rules — colors, fonts, approved language, lockups — live in the HackFirstAid Press Kit.

## 6. Confidentiality and disclosure

Partners receive non-public information about customers, incidents, vulnerabilities, and HackFirstAid methodology. Treat all of it as confidential by default. Specifically:

- Do not share customer incident details — even sanitized — outside the engagement team without written customer consent.
- Do not name customers in marketing, press, social media, or sales references without an executed Customer Reference Agreement.
- Do not disclose unpatched vulnerabilities or attacker TTPs you observed at a customer to any third party, including security researchers, without HackFirstAid's coordination.

- Honor all customer NDAs, BAAs (mandatory for every Medical-vertical engagement under HIPAA), and DPAs as if they were your own. PHI access without an executed BAA is a Sev-1 violation.

## 7. Escalation paths

If you suspect a violation of this Code — by another partner, by a HackFirstAid employee, or by yourself — use the path below. Reports are treated confidentially. Retaliation against a good-faith reporter is itself a violation of this Code.

Severity	What it looks like	Where to go	Response SLA
Sev 1 — Customer at risk	Active incident is being mishandled; partner is pressuring a customer mid-crisis; ransom is being brokered.	Call the on-call line and email <b>incident-escalation@hackfirstaid.com</b> . The Founder is the named owner.	Acknowledged in 1 hr · resolution path in 4 hrs
Sev 2 — Deal-reg conflict	Two partners claim the same opportunity; suspected attribution gaming; pricing collusion.	Email <b>deal-reg@hackfirstaid.com</b> with evidence (dates, contacts, artifacts). Partner Ops Lead owns.	Decision in 5 business days · appeal to Founder in 10
Sev 3 — Conduct or brand misuse	Fear-based ads, brand co-mingling, customer-respect breaches, confidentiality lapses.	Email <b>conduct@hackfirstaid.com</b> . Partner Ops Lead investigates with written findings.	Investigation opened in 3 business days · findings in 15
Sev 4 — Question or ambiguity	You're not sure if something is allowed. Ask before you act.	Email <b>partners@hackfirstaid.com</b> or DM your Partner Ops contact.	Reply within 2 business days

## 8. Consequences of violation

Violations are addressed proportionally. The standard ladder is: written warning → deal-reg forfeiture → tier demotion → suspension → termination. Severe violations — Sev-1 customer harm, ransom facilitation, fraudulent attribution, or retaliation against a reporter — may result in immediate termination and forfeiture of all open referral and resale earnings.

## 9. Acknowledgement

Each partner organization names a Code Owner — typically the executive who signed the Partner Agreement — who is responsible for keeping this Code in front of their team and re-signing annually. New employees joining a partner organization in a customer-facing role must acknowledge the Code within 30 days of hire.

**Partner organization** \_\_\_\_\_

**Code Owner (printed)** \_\_\_\_\_

**Title** \_\_\_\_\_

**Signature** \_\_\_\_\_

**Date** \_\_\_\_\_

*By signing, the Code Owner confirms that the partner organization has read, understood, and will abide by the HackFirstAid Partner Code of Conduct, and accepts the escalation, consequence, and confidentiality terms herein.*