



Code of Ethics

Sparkhound

1. Executive Overview

Sparkhound's Code of Ethics Policy establishes the foundational principles that govern the conduct of all workforce members, principals, officers, and contractors in the performance of company business. This policy affirms Sparkhound's unwavering commitment to legal compliance, integrity, transparency, and fair dealing - values that are essential to maintaining customer trust, protecting company assets, and sustaining long-term business success. In an environment where competitive pressures can tempt shortcuts, this Code provides clear guidance on what is expected of every individual who represents Sparkhound.

From a risk management perspective, a robust Code of Ethics directly supports Sparkhound's obligations under multiple regulatory frameworks including HIPAA's workforce conduct requirements, the FTC Safeguards Rule's administrative safeguards provisions, NIST SP 800-53 personnel security controls, and ISO/IEC 27001:2022 human resource security requirements. The policy addresses critical risk areas including conflicts of interest, misuse of confidential information, insider trading, improper use of company property, gift restrictions, and the requirement to report known or suspected violations. These provisions collectively reduce legal exposure, reputational risk, and cybersecurity risk arising from insider threats.

Leadership at Sparkhound is accountable for modeling ethical behavior, communicating this policy to their teams, and ensuring that a culture of integrity is embedded throughout the organization. The Code is not merely a compliance checkbox - it is a living framework that guides decision-making at every level. By adhering to this policy, Sparkhound protects itself, its clients, its partners, and the communities it serves, while demonstrating to auditors, insurers, and regulators that its governance practices meet or exceed industry standards.

2. Purpose

The purpose of this Code of Ethics Policy is to establish clear, enforceable standards of professional and ethical conduct for all workforce members, principals, officers, and contractors of Sparkhound. This policy is designed to ensure that every individual associated with Sparkhound understands their obligation to act with integrity, comply with applicable laws and regulations, protect confidential information, avoid conflicts of interest, and promptly report known or suspected violations. The Code exists to preserve the trust of customers, partners, and the public, and to protect Sparkhound from legal, financial, and reputational harm that results from unethical conduct.

This policy also fulfills compliance requirements under multiple regulatory and industry frameworks. HIPAA requires covered entities to implement workforce conduct and sanctions

policies as part of its administrative safeguards. The FTC Safeguards Rule mandates that companies implement policies governing employee handling of customer information. NIST SP 800-53 Rev 5 and NIST SP 800-171 Rev 2 both require personnel security controls including rules of behavior. ISO/IEC 27001:2022 requires human resource security policies covering acceptable behavior and responsibilities. Additionally, cyber liability insurance underwriters routinely assess whether a company has documented ethics and acceptable use policies as part of their risk evaluation process. This policy satisfies those requirements and positions Sparkhound for successful audits, assessments, and insurance renewals.

3. Scope

- All Employees, contractors, external consultants and owners of Sparkhound and its subsidiaries are subject to this policy in all aspects of their work-related conduct.
- All Business Activities: This policy applies to all actions taken in connection with Sparkhound's business operations, whether conducted on company premises, remotely, or at client or partner locations.
- All Systems and Information: This policy governs the handling of all company, customer, and vendor information and all use of Sparkhound's technology assets, regardless of location or device.
- Geographic Scope: This policy applies to all locations where Sparkhound and its subsidiaries operate.

4. Policy

Compliance with Laws

1. All workforce members must conduct Sparkhound business in full compliance with all applicable federal, state, and local laws, rules, and regulations, including but not limited to data privacy laws, securities laws, anti-corruption laws, and employment laws.
2. Laws and regulations change frequently. Workforce members are responsible for staying informed about requirements relevant to their roles and must seek guidance when uncertain.
3. Questions about legal compliance obligations should be directed to Human Resources or the designated Speak Up Line.

Public Disclosure and Reports

4. No workforce member may make public disclosures on behalf of Sparkhound without prior authorization from company leadership.

5. All authorized public disclosures, communications, and reports must be full, fair, accurate, timely, and understandable, and must not omit material information that would make such disclosures misleading.
6. This requirement applies to regulatory filings, press releases, marketing materials, social media posts, and any other public-facing communications.

Conflicts of Interest

7. Workforce members must avoid any personal activity, investment, or association that could interfere with their objective judgment in acting in Sparkhound's best interests.
8. Workforce members may not use their position or relationship with Sparkhound for personal financial gain outside of their approved compensation.
9. Even the appearance of a conflict of interest must be avoided. Workforce members must disclose any potential conflict, including financial interests held by immediate family members, to Human Resources promptly.
10. Examples of conflicts include holding a financial interest in a supplier, customer, or competitor of Sparkhound, or receiving personal benefits from a third party who does business with Sparkhound.
11. Disclosure of potential conflicts does not automatically constitute a violation; undisclosed conflicts do.

Misuse of Information

12. Workforce members may not use, disclose, or misappropriate confidential information belonging to Sparkhound, its customers, or its vendors for any unauthorized purpose.
13. Confidential information includes but is not limited to: business strategies, pricing data, marketing plans, software and source code, experimental research, and information about current, former, or prospective customers and employees.
14. These obligations survive the termination of a workforce member's relationship with Sparkhound.
15. All workforce members must comply with Sparkhound's data classification and handling procedures when managing confidential information.

Improper Use or Theft of Company Property

16. Workforce members are required to safeguard all Sparkhound property - physical and digital - from loss, theft, damage, or unauthorized use.
17. Company property includes but is not limited to: confidential information, software, computers, mobile devices, office equipment, and supplies.
18. Company property may not be taken or used for personal purposes without explicit written authorization.
19. Workforce members must appropriately secure all company property within their control, including locking devices when unattended and using approved encryption where

required.

Gifts

20. Workforce members and their immediate family members may not give or receive gifts, travel, or entertainment of more than modest value to or from Sparkhound's customers, vendors, or business partners.
21. Gifts that could be perceived as influencing a business decision are strictly prohibited, regardless of value.
22. Any gift of questionable appropriateness must be disclosed to Human Resources before acceptance or provision.
23. All gift and entertainment activities must be consistent with applicable laws, including anti-bribery and anti-corruption regulations.

Communications

24. All internal and external communications made on behalf of Sparkhound must be accurate, complete, and forthright.
25. This requirement applies to all communication channels including advertising, marketing materials, broadcast media, sales presentations, internal reports, memoranda, and electronic communications.
26. Workforce members must not make false, misleading, or deceptive statements in any company communication.

Fair Dealing

27. Workforce members must deal fairly and honestly with Sparkhound's customers, suppliers, competitors, and colleagues.
28. Unfair practices are prohibited, including manipulation, concealment of material facts, misrepresentation, abuse of privileged information, and any other deceptive practice.
29. Sparkhound is committed to competing vigorously but always within the bounds of applicable law and ethical standards.

Securities Trading

30. Workforce members are prohibited from buying or selling securities of Sparkhound or any client, vendor, or partner while in possession of material, non-public (inside) information.
31. Workforce members may not share inside information with others who might use it for trading purposes - doing so may expose both the sharer and the recipient to legal liability.
32. Immediate family members of workforce members are also subject to these restrictions with respect to information obtained through the workforce member's position.

33. Any uncertainty about securities trading obligations must be directed to Human Resources or the Speak Up Line before any transaction is executed.

Implementation of the Code of Ethics

34. All managers are responsible for communicating this Code to workforce members under their supervision and ensuring understanding and compliance.
35. This policy will be maintained electronically and published on Sparkhound's internal systems and website.
36. Revisions and updates to this Code will be distributed to all workforce members and acknowledged as directed by Human Resources.
37. Ethics training will be provided to all workforce members as part of onboarding and on a periodic basis thereafter.

Making the Right Choices

38. When facing an ethical dilemma not explicitly covered by this Code, workforce members are expected to exercise sound judgment guided by Sparkhound's values of honesty, integrity, and respect.
39. A useful test: ask whether you would be comfortable if your decision appeared in a news report or was reviewed by company leadership, regulators, or customers.
40. When in doubt, workforce members must seek guidance from their manager, Human Resources, or the Speak Up Line before taking action.

Reporting Violations

41. SPEAK UP - REPORT A CONCERN: Concerns under this Code can also be reported through Sparkhound's Speak Up program - anonymously if preferred - in addition to a manager or Human Resources: email Speakup@Sparkhound.com, or submit the Speak Up Form, available at www.sparkhound.com and on SPOT (Sparkhound's intranet). Reports made in good faith are protected from retaliation under Sparkhound's Whistleblower & Non-Retaliation Policy.

Failure to Report

42. Failure to report a known violation of this Code or applicable law is itself a violation of this policy.
43. Workforce members who knowingly conceal violations may be subject to the same disciplinary consequences as those who committed the original violation, up to and including termination of employment.

Non-Retaliation

44. Sparkhound strictly prohibits retaliation against any workforce member who in good faith reports a suspected or actual violation of this Code. Non-retaliation protections and the

process for reporting retaliation are set out in full in Sparkhound's Whistleblower & Non-Retaliation Policy.

Other Policies

- 45. This Code of Ethics must be read and applied in conjunction with all other Sparkhound policies, standards, procedures, and guidelines.
- 46. In cases of conflict between this Code and another policy, the more restrictive or protective standard applies, and Human Resources should be consulted for guidance.

Right to Change

- 47. This Code of Ethics is not a contract of employment and does not create any contractual rights or obligations.
- 48. Sparkhound reserves the right to amend, modify, suspend, interpret, or eliminate any provision of this Code at any time, with or without prior notice, subject to applicable legal requirements.
- 49. Workforce members will be notified of material changes to this Code and may be required to acknowledge the updated version.

5. Enforcement

Sparkhound takes violations of this Code of Ethics seriously. Compliance with this policy is a condition of continued employment or engagement with Sparkhound. Violations - including failure to report known violations - will be investigated and may result in disciplinary action commensurate with the severity of the offense, up to and including immediate termination of employment or termination of a contractor or vendor relationship. In cases where violations involve potential criminal conduct, Sparkhound may refer the matter to appropriate law enforcement authorities.

Enforcement of this policy is the shared responsibility of all managers, Human Resources, and senior leadership. The reporting, investigation, and disciplinary escalation process is governed by Sparkhound's Whistleblower & Non-Retaliation Policy.

Retaliation against any workforce member who reports a violation in good faith is itself a serious violation of this policy and will be subject to disciplinary action up to and including termination. Sparkhound is committed to ensuring that all workforce members can report concerns without fear of reprisal.

6. Roles and Responsibilities

Employees, Contractors and External Consultants - Read, understand, and comply with this Code of Ethics in all work-related activities; report suspected violations promptly; complete required ethics training; protect confidential information and company property; avoid conflicts of interest and disclose them when they arise.

Managers and Supervisors - Communicate this Code to all direct reports; model ethical behavior; promptly escalate reported violations to Human Resources and senior leadership; ensure workforce members under their supervision complete required ethics training; address minor concerns proactively and refer serious matters for formal investigation.

Human Resources - Maintain and update this Code of Ethics Policy; advise workforce members and leadership on ethical and compliance questions; ensure the policy is communicated and accessible to all workforce members; report significant compliance matters to senior leadership and the board as appropriate. Reporting-channel oversight and investigations are governed by the Whistleblower & Non-Retaliation Policy. Coordinate disciplinary actions resulting from Code violations in partnership with Legal and management; maintain records of investigations and outcomes; integrate Code of Ethics requirements into onboarding, training, and performance management processes; ensure workforce members acknowledge this policy upon hire and following updates. Address ethics matters involving the handling of personal data, customer information, or privacy-related obligations; ensure Code provisions related to information misuse are aligned with applicable privacy laws including HIPAA and applicable state privacy regulations.

IT / Security Team - Provide guidance on matters involving information security, data confidentiality, insider threat, and improper use of company systems or data; support investigations involving technology-related conduct; ensure ethics obligations are aligned with information security policies and controls.

Executive Committee - The Executive Committee is responsible for reviewing the design and operating effectiveness of Sparkhound's internal controls, evaluating risks to the company's objectives, and holding the CEO accountable for performance against this Code of Ethics and Sparkhound's other governing policies. At least one member of the Executive Committee is independent of the day-to-day execution of the controls under review and does not report to the CEO in that capacity, providing an objective check on management decisions. The Executive Committee meets no less than quarterly to review control performance, significant risks, incidents, and the CEO's conduct relative to this Code, and has the authority to request additional information or direct corrective action.

7. Other Provisions as Required by Laws

This Code of Ethics Policy is subject to and must be interpreted in light of the following legal, regulatory, and contractual obligations. Workforce members and leadership should be aware that violations of this Code may also constitute violations of applicable law, triggering civil penalties, criminal liability, or regulatory sanctions.

- **Sarbanes-Oxley Act (SOX) — Section 301 and 406:** Requires public companies to adopt a code of ethics for senior financial officers and establish confidential reporting mechanisms for employees. Relevant to public disclosure and securities trading provisions. (<https://www.sec.gov/divisions/corpfin/guidance/codeofethics101703.htm>)
- **HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164):** Require workforce members to handle protected health information (PHI) in accordance with established policies and impose sanctions for violations. Relevant to the information misuse and confidentiality provisions of this Code. (<https://www.hhs.gov/hipaa/for-professionals/security/index.html>)
- **FTC Safeguards Rule (16 CFR Part 314):** Requires financial institutions and related entities to implement safeguards for customer financial information, including employee training and conduct requirements. Relevant to information handling and confidentiality provisions. (<https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>)
- **Securities Exchange Act of 1934 — Insider Trading Provisions:** Federal law prohibiting trading in securities based on material non-public information. Violations may result in civil and criminal penalties. Directly relevant to the securities trading provisions of this Code. (<https://www.sec.gov/divisions/enforce/insider-trading.shtml>)
- **Foreign Corrupt Practices Act (FCPA) and UK Bribery Act:** Anti-corruption laws prohibiting bribery of government officials and others. Relevant to gift, entertainment, and fair dealing provisions. (<https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act>)
- **State and Federal Whistleblower Protection Laws:** Multiple federal and state laws protect employees who report violations of law from retaliation, including the Dodd-Frank Act and Sarbanes-Oxley whistleblower protections. These laws reinforce and supplement the non-retaliation provisions of this Code. (<https://www.sec.gov/whistleblower>)
- **NIST SP 800-53 Rev 5 — Personnel Security (PS) Controls:** Federal security controls including PS-6 (Access Agreements) and PS-8 (Personnel Sanctions) that require documented conduct requirements and consequences for violations. Applicable to all workforce members with access to federal systems or data. (<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>)
- **ISO/IEC 27001:2022 — Human Resource Security (Section A.6):** Requires organizations to ensure that workforce members understand their information security responsibilities and that terms and conditions of employment include security obligations. (<https://www.iso.org/standard/82875.html>)

- **Cyber Liability Insurance Requirements:** Many cyber insurance policies require evidence of documented employee conduct policies, ethics training, and incident reporting mechanisms as conditions of coverage. Non-compliance with this Code may affect Sparkhound's ability to obtain or maintain cyber liability insurance coverage.

8. Related Standards

- **HIPAA Security Rule (45 CFR §164.308 – Administrative Safeguards):** Requires covered entities and business associates to implement policies governing workforce conduct, sanctions for violations, and training. This Code supports HIPAA workforce security requirements.
- **NIST Cybersecurity Framework (CSF) — Govern (GV) and Protect (PR) Functions:** The CSF Govern function requires organizations to establish and communicate policies, procedures, and expectations for cybersecurity risk management, including ethics and conduct. This Code directly supports the GV.PO (Policy) and GV.OC (Organizational Context) categories.
- **NIST SP 800-53 Rev 5 — Personnel Security (PS) Family:** Controls PS-3 (Personnel Screening), PS-6 (Access Agreements), PS-7 (External Personnel Security), and PS-8 (Personnel Sanctions) require documented behavioral expectations and enforcement mechanisms for all workforce members.
- **NIST SP 800-171 Rev 2 / CMMC — 3.1 (Access Control) and 3.2 (Awareness and Training):** Requires organizations handling Controlled Unclassified Information (CUI) to establish rules of behavior for all workforce members with access to CUI and to train them accordingly.
- **FTC Safeguards Rule (16 CFR Part 314):** Requires financial institutions to implement information security programs that include employee conduct policies, training, and oversight of service providers. This Code supports Safeguards Rule compliance.
- **SOC 2 Trust Services Criteria — CC1 (Control Environment) and CC2 (Communication and Information):** SOC 2 requires organizations to demonstrate a commitment to integrity and ethical values (CC1.1) and to communicate those values to all relevant parties (CC2.2). This Code directly supports SOC 2 CC1 and CC2 criteria.
- **ISO/IEC 27001:2022 — Section A.6 (People Controls):** Requires that terms and conditions of employment include information security responsibilities, that workforce members receive awareness training, and that a disciplinary process exists for violations. This Code addresses all three requirements.
- **Acceptable Use Policy:** Governs the authorized use of Sparkhound's technology assets and systems by all workforce members, complementing the property use and information misuse provisions of this Code.
- **Information Security Policy:** Establishes the overarching framework for protecting Sparkhound's information assets, including classification, handling, access control, and

incident response requirements.

- **Privacy Policy:** Defines Sparkhound's obligations and practices with respect to the collection, use, storage, and disclosure of personal information, complementing the information confidentiality provisions of this Code.
- **Incident Response Policy:** Defines the procedures for identifying, reporting, and responding to security incidents, including those arising from employee misconduct or insider threats.
- **Human Resources Policy:** Governs employment practices, onboarding, training, performance management, and disciplinary procedures that support enforcement of this Code.
- **Whistleblower & Non-Retaliation Policy,** which governs the reporting channels, investigation process, and non-retaliation protections referenced throughout Sections 3.12 and 4 of this Code.

9. Definition and Terms

Workforce Member: Any individual whose conduct in the performance of work for Sparkhound is under the direct control of Sparkhound, regardless of whether they are compensated. Includes employees, contractors and external consultants.

Code of Ethics (the Code): This document and all of its provisions establishing the standards of professional, legal, and ethical conduct required of all workforce members and principals of Sparkhound.

Confidential Information: Any non-public information belonging to Sparkhound, its customers, or its vendors that is not intended for public disclosure, including but not limited to business strategies, pricing data, marketing plans, software and source code, personnel information, and customer data.

Conflict of Interest: Any situation in which a workforce member's personal interests, financial interests, or outside activities could - or could appear to - interfere with their ability to act objectively and in the best interests of Sparkhound.

Speak Up Line: The designated confidential reporting channel established by Sparkhound through which workforce members may report actual or suspected violations of this Code, seek ethical guidance, or raise compliance concerns. Contact information for the Speak Up Line is maintained by Human Resources and distributed to all workforce members.

Inside Information (Material Non-Public Information): Information about a company that has not been made available to the general public and that a reasonable investor would consider important in making a decision to buy, sell, or hold securities of that company.

Insider Trading: The illegal practice of buying or selling securities while in possession of material non-public (inside) information about the issuing company, or the illegal sharing of such information with others who then trade on it.

Gift: Anything of value - including cash, merchandise, discounts, services, meals, entertainment, travel, or other benefits - given to or received from a customer, vendor, competitor, government official, or other third party in connection with Sparkhound business.

Retaliation: Any adverse action - including termination, demotion, harassment, exclusion, or other negative treatment - taken against a workforce member because they reported a suspected violation of this Code or participated in an investigation of a potential violation.

Principal: A founder, executive officer, director, or other senior leader of Sparkhound who holds a position of authority and fiduciary responsibility within the organization.

Securities: Financial instruments such as stocks, bonds, options, and other investments issued by a company, government, or other entity that can be bought and sold in public or private markets.

Public Disclosure: Any communication made to the general public, regulatory bodies, investors, or media on behalf of Sparkhound, including press releases, financial filings, advertising, and social media communications.

Fair Dealing: The practice of conducting business with honesty, transparency, and integrity - without manipulation, misrepresentation, concealment of material facts, or other deceptive practices.

Data Classification: The process of categorizing company information according to its sensitivity and the level of protection it requires. This Code applies most directly to information classified as Confidential or Sensitive by Sparkhound.

