SwiftBite
Internal Policy Handbook

Version 4.2 | January 2026

Page 1: Introduction & Code of Conduct

1.1 Mission & Vision

SwiftBite aims to revolutionize the food logistics industry by bridging the gap between culinary excellence and consumer convenience. Our mission is to deliver not just meals, but moments of joy, ensuring that every interaction-from the app interface to the doorstep delivery-is seamless, reliable, and delightful. We envision a world where quality food is accessible to everyone, everywhere, within minutes, powered by ethical practices and cutting-edge technology.

1.2 Core Values

* Customer Obsession: Every decision starts with the customer and works backward. We earn and keep customer trust.
* Bias for Action: Speed matters in business. We value calculated risk-taking.
* Integrity: We act with honesty and adhere to the highest ethical standards in all interactions.
* Ownership: Leaders are owners. They think long-term and do not sacrifice long-term value for short-term results.

1.3 Professional Code of Conduct

All employees, contractors, and partners are expected to maintain the highest standards of professional conduct. This includes treating colleagues, merchants, and customers with respect and dignity. Unprofessional behavior such as shouting, use of profanity, intimidation, or public disparagement of the company is strictly prohibited. Employees must dress appropriately for their roles, particularly those in customer-facing positions or video conferences. Punctuality for meetings and responsiveness to internal communications are mandatory to ensure operational efficiency.

1.4 Anti-Harassment & Non-Discrimination

SwiftBite is committed to providing a work environment free of discrimination and harassment. We do not tolerate harassment based on race, color, religion, sex, national origin, age, disability, or genetic information. Sexual harassment, including unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature, is strictly prohibited. Any employee who believes they have been harassed should report the incident immediately to HR. All complaints will be investigated promptly and confidentially. Retaliation against anyone reporting harassment is grounds for immediate termination.

1.5 Conflict of Interest

Employees must avoid situations where their personal interests conflict, or appear to conflict, with the interests of SwiftBite. This includes, but is not limited to, holding a significant financial interest in a competitor, supplier, or partner; accepting gifts of more than nominal value ($50) from vendors; or using company resources for personal gain. Outside employment (moonlighting) is permitted only if it does not interfere with job performance or pose a conflict of interest, and must be disclosed to the immediate supervisor for approval.

1.6 Social Media Policy

Employees are responsible for the content they publish on social media. While we respect the right to personal expression, employees must not post confidential information, trade secrets, or material that could harm the company's reputation. When posting about work-related matters, employees should clearly state that their views are their own and do not represent SwiftBite. Harassment or bullying of colleagues on social media platforms is a violation of the company's anti-harassment policy.

Page 2: Employment & Workplace Guidelines

2.1 Recruitment & Onboarding

Recruitment at SwiftBite is merit-based. We prioritize skills, cultural fit, and potential for growth. All job openings must be posted internally for at least three days before external recruitment begins. The onboarding process includes a mandatory one-week orientation covering company history, tools training, and compliance workshops. New hires are on a probationary period of 90 days, during which performance goals are set and reviewed monthly. Failure to meet these initial benchmarks may result in the extension of probation or termination of employment.

2.2 Attendance & Leave Policy

Standard working hours are 9:00 AM to 6:00 PM, Monday through Friday, though this may vary for operations and support teams. Employees are expected to be available during core hours (10:00 AM - 4:00 PM). SwiftBite offers a flexible leave policy including 20 days of Paid Time Off (PTO), 10 days of Sick Leave, and observed public holidays. Leave requests exceeding three consecutive days must be submitted at least two weeks in advance. Unplanned absences must be reported to the manager by 9:30 AM on the day of absence. Excessive absenteeism or tardiness will trigger a disciplinary review.

2.3 Remote Work & Telecommuting

Eligible employees may work remotely up to three days a week under the Hybrid Work Model. Remote workers must ensure they have a stable internet connection and a quiet, secure workspace. They must remain accessible via Slack and email during work hours. Company-issued laptops must be used for all work tasks to ensure data security. The company reserves the right to revoke remote work privileges if performance declines or if business needs require in-office presence. Fully remote positions are subject to specific contracts and may require quarterly in-person visits to headquarters.

2.4 Performance Management

Performance reviews are conducted semi-annually in June and December. The review process involves self-assessment, peer feedback (360-degree review), and manager evaluation. Key Performance Indicators (KPIs) are agreed upon at the start of each cycle. Ratings range from "Does Not Meet Expectations" to "Exceeds Expectations." Employees receiving the lowest rating will be placed on a Performance Improvement Plan (PIP) for 60 days. Successful completion of the PIP is required for continued employment. Promotions and salary adjustments are directly tied to these performance outcomes.

2.5 Termination & Separation

Employment is "at-will," meaning either the employee or SwiftBite can terminate the relationship at any time. Resigning employees are requested to provide a two-week notice period to facilitate a smooth handover. In cases of termination for cause (e.g., gross misconduct, theft, data breach), dismissal is immediate without severance. For layoffs or restructuring, severance packages are determined based on tenure and role. All separating employees must undergo an exit interview and return all company assets, including badges, devices, and access keys, on their final day.

2.6 Workplace Relationships

Consensual romantic relationships between co-workers are discouraged but not prohibited unless they involve a direct reporting line. If a relationship develops between a manager and a subordinate, it must be disclosed to HR immediately so that reporting lines can be adjusted to prevent favoritism or conflicts of interest. Failure to disclose such relationships may result in disciplinary action for both parties.

Page 3: Data Privacy & Security Protocols

3.1 Data Classification & Handling

Data at SwiftBite is classified into three categories: Public, Internal, and Confidential. Public data is safe for general release. Internal data (e.g., organizational charts, internal memos) is for employee use only. Confidential data includes customer PII (Personally Identifiable Information), payment details, algorithm source code, and merchant contracts. Confidential data must be encrypted both in transit and at rest. Access to confidential data is granted on a "need-to-know" basis and requires multi-factor authentication (MFA).

3.2 Customer Data Protection

We adhere strictly to GDPR, CCPA, and local data protection laws. Customer data (names, addresses, order history) may only be accessed for legitimate business purposes such as order fulfillment or support resolution. It is strictly prohibited to download customer databases to personal devices or external drives. Sharing customer contact details with third parties without explicit consent is a fireable offense. Anonymized data may be used for analytics and marketing, provided it cannot be reverse-engineered to identify individuals.

3.3 Cybersecurity Measures

All company devices must have the IT-approved antivirus and endpoint protection software installed and active. Employees must not disable these security features. Passwords must be at least 12 characters long, complex, and changed every 90 days. Phishing simulations are conducted monthly; employees who fail these tests repeatedly will be required to undergo remedial security training. The use of unauthorized software (Shadow IT) is prohibited. All software installations must be vetted and approved by the IT Security team.

3.4 Device Management (BYOD)

SwiftBite generally issues company devices. However, where Bring Your Own Device (BYOD) is authorized, the device must be enrolled in the Mobile Device Management (MDM) system. This allows IT to enforce security policies and remotely wipe corporate data in case of device loss or theft. Employees are responsible for the physical security of their devices. Leaving a laptop unlocked and unattended in a public space is a violation of security policy. Lost or stolen devices must be reported to the IT Helpdesk within 2 hours of discovery.

3.5 Data Breach Response

In the event of a suspected or confirmed data breach, the incident must be reported immediately to the Chief Information Security Officer (CISO). The Incident Response Team (IRT) will be activated to contain the breach, assess the impact, and notify affected parties. Employees must not speak to the media or post about the breach on social media. All external communication regarding security incidents is handled exclusively by the Legal and PR departments. Post-incident reviews will be conducted to identify root causes and prevent recurrence.

3.6 Third-Party Data Sharing

When sharing data with vendors, partners, or API integrators, a Data Processing Agreement (DPA) must be signed. This agreement ensures the third party adheres to SwiftBite's security standards. Regular audits of third-party security practices are conducted annually. If a vendor fails to meet security requirements, the partnership will be suspended until remediation is verified. We do not sell customer data to data brokers.

Page 4: Delivery Operations & Fleet Management

4.1 Rider Recruitment & Vetting

Delivery partners (riders) are the face of SwiftBite. Applicants must pass a background check, including criminal record and driving history reviews. Valid driver's licenses and vehicle registration are mandatory for motorized delivery. Riders must also complete a food handling safety course. Vehicles used for delivery must meet local emission standards and be less than 10 years old. We reserve the right to reject applicants with a history of violent offenses, theft, or severe traffic violations.

4.2 Delivery Gear & Branding

Riders are required to use SwiftBite-branded insulated delivery bags to ensure food temperature and hygiene are maintained. While wearing branded apparel is optional for independent contractors, using the branded equipment is mandatory for quality assurance. The insulated bag must be kept clean and sanitized daily. Failure to use the proper equipment during a delivery can result in penalties or deactivation from the platform. Riders are responsible for replacing damaged gear at their own cost or through company subsidy programs.

4.3 Code of Conduct for Riders

Riders must adhere to all traffic laws and speed limits. Reckless driving reported by customers or pedestrians will be investigated and may lead to suspension. Riders must not open food containers or tamper with orders. "Contactless delivery" protocols must be followed strictly when requested. Interactions with customers and restaurant staff must be polite. Any form of aggression, harassment, or intoxication while on duty will result in immediate permanent deactivation.

4.4 Order Handling & Timeliness

Riders are evaluated on metrics including Acceptance Rate, Completion Rate, and On-Time Arrival. Consistently late deliveries without valid reasons (e.g., extreme weather, accidents) affect the rider's tier status and earnings multiplier. Riders must verify the order number and customer name at the restaurant before pickup to prevent mix-ups. If a customer is unreachable upon arrival, the rider must wait for 5 minutes and attempt to contact them twice via the app before marking the delivery as failed.

4.5 Accident & Incident Reporting

If a rider is involved in a traffic accident while on an active delivery, their safety is the priority. They must contact emergency services if needed and then notify SwiftBite Rider Support. Insurance coverage provided by SwiftBite applies only from the moment an order is accepted until it is delivered. Riders must document the accident with photos and police reports where applicable. False claims for insurance or compensation are considered fraud and will be prosecuted.

4.6 Vehicle Maintenance & Sustainability

Riders are responsible for the maintenance and fuel costs of their vehicles. SwiftBite incentivizes the use of electric vehicles (EVs) and bicycles through the "Green Mile" program, offering higher base pay for zero-emission deliveries. Periodic vehicle inspections may be requested. Riders using bicycles must ensure they have functioning lights and wear helmets at all times.

Page 5: Customer Support & Service Standards

5.1 Customer Interaction Guidelines

Support agents must use the "EMPATHY" framework: Engage, Mirror, Probe, Apologize, Take Action, Thank, and Yield. Interactions should be professional yet conversational, avoiding overly robotic scripts. Agents must not interrupt the customer and should aim for First Contact Resolution (FCR). Profanity or abuse from customers is not tolerated; agents are empowered to warn the customer and, if the behavior continues, politely disconnect the chat or call after documenting the incident.

5.2 Complaint Resolution & Compensation

Agents have a tiered authority limit for issuing refunds and credits. Level 1 agents can issue credits up to $20; amounts above this require Team Lead approval. Refunds are processed to the original payment method within 5-7 business days. Compensation is offered for missing items, incorrect orders, or severe delays (>45 minutes). We do not offer compensation for taste preferences unless the food is spoiled or undercooked. "Appeasement abuse" by customers (frequent false claims) is monitored, and accounts flagged for fraud may be suspended.

5.3 Handling Food Safety Incidents

Reports of food poisoning or foreign objects in food are treated as "Critical Incidents." The agent must immediately escalate the ticket to the Safety Response Team. The customer will be asked to provide photo evidence and medical reports if applicable. The restaurant partner is notified immediately to pause orders while an internal investigation is conducted. If the restaurant is found at fault, they are liable for damages and may be removed from the platform.

5.4 Privacy in Support

Support agents must verify the identity of the customer before discussing account details. Verification methods include confirming the last order details or the email address on file. Agents must never ask for full credit card numbers or passwords. Screen sharing with customers is prohibited. All support chats and calls are recorded for quality assurance and training purposes; this must be disclosed to the customer at the start of the interaction.

5.5 Social Media & Crisis Communication

The Customer Support team works closely with Marketing to handle public complaints on social media. Public responses should be prompt (within 1 hour) and encourage the user to move the conversation to a direct message (DM) for resolution. In the event of a widespread service outage, official communication templates approved by the Crisis Management Team must be used. Agents should not speculate on the cause of outages or give estimated fix times unless confirmed by Engineering.

5.6 VIP & Subscription Support

Subscribers to "SwiftBite Gold" receive priority support routing, bypassing standard queues. Agents handling VIP accounts receive specialized training to provide concierge-level service. Compensation policies for Gold members are more generous, often involving instant credits without standard approval workflows, to ensure retention of high-value users.

Page 6: Merchant Partnership Guidelines

6.1 Merchant Onboarding & Validation

To partner with SwiftBite, restaurants must provide valid business licenses, health inspection certificates (rated B or higher), and tax identification documents. We do not partner with "ghost kitchens" that operate out of residential addresses unless they meet specific commercial zoning and hygiene standards. Menus must be submitted with accurate descriptions, allergen information, and high-resolution photos. The onboarding process includes a tablet setup and training session on the Merchant Portal.

6.2 Quality Control & Hygiene

Merchants are expected to maintain high hygiene standards. SwiftBite reserves the right to conduct unannounced "mystery shopper" audits. If a restaurant's rating drops below 3.5 stars, they are placed on a "Quality Watchlist." Failure to improve within 30 days results in suspension. Packaging must be tamper-evident (e.g., sealed with stickers) and spill-proof. Using non-recyclable plastic packaging is discouraged and may incur a sustainability surcharge in certain jurisdictions.

6.3 Commission & Payout Structure

The standard commission rate is 25% on delivery orders and 10% on pickup orders. Exclusive partners may negotiate lower rates. Payouts are processed weekly on Tuesdays for the previous week's sales, net of commission and any adjustments for refunds caused by restaurant error (e.g., missing items). Merchants can opt for daily payouts for a small processing fee. Disputes regarding payouts must be raised within 14 days of the statement date.

6.4 Order Management Protocols

Merchants must update their preparation times in real-time to ensure accurate delivery estimates. Orders must be accepted within 2 minutes of receipt on the tablet. Auto-acceptance can be enabled but requires strict adherence to prep times. If a restaurant runs out of an item, they must update the menu immediately. Calling the customer to substitute items is permitted but discouraged; cancelling the item via the portal is the preferred process. High cancellation rates by the merchant negatively impact their algorithm ranking.

6.5 Marketing & Promotions

Merchants can purchase "Featured" slots on the app homepage. All promotional assets must adhere to SwiftBite's brand guidelines. Co-funded promotions (e.g., "Buy One Get One Free") require prior approval from the Account Manager. SwiftBite strictly prohibits "markups" where menu prices on the app are significantly higher than in-store prices. Price parity is monitored, and violators may be suppressed in search results.

6.6 Termination of Partnership

SwiftBite may terminate a partnership with 30 days' notice for any reason. Immediate termination occurs for severe violations, including health code failures, fraudulent activity (e.g., fake orders to boost ratings), or abusive behavior toward riders. Upon termination, the merchant must return all leased hardware (tablets, printers) within 7 days. Outstanding payments will be held for 90 days to cover potential chargebacks or customer refunds.

Page 7: Financial Policies & Expense Management

7.1 Payroll & Compensation

Salaries are paid on the 25th of each month. If the 25th falls on a weekend, payment is made on the preceding Friday. Payroll discrepancies must be reported to the Finance Department within 3 business days. Bonuses and commissions are calculated quarterly and paid out in the second month of the following quarter. SwiftBite contributes to statutory retirement funds and insurance plans as mandated by local labor laws.

7.2 Expense Reimbursement

Employees can claim reimbursement for business-related expenses such as travel, client entertainment, and software subscriptions. All expenses must be pre-approved by the line manager. Claims must be submitted via the "ExpenseOne" portal within 30 days of incurring the cost, accompanied by valid digital receipts. The limit for client dinners is $75 per person. Alcohol is reimbursable only for client entertainment, not for solo meals or internal team lunches, unless authorized for a specific celebration.

7.3 Procurement & Vendor Management

Purchases exceeding $1,000 require three competitive quotes. Purchases over $10,000 require approval from the CFO. The Procurement team maintains a list of preferred vendors who offer negotiated rates. Employees must not split purchase orders to bypass approval limits (structuring). Signing contracts on behalf of SwiftBite is restricted to Director-level employees and above, and all contracts must be reviewed by Legal before signing.

7.4 Corporate Credit Cards

Corporate cards are issued to senior management and employees with frequent travel needs. Personal expenses on corporate cards are strictly prohibited. Cash withdrawals on credit cards are blocked. Lost cards must be reported immediately. Card statements are audited monthly; failure to provide receipts for transactions results in the amount being deducted from the employee's next paycheck.

7.5 Fraud Prevention & AML

SwiftBite adheres to Anti-Money Laundering (AML) regulations. We monitor transactions for suspicious patterns, such as unusually large orders, rapid frequency of high-value orders from the same IP, or the use of multiple credit cards by a single account. The Fraud Risk team utilizes AI-driven tools to flag anomalies. Suspicious internal activity, such as kickbacks from vendors or phantom employees on payroll, is investigated by the Internal Audit team. Whistleblowers reporting financial misconduct are protected under the Whistleblower Policy.

7.6 Budgeting & Forecasting

Department heads are responsible for creating annual budgets in Q4 of the preceding year. Budget variance reports are reviewed monthly. Variances exceeding 10% require a written explanation to the Finance Committee. Unused budget does not roll over to the next fiscal year unless specifically approved for capital expenditure projects.

Page 8: Health, Safety & Emergency Procedures

8.1 Workplace Safety (OSHA Compliance)
SwiftBite is committed to maintaining a hazard-free workplace. Walkways must remain clear of obstructions. Electrical equipment must be inspected annually. Ergonomic assessments are available for all employees; requests for standing desks or specialized chairs require a doctor's note or approval from the Safety Officer. Fire drills are conducted semi-annually. All employees must know the location of the nearest emergency exit and fire extinguisher.

8.2 Emergency Evacuation Plan
In the event of a fire, earthquake, or other emergency, the alarm will sound. Employees must evacuate via the stairwells immediately-elevators are not to be used. Designated "Fire Wardens" in orange vests will guide the evacuation. The assembly point is the parking lot across the main street. Employees must not re-enter the building until the "All Clear" is given by the Fire Department. Roll call will be taken at the assembly point to ensure everyone is accounted for.

8.3 Health Benefits & Wellness
SwiftBite provides comprehensive health insurance covering medical, dental, and vision for full-time employees. Coverage begins on the first day of the month following the start date. We also offer a Mental Health Assistance Program (MHAP) which provides 5 free counseling sessions per year. A dedicated "Wellness Room" is available in the office for rest, prayer, or lactation needs. Smoking and vaping are prohibited inside the building and within 25 feet of entrances.

8.4 Substance-Free Workplace
The possession, use, sale, or being under the influence of illegal drugs or alcohol during working hours is strictly prohibited. Exceptions for alcohol consumption exist only for company-sanctioned events. Prescription medication that impairs the ability to operate machinery or vehicles must be reported to the manager if the employee's role involves such tasks. Random drug testing may be conducted for safety-sensitive roles (e.g., fleet managers, warehouse operators).

8.5 Communicable Disease Protocol
Employees exhibiting symptoms of contagious illnesses (flu, COVID-19, etc.) must not come to the office. They should work remotely or take sick leave. In the event of a pandemic, the Crisis Management Team will enforce specific protocols, such as mandatory masking, social distancing, or full remote work. Vaccination drives may be organized on-site, and time off is granted for vaccination appointments and recovery from side effects.

8.6 Security & Access Control
Access to the office is controlled via ID badges. Tailgating (allowing someone to follow you through a secure door) is prohibited. Visitors must sign in at the reception, sign a Non-Disclosure Agreement (NDA), and be escorted by an employee at all times. The last person leaving the office must ensure all windows are closed and the alarm system is armed. Security cameras operate 24/7 in common areas; footage is retained for 30

days and accessed only for security investigations.