Security & Acceptable Use Policy

Applies to: all employees, contractors, interns, and third-party personnel with logical or physical access to company systems or data.
Scope: laptops/workstations; source code; CI/CD; cloud infra; analytics; back-office tools; payment rails; customer data; merchant data; rewards logic and transaction data.

Core Principles

1. **Least privilege** — access only what you need to perform your job.
2. **Default-deny** — new services and identities start with no access until explicitly approved.
3. **Data minimization** — collect, retain, and replicate the minimum data necessary to deliver the product.
4. **Defense in depth** — no single control is relied on exclusively.
5. **Regulated data first** — when decisions conflict, choices that reduce risk to cardholder/financial/PII data win.

Identity & Access Controls

- All user access is **individual, traceable, and revocable** — no shared credentials.
- **MFA** is mandatory for: SSO, production systems, code repositories, admin consoles, and financial systems.
- **Password rules:** min length 14 or passphrase; no reuse with any external account.
- **Off-boarding**: revoke access within 4 hours of notice; disable long-lived API tokens immediately.

Endpoint & Workstation Requirements

- Company endpoints must run managed EDR/AV, host firewall, disk encryption, and auto patching.

- Only company-approved devices may access source code or production environments.
- Personal USB storage, portable media, and jailbroken/rooted devices are prohibited for company data.
- Screens must auto-lock after ≤5 minutes idle.

Network & Cloud Security

- Prod and non-prod must be **logically separated**; cross-environment access is restricted and logged.
- All ingress must terminate on managed, patched, TLS-enforcing front doors (WAF/API gateway).
- Secrets live only in **approved secrets managers** — not in code, configs, Slack, or tickets.
- Public URLs must expose only intended surfaces; everything else is private by design.

Data Handling (PII / Rewards / Transaction Data)

- PII, payment, and rewards transaction data must be **encrypted in transit (TLS1.2+)** and **at rest**.
- Exporting raw PII or transaction datasets to email, Slack, Notion, or personal storage is prohibited.
- Use **tokenization/pseudonymization** when feasible in analytics/testing.
- Data retention & deletion follow the data retention standard; no “keep just in case.”

Software Development & Change Control

- All code changes require **peer review**, automated scans, and CI checks passing before merge.
- No direct commits to protected branches; prod deploys are traceable, authorized, and audit-logged.
- Secrets, keys, and credentials must never be committed into repos.

- Third-party SDKs/libraries must be reviewed for security and license before adoption.

Acceptable Use Rules

You **MAY NOT** do the following with company systems or data:

- Bypass or disable security controls, EDR, MFA, or monitoring.
- Scrape, re-identify, or abuse consumer or merchant data for non-business purposes.
- Use company assets for illegal, harassing, abusive, extremist, infringing, or competitive work.
- Store or process company data on unapproved SaaS or personal accounts.
- Pen test / fuzz / scan without explicit written authorization.

You **MUST** promptly report suspected incidents, data mishandling, credential exposure, or lost/stolen devices.

Incident Reporting & Response

- Suspected incidents must be reported **immediately** via the defined IR channel (security@… and Pager).
- Do not attempt to “clean up” incidents yourself. Preserve evidence; stop doing harm; escalate.

Third Parties & Vendors

- Vendors handling PII/financial/production data require prior security review and contractual controls.
- Vendor access must be **least-privilege** and time-bounded; remove access when no longer needed.

Monitoring & Enforcement

- Use of company systems may be **monitored and logged** for security and compliance.
- Violations may result in access revocation, disciplinary action, or legal escalation.

Acknowledgement

All covered persons must read, understand, and attest to this policy and all referenced standards.