

Security Standards and Procedures

Card Prices LLC, a Missouri limited liability company

Version 1.0 · Effective Date: October 13, 2026 · Supplements the Information Security Policy published at

<https://card-prices.com/security>

1. Purpose, Scope and Roles

The Company's Information Security Policy (Article 8 of its Governance Policies) states what the Company commits to: how data is classified, handled, retained and deleted, and how an incident is answered. This document states *how* those commitments are carried out day to day. Where the two differ, the Policy governs.

Scope. card-prices.com, the Card Prices apps and API, the systems that run them, the accounts that administer them, and every device used to do so. It applies to the Member and to any employee, contractor or other person given access ("personnel").

Roles. The Company is operated by its sole Member, who holds each role below. If personnel are added, the Member may delegate a role in writing.

Role	Responsibility
Security Lead	Owns this document; approves access; reviews alerts, vulnerabilities and exceptions.
Incident Lead	Declares and directs the response to a security incident; makes or approves every notification.
Privacy Contact	Receives and answers requests from individuals, partners and regulators about personal data.

Contacts. Security: security@card-prices.com (also published at <https://card-prices.com/.well-known/security.txt>). General and privacy requests: support@card-prices.com.

2. Access Control

- Least privilege.** Access to Confidential and Restricted data, and to the systems that hold it, is limited to the Member and to persons the Member has authorized in writing for a stated purpose. Access is granted at the lowest level that allows the work, and for no longer than it is needed.
- Individual accounts.** Each person uses their own account on every service that supports it. Shared logins are not used for administration.
- Multi-factor authentication** is required on every account that can administer production systems, source code, DNS, cloud infrastructure, payments or company email (Section 3.3).
- Service identities.** Each service and server runs under its own identity and can read only the secrets it needs. Secrets are held in a managed secret store, not in source code, chat, email or tickets.
- Personal data.** Access to user personal data is limited to what is necessary to operate the service, answer a support request, or investigate an incident.

6. **Review and removal.** The Security Lead reviews who and what holds access at least every six months and when a role changes. Access is removed within one business day of a person's engagement ending, and credentials they could have known are rotated.
7. **Partner credentials.** Tokens that let the Company act on a partner platform for a customer (for example a seller's marketplace authorization) are stored encrypted, are used only for the purpose the customer approved, and are deleted when the customer disconnects or the partnership ends.

3. Security Baseline for Daily Operations

3.1 Devices

- Every workstation and laptop locks its screen automatically after no more than 10 minutes idle and requires a password, PIN or biometric to unlock. Screens are locked whenever a device is left unattended.
- Laptops and any other portable device that holds Confidential or Restricted data use full-disk encryption.
- Operating systems and browsers install security updates automatically.
- A lost or stolen device is reported to the Security Lead the same day; its sessions are revoked and the credentials it held are rotated.

3.2 Passwords

- Passwords are at least 14 characters, unique to each service, and generated and stored in a password manager. Default passwords are changed before a system is put to use.
- Passwords and other credentials are never sent by email or chat or written into tickets or documents.
- Servers accept administrative logins by key or managed identity only; password logins over SSH are disabled.

3.3 Multi-factor authentication

Multi-factor authentication is enabled on, at minimum: company email and identity provider; source-code hosting; DNS and content delivery; each cloud infrastructure provider; payment processing; the domain registrar; and each partner developer portal. An authenticator app or hardware key is preferred over SMS.

3.4 Clear desk and clear screen

Confidential and Restricted information is not left on paper, whiteboards or unattended screens. Printed material containing it is shredded when no longer needed. Work on such information in public places is avoided where a screen can be overlooked.

4. Endpoint Protection

1. Anti-malware software is installed on every company workstation, laptop and server, with automatic definition updates.
2. On workstations and laptops, real-time protection is enabled and may not be switched off.

3. On servers, real-time protection is enabled unless the Security Lead records an exception for a host where it materially degrades the service. A host under an exception runs endpoint detection in monitoring mode and a scheduled scan at least weekly.
4. Detections are reviewed by the Security Lead and handled as an incident (Section 7) when they indicate compromise.

5. Network Security

1. **No direct exposure.** Production services are reached through the Company's content-delivery and edge provider, which terminates TLS and filters traffic. Origin servers do not accept application traffic directly from the internet.
2. **Segregation.** Production serving, data storage, data collection and development are run as separate environments with separate credentials. Databases and internal services listen only on private or loopback interfaces and are not reachable from the internet.
3. **Default deny.** Each host, or the network in front of it, allows inbound connections from the internet only on the ports its role requires; everything else is refused.
4. **Administrative access** is by key-authenticated SSH or through an identity-aware access proxy. Administrative web interfaces are not published without authentication.
5. **Encryption in transit.** All external traffic uses TLS 1.2 or later. HTTP is redirected to HTTPS and HSTS is set on the Company's sites.
6. **Monitoring.** Cloud security monitoring is enabled on the Company's cloud subscription and servers; edge security events and service health are monitored; alerts are reviewed by the Security Lead.

6. Data Classification and Encryption

Data is classified as Public, Internal, Confidential or Restricted as defined in Section 1 of the Information Security Policy. In addition to that Policy's handling rules:

- Confidential and Restricted data is stored only on services that encrypt at rest, or is encrypted by the application before it is stored.
- Credentials and partner tokens are held in a managed secret store or encrypted at the application level with a key kept separately from the data.
- Backups that contain Confidential or Restricted data are encrypted; the ability to restore them is tested.
- Restricted data is not copied to personal devices, removable media or development environments.

7. Incident Response Plan

7.1 Reporting channels

Anyone — personnel, a customer, a partner or a researcher — reports a suspected incident to security@card-prices.com. Reports are acknowledged within two business days.

7.2 Roles

The Incident Lead directs the response, decides severity, and makes or approves all external communication. The Incident Lead may engage outside counsel, the affected service providers' support, and technical help as needed.

7.3 Severity

Level	Meaning	Response begins
High	Confirmed or likely unauthorized access to Restricted or Confidential data, or compromise of a production system or credential.	Immediately on discovery
Medium	A vulnerability or event that could lead to the above but shows no evidence that it has.	Within one business day
Low	A policy deviation or blocked attempt with no exposure.	Within five business days

7.4 Procedure

1. **Contain** — revoke or rotate affected credentials, isolate affected systems, stop the exposure.
2. **Assess** — establish what happened, which data and whose, and for how long; preserve logs and evidence.
3. **Notify** — affected API partners and customers without undue delay and no later than 72 hours after a breach of their data is confirmed, or sooner where a contract or law requires; regulators and individuals as the law requires. A notice says what happened, what data was involved, what has been done, and whom to contact.
4. **Remediate** — fix the root cause and verify the fix.
5. **Document** — a written incident report (timeline, scope, impact, actions, prevention) within 14 days of closure.
6. **Review** — update these standards and the Policy where the incident showed a gap.

8. Vulnerability and Threat Management

1. **Sources.** The Company identifies vulnerabilities through cloud security monitoring and vulnerability assessment on its servers; security advisories for the software and dependencies it uses; security review and secret scanning of code changes; and reports received at security@card-prices.com.
2. **Patching.** Operating-system security updates are installed automatically. Other fixes are applied within the following times from when the Company learns of the issue:

Severity	Target
Critical (actively exploited, or remote compromise without authentication)	7 days
High	30 days

Medium and low	90 days, or the next scheduled maintenance
----------------	--

Where a fix cannot be applied in time, the Security Lead records the reason and a compensating control.

3. **Tracking.** Each finding is recorded in the Company's issue tracker and followed to closure.
4. **Review.** Open findings and security alerts are reviewed at least monthly.
5. **Disclosure.** The Company welcomes good-faith reports and will not pursue action against a researcher who reports a vulnerability privately, avoids accessing others' data, and gives reasonable time to fix it.

9. Personal Data Protection

This section is the Company's internal procedure for personal data. What the Company tells individuals is in its Privacy Policy (<https://card-prices.com/privacy>).

1. **Minimization.** The Company collects the personal data it needs to provide an account and the features a user chooses, and no more. From partner platforms it requests only the permissions a feature needs.
2. **Partner platform data.** Data obtained through a partner's API on behalf of a seller (for example, the seller's authorization and their own product listings) is used only to provide the feature that seller enabled, is not sold or shared, and is not combined with other data to profile individuals. The Company does not collect buyers' personal data from partner platforms unless a feature requires it and the partner's terms allow it.
3. **Requests.** Requests to access, correct, delete or export personal data are received at support@card-prices.com, verified, and answered within 30 days. The Company assists partners and their sellers in answering such requests where the Company holds the data.
4. **Retention and deletion.** Personal data is kept for the periods in Section 4 of the Policy. When a customer disconnects a partner account, or a partnership ends, the tokens and partner data held for it are deleted within 30 days unless the law requires them to be kept.
5. **Processors.** Personal data is stored and processed only with service providers that are bound by data-protection terms. Data is stored and processed in the United States.
6. **Breaches** of personal data are handled under Section 7.
7. **Data Protection Officer.** The Company has not appointed a statutory Data Protection Officer. The Privacy Contact (Section 1) performs that function.

10. Exceptions and Review

An exception to any requirement here is approved by the Security Lead in writing, with its reason, its compensating control and a date on which it is revisited. This document is reviewed at least once a year, and after any High-severity incident or material change to the Company's systems.

Adoption

Adopted by the sole Member of Card Prices LLC on October 13, 2026 as a standard under Article 8 of the Company's Governance Policies.

Name	Signature	Date
Eric Schnelker, Member		October 13, 2026

Version	Date	Change
1.0	October 13, 2026	First adoption.