

Information Security Policy

Creator's Deck, LLC | Version 1.0 | Effective October 17, 2026

Policy owner: Company owner. Adopted at the owner's direction. This document defines mandatory requirements; implementation status is tracked separately.

1. Purpose and scope

Creator's Deck, LLC adopts this policy to protect the confidentiality, integrity, and availability of information used by Creator's Deck. It applies to the owner, staff, contractors, application, databases, source code, administrator accounts and devices, backups, support operations, and service providers with access to company information.

This policy takes effect October 17, 2026, version 1.0, at the company owner's direction. It establishes mandatory operating requirements. Implementation evidence and outstanding actions are maintained separately; publication is not a claim that every control has already been verified or that a platform has approved the service.

2. Responsibility and review

The company owner is the accountable security owner until a replacement is formally designated. The security owner maintains the asset and data inventory, approves access and exceptions, reviews suppliers, coordinates incidents and recovery, and ensures this policy is available to everyone with system access. Personnel must acknowledge the policy before receiving administrative access.

Review the policy at least annually and after material changes or incidents. Maintain dated versions, access reviews, implementation evidence, exceptions, and review decisions. The next scheduled policy review is no later than October 17, 2027.

3. Access management and administrator devices

Use individual accounts and least privilege. Administrative access to hosting, source control, identity administration, and partner platforms must use MFA wherever supported; verify and record its configuration. Do not share passwords or recovery codes. Review access quarterly and promptly remove access when a person's role or engagement ends.

Administrative devices must use supported software, current security updates, disk encryption, screen locking, and appropriate malware protection. Keep recovery material in an access-controlled credential manager. Download confidential data only for a documented purpose, restrict recipients, and remove local copies when that purpose ends.

Access and data protection

Creator's Deck, LLC | Version 1.0 | Effective October 17, 2026

4. Information classification and permitted use

Classify passwords, API credentials, tokens, database credentials, and recovery codes as restricted. Classify private planner information, earnings, private messages, and profile photos as confidential. Community information is shareable only with the audience selected by the user; shared profile information never authorizes disclosure of private planner or earnings data.

Maintain an inventory of data sources, fields, purposes, locations, access, recipients, and retention. Collect only what is necessary for the authorized service. Do not sell personal or platform data, use it for unrelated advertising, or access data beyond user consent and approved platform permissions. Use synthetic data for development and testing wherever possible.

5. Authentication and application authorization

Derive identity from validated server-side authentication. Enforce account ownership, sharing visibility, and conversation membership on the server. Validate input, limit request sizes, bind database parameters, and protect state-changing requests against cross-site misuse. Test anonymous and cross-account access before releases affecting data access.

Account deletion must invalidate the retired account identity and prevent old sessions or delayed writes from restoring deleted information. New sign-in after deletion must create a separate empty account. Do not include confidential data or credentials in shared URLs, client bundles, error messages, or browser caches.

6. API authorization and secrets

Use approved platform authorization flows; never collect a creator's or seller's TikTok password. Before activating a TikTok connection, implement an expiring, single-use authorization state bound to the initiating account, server-side code exchange, validated account binding, and safe denial, expiration, refresh, disconnect, and revocation handling.

Restrict secrets to server-side configuration. Before storing platform tokens, encrypt them using a server-controlled key managed separately from the stored token data. Limit decryption access. Keep tokens, passwords, authorization codes, and secret URLs out of source control, logs, analytics, support screenshots, and downloadable user backups. Rotate exposed credentials promptly and after relevant access changes.

Data and infrastructure

Creator's Deck, LLC | Version 1.0 | Effective October 17, 2026

7. Infrastructure, encryption, and environments

Require HTTPS for browser and external API traffic. Keep the database closed to public internet connections by default. Any temporary external access requires documented necessity, narrow source restrictions, an expiry, and owner approval. Use authenticated internal service connections and provider-managed encrypted storage. Verify database transport protection before asserting end-to-end encryption in transit; private networking alone is not evidence of transport encryption.

Separate development, staging, and production credentials and data. Maintain an inventory of exposed services and provider protections. Do not represent provider certifications as company certifications. Assess network isolation, access controls, and alerting for the actual hosting plan before connecting production platform data.

8. Changes and vulnerability management

Review release changes and run relevant build, input-validation, authentication, and authorization checks. Keep rollback instructions and dated validation results. Review dependency and secret-scanning findings before production releases and at least monthly. Evaluate critical security notices promptly.

Triage a suspected critical exposure within one business day. Mitigate promptly, including disabling affected functionality or access when necessary. Record severity, owner, action, and verification. Unresolved high-risk exceptions must be reviewed at least weekly and must not override a platform restriction. These are operating requirements, not a claim of completed scanning or penetration testing.

9. Logging and security monitoring

Record security-relevant operational events without passwords, tokens, authorization codes, private message bodies, or unnecessary personal information. Restrict log access. Review log content and approve documented retention limits for each log source before production platform access.

Configure monitoring and alert ownership for sustained service failures, suspicious authentication or authorization activity, unexpected access, and backup failures. Test alert delivery and escalation before production launch and after changes. Track provider-managed safeguards separately from monitoring configured by the company.

10. Incident response

Anyone with system access must promptly report suspected compromise, unintended disclosure, lost administrator devices, or credential exposure to the security owner through the security contact. The owner must record discovery time, scope, affected systems and data, containment decisions, and evidence handling.

Contain the incident, restrict affected access, revoke or rotate exposed credentials, investigate impact, and verify remediation and recovery. Preserve necessary evidence with restricted access and avoid unnecessary copies of personal data. Notify TikTok, affected people, and authorities when required by applicable agreements and law; record the applicable deadlines and decisions. Complete a post-incident review and track corrective actions.

Privacy and recovery

Creator's Deck, LLC | Version 1.0 | Effective October 17, 2026

11. Privacy, retention, and deletion

Publish an accurate privacy notice explaining collection, purpose, sharing, retention, and privacy contact options. Verify identity before acting on access, correction, export, or deletion requests. Keep active account information only for its documented purpose and remove eligible data through the account-deletion workflow or a verified support request. Do not invent a universal TikTok retention deadline; document and enforce any data-specific platform obligation that applies.

Deletion must cover saved workspaces, profiles, photos, notification subscriptions, community associations, messages, connected platform data, and relevant report snapshots. Describe shared-content effects to users. Retain only minimal pseudonymous security records needed to block retired sessions and route a future sign-in; review their necessity at least annually. Record completion without retaining deleted content or unnecessary identifiers.

Disconnecting a platform must stop future access and remove or revoke stored credentials as supported. Before TikTok integration is activated, implement and test platform revocation and authorization-end deletion separately from full Creator's Deck account deletion, and update the privacy notice to describe actual fields and retention.

12. Backups and recovery

Maintain access-controlled backups appropriate to the service. Confirm the provider recovery window and backup completion; a paid plan or an export request alone is not evidence of a usable backup. A user-downloaded planner JSON file is not a full service backup. Keep exports encrypted and restricted; never commit database exports or credentials to source control.

Document retention for each backup location and delete separately managed exports when no longer needed. Provider recovery copies may retain deleted data until their retention period expires; isolate them from routine use. Keep a separately protected deletion record sufficient to reapply deletions after recovery without retaining deleted content. Test recovery in an isolated environment and reapply deletions before reopening restored data to users.

Record the initial restore test and subsequent tests at least quarterly and after material backup changes. Measure recovery performance before setting recovery time and recovery point objectives. Production platform data must not be enabled until backup recovery and deletion reapplication are verified.

Governance and publication

Creator's Deck, LLC | Version 1.0 | Effective October 17, 2026

13. Suppliers and production readiness

Review suppliers before granting data access and at least annually for purpose, necessary permissions, processing location, security information, contractual terms, and retention. Current service roles include Render for hosting and database operations, Google for sign-in, and browser push providers for enabled notifications. Update the inventory and notice before adding a new integration.

Before production platform access, verify required platform/category/scope approvals, administrative MFA, data inventory and retention, token protections, environment and transport safeguards, monitoring, incident handling, backup restoration, deletion, and policy acknowledgments. Record any outstanding work and do not describe an unverified control as implemented.

14. Exceptions, publication, and contact

Every exception requires a documented reason, affected information, risk, compensating controls, accountable owner, expiry, and review date. Exceptions cannot authorize access prohibited by a platform or applicable obligation. Maintain implementation records privately and disclose appropriate evidence to authorized reviewers through approved channels.

Public policy: <https://creators-deck-google-staging.onrender.com/security>. Privacy notice: <https://creators-deck-google-staging.onrender.com/privacy>. Security and privacy contact: mjpeyton25@gmail.com. This policy does not claim SOC 2, ISO 27001, a completed independent security audit, legal certification, or TikTok approval.