Information Security Policy

Purpose, authority and organizational responsibilities

Approved and effective: 28 October 2026 | Public controlled policy

1. Document control and authority

Organization: CC Connect Agency. Document ID: CC-SEC-001. Version: 2.0. Approved and effective: 28 October 2026. Policy owner: Camilla Kezia da Silva Almeida, Partner. Review: at least annually and after material changes or significant incidents.

This version was adopted by management through written electronic approval on 28 October 2026. It is the governing information security policy of CC Connect Agency from that date. The approval, ownership and public publication record appears on page 5.

This policy specifies mandatory organizational rules. Statements of policy do not certify that a technical control is deployed, audited or independently certified. Technical review answers must be supported by current implementation evidence.

2. Purpose and scope

Protect the confidentiality, integrity and availability of information used to deliver marketplace management services and operate the CC Connect application, including authorized TikTok Shop integrations.

The policy applies to management, employees, contractors and other authorized personnel; applications, endpoints, repositories, cloud services and integrations; and merchant, customer, order, support, credential and operational data handled for authorized services. Merchant users must access only stores and records they are authorized to use.

3. Accountability and responsibilities

Agency Management is accountable for approval, resources, risk decisions, access authorization, supplier oversight, incident coordination and review. A named operational security owner and a monitored reporting channel must be recorded on page 5.

Personnel must follow this policy, protect credentials and confidential data, use approved systems, report suspected incidents immediately and cooperate with corrective actions. Contractors must accept equivalent confidentiality and security obligations before access.

In a small or single-operator organization, one individual may perform multiple roles. Management must document those assignments and use traceable approvals, activity records and independent specialist review where warranted by risk. A separate security department or independent reviewer must not be claimed unless it exists.

Access and secure operations

Identity, infrastructure, endpoints and application changes

4. Identity and access management

Grant access only for an approved business need, using individual identities, minimum required privileges and explicit store or tenant authorization. Approvals must record the user, role, scope, approver and date. Sharing accounts, passwords, API tokens or recovery codes is prohibited.

Use unique passwords and an approved password manager. Require multi-factor authentication for privileged, marketplace, email, repository and other sensitive accounts wherever supported. A capability that is not yet enabled must be recorded as a gap, assigned an owner and remediated; it must not be reported as implemented.

Review access at least quarterly and after role changes, suspicious activity or contract termination. Revoke access promptly when no longer authorized. Protect recovery methods and terminate compromised sessions and credentials.

5. Secrets and integration permissions

Request only API permissions required for the authorized service. Obtain and retain merchant authorization before processing their data. Keep secrets server-side in approved restricted secret storage; never include live secrets in browser code, public repositories, screenshots, exported reports or ordinary logs.

Restrict secret access to approved roles. Rotate or revoke exposed secrets promptly and review dependent integrations. Store refresh tokens and recovery material with equivalent protection. Remove obsolete authorizations and credentials when service access ends.

6. Infrastructure and endpoint security

Maintain an inventory of hosting services, systems, devices and responsible parties. Document network boundaries, administrative access paths and the division of responsibility between the agency and its service providers.

Require appropriate filtering, secure administrative access and monitoring for the deployment model. Provider-managed controls must be verified with current evidence before being described as implemented. Do not claim a dedicated firewall, IDS/IPS or other technology solely because a cloud provider is used.

Use maintained operating systems and browsers, screen locks, device encryption where supported, security updates and approved storage. Restrict installation of software and use of personal or removable storage according to risk. Lost or compromised devices must be reported immediately.

7. Secure application development and changes

Validate inputs and enforce authorization on the server, including separation of each merchant and tenant. Review changes before release, test critical permissions and workflows, restrict deployment access and retain a record of the change, reviewer or responsible operator, validation and rollback approach.

Separate production from testing where supported. Use synthetic or minimized test data. Assess and remediate vulnerabilities according to severity; urgent exposure requires prompt containment. Keep dependencies updated and do not expose secrets or confidential customer data in debugging output.

Data protection and suppliers

Information classification, lifecycle and authorized processing

8. Classification and authorized use

Classify passwords, API keys, tokens and recovery codes as restricted. Classify identifiable merchant, customer, order and support data as confidential. Treat internal operating records as internal unless approved for public release.

Collect, access and disclose only the minimum information needed for the authorized service. Document the processing purpose, data categories, systems, recipients and applicable retention rule. Do not sell data or use marketplace data for unrelated purposes.

9. Storage, transmission and handling

Use approved systems with access restrictions and encrypted transmission. Verify storage encryption, access protection and relevant provider responsibilities before storing confidential production data. Restrict exports and sharing; protect downloaded files and remove temporary copies when no longer required.

Keep merchant data logically segregated and enforce per-store permissions. Do not put customer information or credentials in public documents, public links or code repositories. Share confidential information only through approved channels with authorized recipients.

10. Retention, deletion and end of service

Maintain a retention schedule identifying each data category, business purpose, applicable legal or contractual obligations, retention trigger, deletion method and owner. Do not retain information indefinitely or assign a retention period without a documented basis.

When authorization or the service relationship ends, stop unauthorized processing, revoke access and credentials, and return or securely delete data no longer required. Document completion and any justified legal retention. Restricted retention must limit access and use to the documented obligation.

Include exports, local files, logs, temporary data and supplier-held copies in the deletion assessment. Backups must follow the documented expiry and restoration procedure; deleted data must not be reintroduced into active processing. Handle personal-data requests through the designated privacy contact and record the outcome.

11. Supplier and third-party oversight

Assess suppliers before allowing access to confidential information. Review the service purpose, data location, access, encryption, incident cooperation, deletion capabilities and continuity responsibilities. Retain relevant contracts or terms and evidence supporting the selected controls.

Limit third-party access, review material supplier changes and remove obsolete access. Management must assess risk before approving a new processor or changing where personal data is stored or processed. Location and subprocessors must be described accurately in the review.

12. Records and auditability

Keep records sufficient to demonstrate authorization, significant administrative actions, security review, incident handling and data deletion. Protect records against unauthorized access and modification. Restrict log contents to the necessary information and exclude passwords, tokens and unnecessary personal data.

Incidents, continuity and review

Operational response, awareness and maintenance

13. Security incident response

Any suspected unauthorized access, data exposure, account compromise, malware, lost device or material service disruption must be reported immediately to the named security owner through the reporting channel on page 5.

The security owner must open an incident record, assess affected systems and data, preserve relevant evidence and coordinate containment. Actions may include revoking credentials, isolating affected access, disabling unsafe processing and involving the relevant provider.

Management must assess the impact on merchants and individuals, coordinate required notifications to platforms, affected parties and authorities under applicable contractual and legal obligations, and document the facts, decisions, responsible persons and timestamps. No notification is to be represented as sent unless it was actually delivered.

Restore service only after validating containment and corrective action. Record the root cause where established, recovery validation, lessons learned and assigned remediation tasks.

14. Continuity and recovery

Identify critical services and dependencies. Document which data requires backup, the approved backup location, access protection, recovery objectives and responsibility for restoration. Verify provider capabilities instead of assuming backups or recovery guarantees exist.

Test recovery at least annually and after significant changes where the agency controls restoration. Record the test scope, outcome, gaps and follow-up actions. If a provider controls restoration, retain the applicable service commitments and the agency escalation procedure.

15. Awareness and confidentiality

Provide security guidance before granting access and refresh it at least annually. Cover phishing, confidential information, individual accounts, MFA, safe exports, incident reporting and marketplace data restrictions. Retain acknowledgment or training records, including management when the organization has only one operator.

Non-compliance must be reviewed by management and addressed through access restriction, corrective guidance, contractual action or other appropriate measures.

16. Risk management, exceptions and review

Maintain a risk and implementation register. Each unresolved control must have a description, risk, owner, required action and target date. Exceptions require written management approval, justification, compensating safeguards, review date and expiry. An exception does not make an unimplemented control compliant.

Review this policy at least annually and after significant incidents, architecture changes, new data use, material provider changes or relevant marketplace requirement changes. Record the review date, reviewer, decision and next review due date. Retain superseded versions and approval history.

17. Publication and external representations

Publish the approved version in the repository recorded on page 5 and make it accessible to all in-scope personnel. Retain evidence of the publication date, distribution and acknowledgments. A public publication is permissible only for a copy without secrets, customer data or restricted security detail.

External questionnaires must match the approved policy and actual operational evidence. This policy does not assert ISO 27001, ISO 27701, SOC 2 or another independent certification.

Approval and publication record

Adopted policy - completed management and publication record

Organization and business identification

CC Connect Agency. Business identification supplied: 62.992.686 CAMILLA KEZIA DA SILVA ALMEIDA. CNPJ: 62.992.686/0001-00.

Policy and status

CC-SEC-001, version 2.0. Approved, adopted and in force. This is the public controlled policy, not an approval template.

Approving management representative

Camilla Kezia da Silva Almeida. Management role: Partner (Socia), as declared by the approving representative.

Approval and effective date

28 October 2026. Management expressly approved adoption of version 2.0 and authorized its publication in a written electronic instruction.

Operational security owner and contact

Camilla Kezia da Silva Almeida, acting for Agency Management. Security reports: ccconnectagency@gmail.com. Management is responsible for monitoring this channel and coordinating the policy requirements.

Publication record

Public policy page: https://cc-connect-erp.ccconnectagency.chatgpt.site/seguranca-da-informacao . Publication date: 28 October 2026.

Controlled PDF location

https://cc-connect-erp.ccconnectagency.chatgpt.site/documents/CC_Connect_Information_Security_Policy_v2_EN.pdf

Management acknowledgment and distribution

Management receipt, adoption and acknowledgment are recorded by the written approval instruction. This public controlled copy is accessible to relevant personnel. Additional personnel must acknowledge the policy before receiving access; acknowledgment records must be retained by management.

Next scheduled review

No later than 28 October 2027, or earlier after a material change or significant security incident.

Approval record and signature method

Approval source: written electronic management instruction on 28 October 2026 expressly approving the policy and authorizing publication. This document records that approval; it does not represent a handwritten signature or a certificate-based digital signature.

The technical controls specified by this policy remain subject to implementation and verification records. Adoption and publication do not constitute an independent security certification.