BIGVIRALS

INFORMATION SECURITY POLICY

A written security framework for daily operations, TikTok Shop API data protection, and organizational governance

Legal Entity / TikTok Shop Developer	江西省深蓝智科文化有限公司
Service Brand	BIGVIRALS
Application	bigvirals-Creator Outreach
Official Website	https://www.bigvirals.com/
Privacy Policy	https://www.bigvirals.com/privacy.html
Contact	support@bigvirals.com
Version	1.0
Effective Date	July 12, 2026
Review Cycle	At least annually and after material business, system, legal, platform, or security changes
Document Status	Approved policy baseline

Entity and brand clarification

江西省深蓝智科文化有限公司 is the legal entity, TikTok Shop developer, and operator of the Services. BIGVIRALS is a product and service brand operated by the Company and is not a separate legal entity. bigvirals-Creator Outreach is the TikTok Shop application operated by the same Company.

Approved by: Management of 江西省深蓝智科文化有限公司

Approval Date: July 12, 2026

Document Control

Policy Owner	Information Security Owner designated by Company Management
Accountable Executive	Company Management
Applies To	Employees, contractors, temporary personnel, systems, applications, devices, cloud services, APIs, data stores, and service providers used for BIGVIRALS operations
Primary Data Domains	Merchant, seller, creator, campaign, customer, platform, authentication, technical, operational, and confidential business data
Review Frequency	At least once every 12 months and whenever a material change or significant security incident occurs
Exception Authority	Company Management or its formally delegated Information Security Owner
Public Availability	May be shared with TikTok Shop, merchants, partners, auditors, regulators, and other authorized reviewers

Revision History

Version	Date	Owner	Summary
1.0	July 12, 2026	Company Management	Initial comprehensive policy baseline; clarified legal entity, brand, application, data governance, access controls, security operations, incident response, and review requirements.

Policy Statement

江西省深蓝智科文化有限公司 (the "Company") is committed to protecting the confidentiality, integrity, and availability of information processed through the BIGVIRALS service and the bigvirals-Creator Outreach application. This policy establishes the minimum security baseline for daily operations and applies throughout the organization.

The Company will implement controls that are appropriate to its size, systems, data sensitivity, legal obligations, contractual commitments, and platform requirements. Security controls will be documented, reviewed, tested where practical, and improved when risks, technology, business operations, or regulatory expectations change.

Important implementation principle

This policy defines mandatory control objectives. Each control must be supported by operational evidence appropriate to the Company, such as access lists, configuration records, training records, risk reviews, incident logs, backup reports, vendor assessments, or change records. The policy does not claim any external certification.

Contents

1. Purpose and Objectives

This policy establishes an organization-wide information security framework that serves as the baseline for daily operations. Its objectives are to:

- Protect merchant, seller, creator, customer, platform, employee, and business information against unauthorized access, use, disclosure, alteration, loss, or destruction.
- Maintain the confidentiality, integrity, availability, authenticity, and lawful use of information and systems.
- Define clear security responsibilities for management, personnel, developers, administrators, contractors, and service providers.
- Support secure use of TikTok Shop APIs, OAuth authorizations, access tokens, application credentials, and related platform data.
- Provide a repeatable process for identifying, assessing, treating, monitoring, and accepting information security risks.
- Ensure policies and controls are reviewed regularly and updated after material changes, incidents, legal changes, or platform requirements.
- Enable timely prevention, detection, investigation, containment, remediation, recovery, and notification of security incidents.

2. Scope

This policy applies to all information and technology used to provide or support BIGVIRALS services, regardless of whether the information is stored, transmitted, displayed, processed, or accessed electronically, verbally, or in physical form.

The scope includes:

- All employees, directors, interns, contractors, consultants, temporary workers, and third parties who access Company systems or data.
- The BIGVIRALS website, the bigvirals-Creator Outreach application, APIs, databases, code repositories, cloud environments, development and production systems, communication tools, support tools, and administrative portals.
- Company-owned and authorized personal devices used for business purposes.
- TikTok Shop data and credentials received through approved APIs and user authorization flows.
- Merchant, seller, creator, campaign, customer, platform, account, authentication, security, billing, operational, and confidential business information.
- Third-party service providers that host, transmit, store, support, analyze, secure, or otherwise process Company information.

Where local law, a contract, or a platform requirement imposes a stricter obligation than this policy, the stricter obligation will apply.

3. Governance and Responsibilities

3.1 Company Management

- Approves this policy and provides appropriate authority and resources for information security.
- Designates an Information Security Owner and ensures material risks are reviewed and accepted by an accountable decision-maker.

- Ensures security is considered in business planning, product design, vendor selection, and operational changes.
- Reviews significant incidents, unresolved high risks, policy exceptions, and material audit findings.

3.2 Information Security Owner

- Maintains the information security framework, risk register, policies, standards, and evidence records.
- Coordinates access reviews, vulnerability management, incident response, training, supplier reviews, and periodic policy review.
- Escalates material risks and incidents to Company Management and coordinates communications with TikTok Shop or other authorized parties when required.
- Tracks corrective actions to closure and verifies that exceptions are approved, time-limited, and reviewed.

3.3 System and Data Owners

- Identify the sensitivity and business importance of systems and data under their responsibility.
- Approve access based on job need and ensure access is reviewed and removed when no longer necessary.
- Define retention, backup, recovery, and security requirements consistent with law, contracts, platform rules, and this policy.
- Participate in risk assessments, change reviews, incident investigations, and corrective actions.

3.4 All Personnel

- Use Company systems and information only for authorized business purposes.
- Protect credentials, devices, confidential information, and platform data.
- Follow approved security procedures and complete required training.
- Promptly report suspected phishing, credential exposure, malware, unauthorized access, data loss, policy violations, or other security concerns.
- Do not bypass security controls, install unauthorized software, share accounts, or disclose protected information through unapproved channels.

4. Information Security Risk Management

The Company will maintain a risk-based process to identify and manage threats to information, systems, and services.

- Risk assessments will be performed at least annually and before significant new systems, integrations, data uses, suppliers, or material architectural changes are introduced.
- Risks will be evaluated using likelihood and impact, considering data sensitivity, service availability, legal obligations, platform requirements, affected users, financial loss, and reputational harm.
- Risk treatment options include mitigation, avoidance, transfer, or documented acceptance by authorized management.
- High and critical risks will receive priority, assigned owners, target completion dates, and status tracking.
- Accepted risks and policy exceptions must include a rationale, compensating controls where possible, an approver, and an expiration or review date.
- Risk assessments will be updated after significant incidents, material control failures, or changes in the threat environment.

5. Asset Management

The Company will identify and manage information assets necessary to operate the Services.

- Maintain an inventory of material systems, cloud accounts, databases, applications, code repositories, domains, devices, integrations, secrets, and critical service providers.
- Assign an owner to each material information asset or system.
- Document the business purpose, data types, environment, criticality, and primary dependencies for material assets.
- Use approved software and services. Unauthorized tools must not be used to store or process protected data.
- Remove, sanitize, securely erase, or otherwise protect information before devices, storage media, accounts, or systems are reassigned, returned, decommissioned, or disposed of.
- Review the asset inventory periodically and after material technology changes.

6. Data Classification and Handling

Information will be classified according to sensitivity and business impact. The following baseline categories apply:

Class	Examples	Minimum Handling	Disclosure
Public	Published website content, approved marketing material, public policy pages	Integrity protection; authorized publication process	May be shared publicly after approval
Internal	Routine operational procedures, non-public business communications	Access limited to personnel with business need	No public disclosure without authorization
Confidential	Merchant, creator, campaign, customer, contract, financial, source-code, system, and non-public platform information	Least privilege; approved storage and transmission; logging where appropriate	Only authorized recipients with legitimate need
Restricted	Access tokens, refresh tokens, client secrets, passwords, security keys, sensitive personal data, incident evidence	Strongest access controls; encryption or equivalent protection; no unnecessary copying; prohibited from logs and unsecured communications	Only specifically authorized personnel and systems

- Data must be collected, accessed, copied, exported, transmitted, and retained only when necessary for an authorized purpose.
- Confidential and Restricted data must not be sent through personal email, public file-sharing links, unapproved messaging applications, or other unauthorized channels.
- Production data must not be used in development or testing unless necessary, approved, minimized, and protected. Synthetic or de-identified data is preferred.
- Screenshots, exports, logs, and support attachments containing protected data must be limited, secured, and deleted when no longer required.
- Data classification and handling requirements must be included in relevant training, supplier agreements, and operating procedures.

7. Identity and Access Management

Access to systems and data will follow the principles of least privilege, need-to-know, separation of duties where practical, and individual accountability.

- Each user must have a unique account. Shared accounts are prohibited unless technically unavoidable, formally approved, and protected by compensating controls and activity logging.
- Access requests must be approved by an appropriate system or data owner before access is granted.
- Role-based access controls will be used where supported. Privileged rights will be limited to personnel whose duties require them.
- Administrative and production access will be separated from ordinary user access where practical.
- Access rights will be reviewed at least quarterly for privileged and production access and at least annually for other material systems.
- Access will be removed promptly when employment or engagement ends, and adjusted promptly when responsibilities change. High-risk involuntary termination access will be disabled immediately where practical.
- Dormant, unnecessary, expired, or duplicate accounts will be disabled or removed.
- Remote administrative access must use approved secure methods and multi-factor authentication where supported.
- Service accounts must have a defined owner, documented purpose, minimum permissions, controlled credentials, and periodic review.

8. Authentication, Secrets, and API Credential Security

- Strong, unique passwords or passphrases must be used. Passwords must not be reused across unrelated services or shared through insecure channels.
- Multi-factor authentication is required for privileged accounts, production systems, cloud administration, source-code repositories, email, and other high-risk systems where available.
- Passwords, API keys, client secrets, access tokens, refresh tokens, encryption keys, and other secrets must not be hard-coded in source code or stored in public repositories.
- Secrets must be stored in an approved secrets-management mechanism or otherwise protected using strong access restrictions and encryption or equivalent safeguards.
- Sensitive credentials must not appear in application logs, analytics events, support tickets, screenshots, or error messages.
- Credentials must be rotated after suspected exposure, personnel changes affecting access, material security events, or according to system and provider requirements.
- OAuth tokens and TikTok Shop application credentials will be used only for authorized functions and only within approved scopes.
- Revoked, expired, disconnected, or no-longer-required tokens must be invalidated, deleted, or made inaccessible promptly.

9. Cryptography and Key Management

The Company will use industry-accepted cryptographic protections where appropriate to the data sensitivity, system capability, and applicable requirements.

- Protected data transmitted over public or untrusted networks must use secure encrypted protocols, such as current supported TLS configurations.

- Restricted data and sensitive credentials stored electronically must be encrypted or protected using an equivalent control where technically supported.
- Cryptographic keys and secrets must be separated from protected data where practical, limited to authorized systems and personnel, and rotated or replaced when compromised or required.
- Obsolete or insecure protocols and algorithms must not be used where a secure alternative is reasonably available.
- Certificates, domains, and encryption-related configurations must be monitored for expiration and renewed before service disruption.

10. Endpoint, Network, and Cloud Security

10.1 Endpoints

- Business devices must use supported operating systems, automatic screen locking, strong authentication, security updates, and endpoint protection appropriate to the platform.
- Full-disk encryption must be enabled on portable devices that store or access Confidential or Restricted data where supported.
- Devices must be protected from unauthorized physical access and must not be left unattended in insecure locations while unlocked.
- Lost, stolen, compromised, or suspicious devices must be reported immediately. Remote lock or wipe will be used where available and appropriate.
- Local storage of protected data must be minimized and removed when no longer required.

10.2 Network Security

- Internet-facing services must be protected by appropriate firewalls, access controls, secure configuration, and monitoring.
- Administrative interfaces must not be publicly exposed unless necessary and must use strong authentication, restricted access, and monitoring.
- Production environments should be logically separated from development and testing environments.
- Wireless and remote access used for business operations must use secure configurations. Untrusted public networks require an approved secure connection method.
- Network rules and exposed services will be reviewed periodically and after material changes.

10.3 Cloud and Infrastructure Security

- Cloud accounts must use least privilege, multi-factor authentication for privileged users, activity logging, secure baseline configurations, and controlled administrative access.
- Public storage, databases, and services are prohibited unless explicitly required, reviewed, and configured to expose only approved information.
- Security groups, identity policies, storage permissions, backups, and logging settings must be reviewed periodically.
- Production changes must follow the change-management requirements in this policy.
- Infrastructure configuration must be documented sufficiently to support secure operations, recovery, and review.

11. Secure Development and Change Management

Security and privacy requirements will be incorporated into the design, development, testing, deployment, and maintenance of BIGVIRALS systems.

- New features and integrations must be reviewed for data needs, authorization scopes, access controls, privacy impact, abuse risks, logging, retention, and deletion requirements.
- Code must be stored in access-controlled repositories. Changes must be attributable to an individual account.
- Material code changes should receive peer review or an equivalent independent review before production deployment where practical.
- Dependencies and third-party libraries must be obtained from trusted sources and maintained at supported versions.
- Application inputs must be validated and outputs appropriately encoded to reduce injection and related security risks.
- Secrets must not be committed to source code. Automated or manual secret checks should be used where practical.
- Development and testing environments must be separated from production. Production data use outside production must be minimized and approved.
- Changes must include testing, approval, rollback or recovery planning appropriate to risk, and records sufficient to identify what changed, who approved it, and when it was deployed.
- Emergency changes may use an accelerated process but must be documented and reviewed after implementation.

12. Vulnerability and Patch Management

- The Company will monitor relevant vulnerability advisories, provider notices, dependency alerts, and security findings for systems in scope.
- Operating systems, applications, libraries, devices, and infrastructure will be maintained at supported versions where reasonably possible.
- Vulnerabilities will be prioritized according to severity, exploitability, exposure, data sensitivity, and business impact.
- Target remediation timelines are: Critical - as soon as practicable and normally within 14 days; High - normally within 30 days; Medium - normally within 90 days; Low - according to risk and maintenance planning.
- Where a target cannot be met, the risk owner must document the reason, compensating controls, responsible owner, and revised target date.
- Internet-facing and production systems will receive priority. Confirmed active exploitation requires immediate escalation and containment action.
- Remediation will be verified through retesting, version confirmation, configuration review, or another appropriate method.
- Security testing may include dependency scanning, configuration review, code review, vulnerability scanning, or penetration testing according to system risk and business maturity.

13. Logging, Monitoring, and Security Testing

- Material systems must generate logs sufficient to support security monitoring, troubleshooting, incident investigation, access accountability, and compliance review.
- Logs should include, where appropriate, authentication events, privileged actions, access-control changes, API activity, system errors, security alerts, and material data-administration events.
- Logs must not intentionally record passwords, access tokens, refresh tokens, client secrets, complete payment credentials, or other unnecessary Restricted data.

- Access to security logs will be restricted and protected against unauthorized alteration or deletion.
- Critical security alerts will be reviewed promptly. Suspicious activity will be investigated and escalated according to the incident-response process.
- System clocks should be synchronized to a reliable time source to support accurate investigation.
- Security and audit logs will be retained for a risk-based period and, where practical, for at least 90 days, unless a longer period is required by law, contract, platform requirement, or an active investigation.
- Control effectiveness will be tested periodically through access reviews, restore tests, vulnerability checks, configuration review, incident exercises, or other appropriate methods.

14. TikTok Shop and Platform Data Protection

Platform data principle

TikTok Shop data belongs to the authorized user or relevant data subject and may be accessed only through approved APIs, approved scopes, and valid authorization. Platform data must be used only for the disclosed BIGVIRALS service purpose.

- The Company will request only API permissions reasonably necessary for the disclosed creator outreach, collaboration management, service operation, merchant support, security, and compliance functions.
- TikTok Shop data will be accessed only after the relevant seller, creator, partner, merchant, or authorized representative completes the applicable authorization process.
- The Company will not attempt to bypass platform access controls, exceed approved scopes, scrape protected data, or access data after authorization is revoked.
- TikTok Shop data will not be sold, rented, traded, or disclosed to unrelated parties.
- Platform data will not be used for unrelated advertising, unauthorized profiling, surveillance, harassment, spam, or deceptive activity.
- Access to platform data will be restricted to authorized personnel and systems with a legitimate operational need.
- Access tokens, refresh tokens, client credentials, and platform secrets will be protected as Restricted data.
- Data exports will be minimized, approved, protected, and deleted when no longer necessary.
- The Company will cooperate with TikTok Shop regarding security, privacy, compliance, audit, access, correction, deletion, authorization revocation, and incident-response requests as required.
- Material changes to the application, data use, permissions, ownership, service purpose, or security architecture will be reviewed and submitted for platform review when required.

15. Privacy, Data Minimization, Retention, and Deletion

- Personal data and platform data will be collected and processed only for specific, legitimate, disclosed, and authorized purposes.
- The Company will minimize the categories, volume, precision, and retention period of data collected or generated.
- Access, correction, deletion, and authorization-revocation requests will be handled according to applicable law, contracts, platform requirements, and the BIGVIRALS Privacy Policy.
- Retention periods will be based on business need, legal obligations, contract requirements, security needs, and platform instructions.

- When TikTok Shop authorization or the applicable service relationship ends, active use of affected platform data will stop. Unless continued retention is required by law, contract, security, dispute resolution, or platform instruction, affected data will be deleted or irreversibly de-identified within 30 days.
- Residual copies in protected backups may remain for up to 90 days before being overwritten or deleted through normal backup processes, unless longer retention is legally required or necessary for an active incident or dispute.
- Deletion must include relevant production stores, exports, local copies, and connected systems where reasonably possible. Backup data will not be restored for routine business use after a valid deletion request.
- Records required for tax, accounting, contract, fraud prevention, audit, or legal claims may be retained for the required period with restricted access.
- Data disposal must use secure deletion, cryptographic erasure, de-identification, physical destruction, or another method appropriate to the medium and sensitivity.

16. Third-Party and Supplier Security

The Company remains accountable for selecting and managing third parties that process, store, transmit, or access protected information on its behalf.

- Security and privacy risk will be considered before engaging material service providers.
- Due diligence will be proportionate to the service and may include review of security documentation, data locations, access controls, breach history, certifications or audit reports, subprocessors, deletion practices, and contractual protections.
- Contracts or equivalent terms should require confidentiality, authorized processing, appropriate security controls, incident notification, cooperation, deletion or return of data, and compliance with applicable law and platform requirements.
- Provider access will be limited to the minimum necessary and removed when the service or need ends.
- Material providers will be reviewed periodically and after significant incidents or changes.
- The Company will maintain a record of material service providers and the data or systems they support.
- A provider must not receive TikTok Shop data unless the disclosure is necessary, authorized, permitted by platform requirements, and protected by appropriate terms and controls.

17. Security Incident Response and Notification

All suspected or confirmed information security incidents must be reported promptly. The Company will maintain a practical incident-response process covering preparation, identification, containment, investigation, remediation, recovery, notification, and lessons learned.

- Personnel must immediately report suspected phishing, credential compromise, malware, unauthorized access, exposed storage, lost devices, accidental disclosure, system intrusion, data alteration, service disruption, or policy violations.
- The incident coordinator will record the event, assign severity, preserve relevant evidence, identify affected systems and data, and escalate according to impact.
- Containment may include disabling accounts, revoking tokens, rotating secrets, isolating systems, blocking malicious activity, suspending integrations, or temporarily restricting service functions.
- Investigation will identify the likely cause, scope, affected data, affected users, attacker actions, control failures, and required remediation.
- Recovery will include validation that affected systems are secure before normal operations resume and heightened monitoring where appropriate.

- The Company will notify TikTok Shop, affected merchants, creators, users, regulators, law enforcement, insurers, or other parties without undue delay and within any timeline required by law, contract, or platform policy.
- External communications must be accurate, coordinated, and approved by authorized management.
- A post-incident review will document root cause, impact, response effectiveness, corrective actions, owners, and target dates.
- Incident records will be retained according to legal, contractual, platform, audit, and security needs.

Security concerns may be reported to: support@bigvirals.com

18. Business Continuity, Backup, and Recovery

- The Company will identify systems and services whose loss would materially affect operations, security, merchant support, or platform obligations.
- Critical data and configurations will be backed up at a frequency appropriate to business impact and recovery needs.
- Backups must be access-controlled, protected from unauthorized alteration or deletion, and separated from production risk where practical.
- Recovery procedures and responsible contacts will be documented for material systems.
- Restore capability will be tested periodically and after significant changes. Failed tests will result in corrective action.
- Business continuity plans will address key dependencies, communication, alternative work methods, critical suppliers, and safe service restoration.
- Security controls must remain effective during continuity and recovery operations. Emergency access must be time-limited and reviewed after use.

19. Personnel Security and Training

- Security responsibilities will be communicated before or when personnel receive access to Company systems or protected data.
- Personnel must accept applicable confidentiality, acceptable-use, data-protection, and security obligations.
- Security awareness training will be provided at onboarding and at least annually thereafter, with additional role-based training for administrators, developers, support personnel, and others with elevated access.
- Training will address phishing, credential protection, data handling, privacy, incident reporting, device security, social engineering, approved tools, and platform data obligations.
- Where lawful and appropriate, screening or reference checks may be performed for roles with significant access to sensitive systems or data.
- Access and Company assets must be returned, disabled, or transferred promptly when personnel leave or change roles.
- Violations may result in access restriction, disciplinary action, contract termination, or legal action, consistent with applicable law and agreements.

20. Physical and Environmental Security

- Devices, paper records, and storage media containing protected information must be secured against unauthorized physical access, theft, loss, and damage.
- Work areas must be arranged to prevent unauthorized viewing of protected information. Screens must be locked when unattended.
- Visitors must not receive unsupervised access to protected systems or information unless authorized.

- Sensitive paper records and retired media must be securely destroyed or sanitized.
- Cloud and data-center physical security may be provided by approved infrastructure providers and will be considered during supplier due diligence.
- Environmental risks, including power loss, fire, water, and equipment failure, will be considered for critical infrastructure and business continuity.

21. Compliance, Audit, and Evidence

- The Company will comply with applicable privacy, cybersecurity, consumer, employment, contractual, and platform obligations relevant to the Services.
- The Information Security Owner will maintain evidence sufficient to demonstrate implementation of material controls.
- Evidence may include policies, risk assessments, access reviews, asset inventories, security configurations, change records, vulnerability reports, training records, incident records, backup tests, deletion records, and supplier reviews.
- Security controls will be reviewed at least annually and may be reviewed more frequently based on risk, incidents, significant changes, or platform requests.
- Material findings will be assigned an owner, priority, corrective action, and target date. Completion will be verified and documented.
- The Company will cooperate with authorized audits, compliance reviews, and information requests from TikTok Shop, merchants, regulators, or contractual partners, subject to confidentiality and legal requirements.
- Records provided for review must be accurate and must not misrepresent control implementation, certification, ownership, or operational capability.

22. Exceptions, Enforcement, and Policy Review

22.1 Exceptions

- Exceptions must be documented before implementation whenever practical.
- Each exception must describe the control, business reason, risk, affected systems and data, compensating safeguards, owner, approver, start date, and expiration or review date.
- Exceptions involving Restricted data, production access, platform credentials, or unresolved high risk require approval by Company Management.
- Expired exceptions are not valid and must be renewed or closed.

22.2 Enforcement

Failure to comply with this policy may result in removal of access, corrective action, disciplinary action, contract termination, notification to affected parties or platforms, or legal action, as appropriate and permitted by law.

22.3 Review and Update

- This policy will be reviewed at least once every 12 months.
- An out-of-cycle review will occur after a significant security incident, material business or system change, new API or data use, ownership change, major supplier change, or relevant legal or platform requirement.
- Material updates will be approved by Company Management and communicated to relevant personnel.
- Superseded versions will be archived according to document-retention requirements.

Appendix A. Minimum Security Control Baseline

Control Domain	Minimum Requirement	Frequency / Trigger	Evidence Examples
Governance	Approved policy owner, annual review, risk register, management escalation	Annual and material change	Approved policy, review minutes, risk register
Asset Management	Inventory of material systems, data stores, integrations, devices, and providers	Quarterly update or material change	Asset inventory, ownership list
Access Control	Unique accounts, least privilege, approved access, removal on exit	Quarterly privileged review; annual general review	Access requests, review exports, termination checklist
MFA and Credentials	MFA for high-risk systems; protected secrets; no secrets in code or logs	Continuous; rotate after exposure or requirement	MFA settings, secret scans, rotation records
Data Protection	Classification, approved storage and transmission, minimization, deletion	Continuous; review annually	Data map, retention schedule, deletion tickets
Platform Data	Approved scopes and authorization; no sale or unrelated use; token protection	Each integration and material change	Scope approval, OAuth flow, token controls, access logs
Secure Development	Controlled repository, review, testing, environment separation, change records	Each material change	Pull requests, test results, deployment records
Vulnerability Management	Monitor findings; risk-based remediation and verification	Continuous; periodic scanning	Scanner results, patch records, risk acceptance
Logging and Monitoring	Security-relevant logs, alert review, protected log access	Continuous; log review risk-based	Log configuration, alert tickets, investigation records
Incident Response	Reporting, severity, containment, investigation, notification, lessons learned	Each incident; exercise periodically	Incident record, notification log, post-incident review
Backup and Recovery	Protected backups and periodic restore testing for critical systems	According to recovery needs; test periodically	Backup reports, restore-test results
Supplier Security	Risk-based due diligence and appropriate contractual controls	Before engagement; periodic review	Vendor assessment, contract, subprocessor list
Training	Onboarding and annual security awareness; role-based training	Onboarding and annually	Training materials, completion records

Appendix B. Incident Classification and Response Targets

Targets are internal operational goals. Mandatory legal, contractual, or platform timelines take priority where stricter.

Severity	Example Impact	Initial Escalation Target	Management / External Action
Critical	Confirmed large-scale exposure of Restricted data; compromised production administrator or platform credentials; active destructive attack; major service compromise	Immediate and normally within 1 hour of confirmation	Immediate management involvement; urgent containment; assess TikTok Shop, user, regulator, and contractual notification obligations
High	Confirmed unauthorized access to Confidential data; material malware; significant service disruption; exploitable internet-facing weakness with strong evidence of abuse	As soon as possible and normally within 4 hours	Management informed promptly; containment and notification assessment started
Medium	Limited suspected exposure; contained account compromise; security control failure without confirmed material data impact	Same business day	Owner assigned; investigate, remediate, document
Low	Policy deviation or low-impact event with no evidence of unauthorized data access	Within 2 business days	Track and correct through normal security operations

Appendix C. Evidence and Review Register

The following records should be retained in a controlled location as applicable to Company operations. The list is not exhaustive and does not require creation of evidence for a control that is genuinely not applicable; any non-applicability must be documented.

- Current approved information security policy and prior versions.
- Annual policy review record and management approval.
- Information security risk register and accepted-risk records.
- Material system, data, integration, domain, credential, device, and provider inventory.
- Access approvals, privileged-access lists, periodic access reviews, and termination records.
- MFA configuration evidence and credential-rotation records.
- Secure-development, code-review, dependency, test, and deployment evidence.
- Vulnerability findings, remediation tickets, patch records, and verification results.
- Logging and alert configuration, investigation tickets, and security event records.
- Incident records, notifications, post-incident reviews, and corrective-action tracking.
- Backup status, restore-test results, recovery procedures, and continuity reviews.
- Supplier assessments, contracts, data-processing terms, and subprocessor records.
- Training materials, attendance or completion records, and role-based guidance.
- Data retention schedule, deletion requests, deletion evidence, and authorization-revocation records.
- TikTok Shop API scope approvals, authorization-flow documentation, token-protection controls, and relevant platform correspondence.

Appendix D. Reference Materials

This policy is designed to support the Company's TikTok Shop data security and privacy review and ongoing developer responsibilities. The following official materials should be reviewed when the policy or application changes:

- **TikTok Shop Data Security and Privacy Review:** https://partner.tiktokshop.com/docv2/page/data-security-and-privacy-review
- **TikTok Developer Guidelines:** https://developers.tiktok.com/doc/our-guidelines-developer-guidelines
- **TikTok Shop Developer Terms of Service:** https://partner.tiktokshop.com/docv2/page/6506bc942f024f02be400315
- **TikTok Shop Authorization Overview:** https://partner.tiktokshop.com/docv2/page/authorization-overview-202407
- **BIGVIRALS Privacy Policy:** https://www.bigvirals.com/privacy.html

Approval

Policy	BIGVIRALS Information Security Policy
Legal Entity	江西省深蓝智科文化有限公司
Version	1.0
Effective Date	July 12, 2026
Approved By	Management of 江西省深蓝智科文化有限公司
Approval Status	Approved
Next Scheduled Review	No later than July 12, 2027, or earlier upon a material change or significant security incident

Official relationship statement

江西省深蓝智科文化有限公司 is the legal entity and TikTok Shop developer. BIGVIRALS is the service brand. bigvirals-Creator Outreach is the application. https://www.bigvirals.com/ is the official website, and https://www.bigvirals.com/privacy.html is the official Privacy Policy page.

END OF POLICY