July 7, 2026

SUPPLIER DATA SECURITY REQUIREMENT

In addition to any requirements set forth in the Agreement between Supplier and Yum, Supplier(s) will comply with this Supplier Data Security Requirement ("**Security Requirement**") and perform regular monitoring of its compliance. In the event of any conflict between this Security Requirement and any other provision of the Agreement, the provision of this Security Requirement will govern and control to the extent of such conflict or inconsistency. Yum may update this Security Requirement at any time at its discretion, and Yum will provide email notification to the contact on record of any material changes to this Requirement. It is Supplier's responsibility to update Supplier contact information as needed.

1. DEFINITIONS

"**Agreement**" means the agreement between Yum and/or its affiliate(s), on the one hand, and Supplier, on the other, to which this Security Requirement refers.

(a) "**Confidential Information**" for purposes of this Security Requirement, Confidential Information shall mean any data, records, files, content or information, oral or written, in any form or format that is acquired, accessed, collected, received, stored or maintained by Supplier or its affiliates from or on behalf of Yum or its affiliates or customers, or otherwise used in connection with the Agreement, the Services, or the parties' performance of or exercise of rights under or in connection with the Agreement, including but not limited to, Personal Information relating to Yum's customers or end users ("Yum Customer Data") and Yum's employees.

(b) "**Data Protection Laws**" means any applicable law, statute, declaration, decree, directive, legislative enactment order, ordinance, regulation or rule (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regard to the Processing of Personal Information to which a Party is subject, including, but not limited to and to the extent applicable: the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., and any implementing regulations ("**CCPA**"); Regulation (EU) 2016/679 of the European Parliament and of the Council ("**GDPR**"); European Union Member State laws; the UK Data Protection Act 2018; and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), in each case as amended or superseded from time to time.

(c) **"Personal Information**" is a subset of Confidential Information and shall mean any information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, including, but not limited to, his or her name, social security number, physical characteristics, physical address, email address, telephone number, government issued ID number, unique identifier, financial information (e.g. credit card number) or medical information, or any other information that qualifies as "personal information" as such term is defined in the CCPA, or as "personal data" as such term is defined in the GDPR, or "personally identifiable information" or any similar terms under any applicable Data Protection Laws.

(d) "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. "**Multifactor Authentication**" means a multi-layered mechanism that employs multiple forms of verification designed to prevent unauthorized access to data and system resources.

(e) "**Web**" the part of the Internet that can be looked at with a special program (called a browser) and that is made up of many documents which are linked together —often used before another noun.

Capitalized terms not defined in this Security Requirement shall have the meaning given to them in the Agreement.

2. DATA TAXONOMY & CLASSIFICATION

(a) **Relationship to Contract Terms.** For the avoidance of doubt, **"Confidential Information"** as used in this Security Requirement **includes all Yum Data classified as Restricted, Confidential, or Internal under the Information Classification Standard ("ICS")**. Nothing in this section limits Yum's broader contractual definition of Confidential Information. Supplier shall classify, handle, and retain all Yum information in accordance with Yum's **Information Classification Standard ("ICS"):**

i) Restricted Information (Business / commercial data and legally regulated data) means Yum Data where unauthorized disclosure could cause financial, legal, or competitive harm, or that is protected by law or regulation.

ii) Confidential Information (Contextualized data) means Yum Data that is not directly identifiable on its own, but that could become PII or be linked to an individual when combined with other information, and where disclosure could create privacy concerns.

iii) Internal Information (Operational data) means Yum Data used for routine internal business operations that is not legally restricted and not intended for public release.

iv) Public Information means Yum Data that Yum has expressly made publicly available or has expressly designated in writing as "Public."

(b) **Supplier Classification Duties.** Supplier shall: (i) apply the appropriate **classification label** to each Yum Data set it receives or generates; (ii) **preserve classification metadata** throughout the information lifecycle (collection, storage, Processing, sharing, archive, disposal); (iii) **default to the higher protection** when classification is uncertain and promptly seek confirmation from Yum; and (iv) handle records per industry best practices for ICS **retention classification**, including **de-identification** when required and **secure destruction** once retention expires or at Yum's written direction, subject to legal holds.

(c) **Retention and Disposal.** Yum may specify retention and destruction requirements for any category of Yum Data in an Order, statement of work ("SOW"), or written instruction. Supplier shall retain and dispose of Yum Data strictly in accordance with such written requirements and, in all cases, shall dispose of Yum Data securely and irreversibly so that it cannot be reconstructed or retrieved

(d) **Handling by Classification (minimums).** At a minimum: **Restricted** data is limited to need to know, **encrypted in transit** and—where applicable under Yum standards—**at rest**; **Confidential** Information is **encrypted in transit** and handled per ICS; **Internal/Public** data is handled per ICS and may not be downgraded without Yum approval.

3. RIGHT TO AUDIT

(a) An initial cyber security assessment will be performed by Yum prior to the execution of the Agreement. During this assessment, Supplier will be expected to provide relevant industry standard attestations based on and for the products and services provided. These attestations may include but are not limited to PCI Level 1 Service Provider, ISO 27001 and SOC 2 Type 2 with no exceptions or evidence of remediation of those exemptions. If, for some reason, at the time of Agreement execution, any findings or issues identified during Yum's initial cyber security assessment remain unresolved, Supplier shall, within ten (10) business days of execution, provide a written mitigation plan for all open identified issues as an addendum to the Agreement. The mitigation plan shall include specific corrective actions, assigned responsible parties, and timelines for remediation. Supplier shall complete all remediation activities and provide Yum with written evidence of completion within ninety (90) days of contract execution. Evidence may include, but is not limited to, updated policies or procedures, screenshots demonstrating implementation of controls, or a live review session with Yum's Third-Party Cyber Security Team. If Supplier fails to complete remediation within the ninety (90)-day period, Yum may, in its sole discretion, terminate the Agreement and any existing Order Forms or SOWs without penalty. Supplier shall complete a recurring assessment based on the risk designation from Yum that may occur every 1 year, but no less than every 3 years.

(b) During the Term of the Agreement Yum reserves the right, with reasonable notice, to audit and inspect Supplier's facilities, systems, Supplier's data protection controls and risk management program. Upon Yum's request, Supplier will make available to Yum documentation sufficient to demonstrate Supplier's compliance with this Agreement. Such documentation will include a copy of all third-party certifications and/or audits, in their then-most-current form, that relate to Supplier's compliance with data protection, privacy, or information security standards or requirements.

(c) Supplier will provide, at its own expense, an independent audit report, commonly known as a Statement on Standards for Attestation Engagements (SSAE) No. 18 including the Service Organization Control (SOC) reporting framework (SOC 2).

4. SUSPENSION

In the event Supplier believes or determines that it can no longer meet its obligations under this Security Requirement, Supplier shall: (a) immediately cease processing the Yum Data; (b) immediately notify the Yum project lead identified in a current Order Form or SOW; and (c) take all reasonable and appropriate steps to remediate any failure to meet its obligations. All such activities undertaken hereunder shall be at Supplier's expense.

5. IDENTITY, ACCESS & CONNECTIVITY CONTROLS

(a) Scope & Principles. This section applies to: (a) Supplier personnel accessing Yum owned or managed systems; (b) Yum personnel accessing Supplier hosted systems and applications (including SaaS platforms that store or process Yum Data); and (c) service to service integrations. Access must follow least privilege and be explicitly tied to ICS data classes.
These controls establish the minimum identity, access, and connectivity standards applicable to all Suppliers. Where a Supplier provides managed support services, additional operational specifics (e.g., support tiers, approval workflows, or escalation matrices) may be defined in the applicable SOW.

(b) Prohibited Connectivity. Site to site VPNs and any persistent network level tunnels (including IPSec/SSL VPN) between Supplier and Yum are prohibited. Connectivity must be application layer, identity centric (e.g., HTTPS/TLS, SFTP/SSH) and follow Yum's encryption parameters.

(c) Federation & Authentication (SSO + MFA).

i. Supplier users accessing Yum systems: Supplier personnel must authenticate via Yum's SSO and MFA via mobile devices or Supplier provided and managed FIDO Keys; no local or shared accounts or shared MFA devices are permitted.

ii. Yum users accessing Supplier systems (SaaS): At Supplier's expense, Supplier must ensure Yum is granted access to Supplier systems/applications only via Yum's SSO Identity Platform (SAML 2.0 or OIDC). Supplier will honor Yum's MFA assertion and support automated user lifecycle via SCIM 2.0 (or equivalent APIs) for timely provisioning, role changes, and deprovisioning. Direct username/password access for Yum users is not permitted except for documented break glass accounts held in a secure privileged access management vault with post use review and credential rotation.

iii. Machines & service identities: Use mTLS and/or OAuth2 service principals with scoped permissions; no embedded static credentials. Keys/secrets must follow Yum crypto/key management (secure generation & storage, encryption in transit/at rest, 12month rotation, immediate revocation on compromise).

(d) Least Privilege, Role Based Access Controls & Segregation of Duties. Supplier shall implement and maintain:

i. Role Based Access Controls by duty & data class; default is no access. Data Class may also include, but not be limited to separation by Yum User organization, ex. Franchise Organization A is unable to read or modify data for Franchise Organization B.

ii. **First-level (L1) support or analyst roles** — intended only for basic troubleshooting — shall be **read-only and non-destructive** (no capability to change configurations, permissions, security controls, or data states that could impact Yum).

iii. Use Just in Time, time-boxed elevation with ticket/approval linkage; avoid standing admin rights.

iv. Segregate duties (security vs. ops vs. data export/reporting).

v. Unique IDs only; no shared or generic accounts.

(e) Access Lifecycle & Reviews. Immediate removal on separation; quarterly reviews of privileged roles (including SaaS tenant admins & service principals) and semi-annual reviews of standard roles; provide evidence upon request or material change (TVRM).

(f) Logging, Monitoring & Evidence. Supplier shall log admin actions, authorized events (success/failure), privilege grants/changes, and data export jobs; retain per Requirement; provide to Yum on request. Support audits consistent with Right to Audit/TVRM and reassess on material change.

(g) Endpoint & Session Security (Supplier workforce). Supplier shall require managed devices, endpoint protection, full disk encryption (FDE), screen-lock, current patches; timeouts and re-authorization for sensitive ops.

(h) Exceptions. Any exception(s) to this Section requires Yum's written approval.

6. SUPPLIER INFORMATION SECURITY PROGRAM

Supplier shall establish, implement, maintain, and enforce a written information security program (the "Supplier Security Program") appropriate to the nature of the Services and the sensitivity and volume of Yum Data. The Supplier Security Program shall include administrative, technical, and physical safeguards designed to: (i) ensure the confidentiality, integrity, and availability of Yum Data; (ii) protect against anticipated threats or hazards to Yum Data and the systems that Process it; (iii) protect against unauthorized or unlawful access to, use of, disclosure of, or destruction of Yum Data; and (iv) ensure secure retention and disposal of Yum Data.

The controls set forth in Sections 6 through 18 of this Security Requirement constitute minimum requirements of the Supplier Security Program. Supplier shall review and update the Supplier Security Program at least annually and upon any material change in its risk environment or the Services.

7. ACCESS CONTROL

Supplier has policies, controls and procedures that meet or exceed industry-accepted authentication and access controls, including Single Sign-On (SSO), Multifactor Authentication (MFA), and secure remote access that authenticates all users, limits their activity to required systems and data, encrypts connections, and logs activity while on the network. All systems and platforms must be protected with passwords that meet or exceed widely accepted industry configuration and management requirements, including changing all default vendor passwords, requiring users to change passwords at first login and after any reset by someone other than the user, and using passwords to verify identity before granting access. User accounts shall be created and revoked through a standard approval process, be uniquely assigned to individuals (not shared), and be uniquely assigned per restaurant for devices such as routers, switches, and firewalls; accounts must be categorized (e.g., privileged, restaurant, service, or user), and default accounts shall be identified and disabled or removed, with access configured to enforce separation of duties. Franchisee shall ensure that user access is appropriate to each individual's current job function, not excessive, limited to what is needed to perform assigned responsibilities, and reviewed at least annually or whenever users change roles.

8. NETWORK SECURITY

Supplier has policies, controls, and procedures to safeguard and monitor the networks and systems that process Yum Data or provide services to Yum systems including security controls that must be present at any boundary between a trusted network and/or any untrusted or public network.

9. SYSTEM RISK MITIGATION

Supplier has policies, technical controls, and procedures in-place to assess, report, manage, and address internal and third-party risk.

Supplier shall operate a continuous vulnerability management program that includes regular scanning and penetration tests of systems, services, and networks; application security tests; and the timely installation of all relevant vendor security patches.

Supplier also subscribes to relevant manufacturer and industry security advisory services.

10. CRYPTOGRAPHIC CONTROLS

(a) Use of Approved Cryptography. Supplier shall use only modern, publicly reviewed cryptographic algorithms and implementations to protect Yum Confidential Information; proprietary algorithms are prohibited unless reviewed by qualified independent experts and expressly approved by Yum Cybersecurity. Supplier shall comply with applicable export controls and local crypto laws and shall use FIPS 140-2 (or successor) validated cryptographic modules.

(b) When Encryption Is Required. Encrypt Yum Confidential Information: (i) in transit outside the Yum network (all data classes); (ii) at rest where applicable, including aggregated customer/employee data and field-level encryption for national identification numbers; (iii) where required by law or classification; (iv) for transfers [greater than?] > 30 MB; and (v) when saved to portable/removable media. Use Yum-approved transfer systems for manual/automated file movement.

(c) Minimum Cryptographic Parameters. TLS 1.2+ (TLS 1.3 preferred); SHA-256 or stronger for certificate signatures; RSA-2048 or ECDSA P-256 (or stronger) for public-key certs; AES-128 minimum / AES-256 preferred for symmetric encryption; secure transfer protocols such as HTTPS/TLS and SFTP/SSH. SSL and TLS < 1.2 are prohibited.

(d) Certificates, Trust & Clear-Text Prohibitions. Use trusted keys/certificates; any internal Root/Subordinate CA acting on Yum's behalf must be securely operated and controlled. No clear-text HTTP; no clear-text email for transmitting User Data.

(e) Key Management. Secure key generation & storage; encrypt keys in transit/at rest; rotate at least every 12 months; revoke/replace immediately upon compromise; agree to algorithm/length upgrades within mutually agreed timelines.

(f) Evidence, Audit & Exceptions. Supplier shall provide updated crypto configuration evidence/attestations upon material change or upon Yum's request; Yum reserves the right-to-audit; any deviations require a mitigation plan consistent with TVRM.

11. ENDPOINT PROTECTION / LOGGING AND MONITORING

Supplier shall ensure that industry-accepted Endpoint Detection and Response software that is required actively runs on all systems, Supplier owned and managed infrastructure, IaaS, and workstations, etc.

A security incident and event logging monitoring system must be used to log all access attempts to systems, data or application services that process Yum Data or provide services to Yum. Systems administrators must be alerted to all suspected unauthorized attempts to access, manipulate or disable associated systems, data or application services. Alerts will be monitored 24 hours per day, seven days per week, 365 days per year and security event logs will be maintained for a minimum of 90 days.

12. SECURITY INCIDENT NOTIFICATION

Notification. In the event that Supplier becomes aware of any actual or potential incident involving unauthorized access, collection, acquisition, use, transmission, disclosure, corruption or loss in relation to Confidential Information, or breach of any Supplier (or Supplier's Subprocessor) environment containing Confidential Information (a "**Security Incident**"), Supplier shall: (i) notify Yum immediately, and in no event later than forty-eight (48) hours after discovery of the Security Incident, and (ii) reasonably assist Yum with an investigation into the Security Incident, at the Supplier's cost and expense. In connection with any such notification, Supplier shall at minimum set forth (i) the nature of the Security Incident; (ii) the categories and number of individuals affected, as well as the approximate number of Personal Information records concerned; (iii) the potential consequences; (iv) the measures Supplier has taken or will take to minimize possible harm, and (v) the identity and contact details of a contact person (including, where applicable, the identity and contact details of a Data Protection Officer). To the extent the foregoing information is not known or knowable at the time of notification, Supplier may supplement the Security Incident Notification based on the results of its investigation.

Notification required pursuant to this section may be made via telephone call to the following contact:

July 7, 2026

Yum Service Desk (US - 1.877.498.6986 or International – 1.859.586.3727)
YumServiceDesk@yum.com
IncidentResponse@yum.com

Remediation and Notification. In response to a Security Incident, Supplier shall immediately take all steps necessary, at Supplier's expense, to comply with applicable Data Protection Laws and to take any remedial steps necessary to remedy any non-compliance with this Security Requirement and/or to protect Confidential Information. In the event the incident is classified as a Denial of Service (DoS) attack, Supplier will detect and counteract or negate this activity. To the extent the Security Incident gives rise to third-party notification obligations required by applicable Data Protection Laws, subject to all the terms herein, Yum shall be responsible for ultimately making all notifications required by applicable Data Protection Laws, provided that Supplier shall reimburse Yum for any reasonable notification costs. Further, Supplier agrees not to notify any regulatory authority (including but not limited to the Federal Trade Commission, State Attorneys General, Data Protection Authority or similar agency in countries outside of the U.S.), or any customer, end user or other individual, on behalf of Yum, unless Yum specifically requests in writing that Supplier do so and Yum reserves the right to review and approve the form and content of any notification before it is provided to any such party. Supplier shall provide immediate, written, notification to Yum upon receipt of any oral or written notice of inquiry, investigation or review from any individual or administrative agency (such as the Federal Trade Commission, State Attorneys General's offices, Data Protection Authorities or other similar agencies in countries outside of the U.S.) that arises out of or relates to the Security Incident, or that otherwise affects the Services provided by Supplier. Supplier will comply with Yum's requests and make all reasonable efforts to assist Yum in relation to the investigation and remedy of any Security Incident and any claim, allegation, action, suit, proceeding or litigation with respect to the Security Incident.

13. PAYMENT CARD INDUSTRY SECURITY STANDARDS & PAYMENT CARD DATA

(a) Payment Card Industry Security Standards & Payment Card Data (if applicable). If Supplier, or any third party provided/used by Supplier, is responsible for processing, storing and/or transmitting Yum credit and debit cardholder data ("Payment Card Data"), Supplier represents and warrants that Supplier or such third party (as applicable) is and shall continuously remain fully compliant with all applicable Payment Card Industry (PCI) compliance standards as a Service Provider (as classified by the PCI Security Standards Council) for the duration of the Agreement and for as long as it transmits, stores or processes Payment Card Data. Representation shall be provided in the form of a completed, signed PCI Attestation of Compliance (AOC) demonstrating successful fulfillment of requirements (and, where applicable, a Report on Compliance (ROC)). Supplier understands that PCI DSS requirements may exceed or be in addition to the requirements in this Security Requirement. Evidence will be provided upon Yum's request or upon material change consistent with TVRM reassessment triggers.

(b) If a Security Incident involves any actual or threatened unauthorized access to or acquisition of Payment Card Data, then, upon written request, and within twenty-four (24) hours of receipt of the request, Supplier will provide a full and complete copy of the results of any digital forensic examination and remediation recommendations to Yum. This PCI-specific requirement supplements the Security Incident terms above in Section 12.

14. Incident Response Plan Requirements

Supplier will maintain an incident response plan to address a potential event of a Security Incident. Supplier will review the plan on a periodic basis and test annually to ensure the adequacy of the response process and associated procedures.
Supplier will designate, and train specific personnel with Security Incident responsibilities to be available on a 24/7 basis to respond to alerts.

15. Data Storage

Supplier will store, process, and maintain Yum Materials only on identified internal systems or approved third-party providers. Yum Materials must not be transferred to external systems, portable devices, or storage media, except for encrypted backup and recovery purposes as specified.

16. Data Transmission

Supplier agrees that any and all electronic transmission or exchange of system and application data with any Customer and/or any other parties expressly designated by Customer shall take place via secure means (using HTTPS or SFTP or equivalent) and in accordance with the applicable Data Protection Addendum/Agreement.

17. Data Re-Use

Supplier agrees that any and all Yum Materials exchanged shall be used expressly and solely for the purposes enumerated in this Agreement and, with respect to Personal Data, for the purposes originally specified to Users at the time of collection of such Personal Data. Yum Materials shall not be distributed, repurposed or shared across other applications, environments, or business units of Supplier. Supplier further agrees that no Yum Materials of any kind shall be transmitted, exchanged, or otherwise passed to other Suppliers or interested parties except on a case-by-case basis as specifically agreed to in writing by Yum.

18. Systems and Data Backup

Supplier will perform daily incremental and weekly full backups of Yum Materials. Backup media will be securely stored off-site by a reputable, temperature-controlled storage provider. Upon request, Supplier will provide an extract of Yum Materials in an open standard file format at no extra cost. If restoration is needed due to Supplier's actions, Supplier will promptly reconstruct and restore Yum Materials at no additional charge according to current procedures.

19. Physical Security

Supplier shall ensure the use of appropriate facility entry controls (i.e., authorized/guest access, badge readers, ID cards, etc.) to limit and monitor physical access to systems.

20. Application Design, development, and Maintenance

July 7, 2026

Supplier shall have and maintain secure development policies, controls and procedures for a secure System Development Life Cycle (SDLC) that involves security in product development and implementation, trains personnel in secure development and coding concepts and practices, and verifies that products meet security requirements prior to delivery. The secure SDLC shall incorporate leading practices for authentication, authorization, and access control; data validation, transmission, and storage; cryptography; session management; and error handling.

Supplier shall comply with Open Web Application Security Project (OWASP) Top 10 Controls, and with respect to all AI Systems relying on or including a large language model (LLM), use good faith efforts to assess and comply with OWASP Top 10 for LLM Applications to the extent reasonably applicable to the Services.