Yum China Holdings, Inc.

Information Security Policy

Yum China Holdings, Inc. (referred to as **"we"**, **"our"**, or the **"Company"** herein) is committed to managing information security risks by safeguarding our systems from threats, including malicious attacks, data losses, and service disruptions. This policy formalizes our commitment to ensuring the confidentiality, integrity, and availability of information, thereby protecting the interests of our stakeholders.

We commit primarily to the following principles:

1. Establishing Individual Responsibilities for Information Security

Every employee is accountable for maintaining information security. This includes adhering to security protocols, completing mandatory training, and promptly reporting any suspicious activity. Failure to comply may result in disciplinary actions.

2. Ensuring Integrity and Protection of Data

We prioritize the accuracy, consistency, and protection of data against unauthorized access, tampering, or destruction. Security controls-such as encryption and access restrictions-are implemented and maintained throughout the entire data lifecycle.

3. Continuously Improving Information Security Systems

We proactively enhance our technical and organizational security measures through regular reviews and vulnerability assessments. We regularly engage external consultants to assess and independently verify our cybersecurity risk management, striving for continuous optimization of our cybersecurity policies, cybersecurity risk management processes, and technical measures.

4. Monitoring and Responding to Information Security Threats

Cybersecurity risks are actively monitored using automated tools and expert analysis. In the event of an incident, we undertake prompt containment, conduct investigations, and implement mitigation measures.

5. Establishing Information Security Requirements for Third Parties

Third parties who have access to Company data, infrastructure, or services are also required to comply with our information security standards. We have established processes designed to manage cybersecurity threats associated with the use of third-party service providers. These processes include security evaluations before third-parties' admission, ongoing oversight and assessment of their security status, and adopting necessary security measures at termination of services.

Scope

This policy applies to all employees and third parties who have access to Company data, infrastructure, or services.

Compliance

Non-compliance with this policy may result in legal action, contract termination, or internal disciplinary measures.

Detailed controls, roles, and procedures are specified in the Internal Yum China Information Security Policies and Standards.