YANFENG SECURITY STANDARD

1. Scope and General Considerations

This Security Standard sets forth security requirements (security measures and procedures) with respect to YANFENG Information Assets (YANFENG IA) created, collected, received, transferred or otherwise obtained or disclosed by YANFENG to Vendor in connection to the Services.

In the event of any conflict between the provisions of this Standard and other contractual provisions, the provisions that are more protective of YANFENG IA shall prevail.

In order to fulfill YANFENG's high security and compliance standards, Vendor shall implement adequate and appropriate technical and organizational security measures designed and necessary to secure YANFENG IA against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access - in particular where the Processing involves the transmission of data over a network - in light of the relevant risks presented by the Processing. These measures shall ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

Vendor shall periodically review and update such measures and maintain the same in accordance with no less than industry-standard methods of protection. Without limiting its obligations otherwise set forth herein, Vendor shall comply with all applicable laws relating to its Processing of YANFENG IA.

Vendor warrants and represents to have implemented security measures that meet or exceed the requirements laid down in this Security Addendum. Vendor needs to provide YANFENG with sufficient documentation to demonstrate adherence to this Security Standard.

Failure to maintain these obligations constitutes a material breach of this Security Standard and, in addition to YANFENG's other rights, YANFENG may choose to terminate the Agreement.

2. Definitions

"YANFENG"	shall mean the same as in the Agreement
"YANFENG Information Assets" (YANFENG IA)	shall include any body of YANFENG information or knowledge that is defined, organized and managed as a single unit and has a recognisable and manageable value, risk, content and lifecycle. It includes YANFENG's information computing systems and data, including specifically Personal Data.
"Agreement"	shall include any kind of MSA, Statement of Work ("SOW") or any other kind of agreement between YANFENG and Vendor with regards to the Services.

"Security Event"	a) indicates that the security of an information system, service, or network **may have been** breached or compromised; b) indicates that an information security policy **may have been** violated or a safeguard may have failed; c) means a Log Entry with a negative consequence or potentially negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data or execution of malicious code that destroys data has occurred.
"Security Breach"	means a Security Event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to YANFENG IA including Personal Data transmitted, stored or otherwise processed;
"Personal Data "	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
"Processing"	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Security Rules"	mean rules applicable to the Vendor with regards to information security, including regulatory rules and state of the art standards on information security and rules that derive from applicable laws (e.g. privacy laws)
"Services"	mean services as described in the Agreement, or other mutually agreed upon written description of services that has been executed by the parties
"Sub-Contractor"	means any service contractor or service provider engaged by Vendor or by any other Sub-Contractor that directly, or indirectly, impact YANFENG IA. This includes any kind of services involving Processing, accessing, communicating, hosting or managing the YANFENG IA, or adding or terminating services or products to existing information by a person engaged or included to the service by the Vendor.
"Vendor"	any party other than YANFENG that Processes YANFENG IA, including Cloud Vendor service providers

3. Governance

3.1 Personnel

Prior to granting individuals physical or logical access to facilities, systems or data which involve YANFENG IA, Vendor shall take reasonable steps to ensure that its employees, other persons acting under its authority and other persons at the place of work concerned (including third party users, tenants and/or customers) are bound to legally binding obligations that meet or exceed the security measures mentioned in this Security Standard, measures enacted or to be enacted by relevant authorities or as provided by applicable Security Rules (for Sub-Contractors see section 3.2 below).

Pursuant to local laws, regulations, ethics and contractual constraints all Vendor's employment candidates and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Vendor shall ensure that their staff that has access to YANFENG IA is adequately informed and skilled to ensure the protection of YANFENG IA.

3.2 Sub-Contractors

Whenever Vendor subcontracts work that relates to YANFENG IA to Sub-Contractors the applicable requirements set forth under this Security Standard need to be complied with at all times. Vendor shall provide the list of Sub-Contractors and applicable certifications upon request. YANFENG may object to the use of a new Sub-Contractor in writing if the new Sub-Contractor represents an unacceptable risk to the security of the YANFENG IA.

Pursuant to local laws, regulations, ethics and contractual constraints all Vendor's Sub-Contractors shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Vendor shall ensure that all the Vendor's sub-contractors that touch YANFENG IA holds applicable security certifications and adheres to security best practices.

Vendor shall ensure that all Sub-Contractors have been bound by an agreement including explicit coverage of all relevant security requirements compatible with this Standard and pursuant to applicable Security Rules. Sub-Contractors specifically need to be obliged to bind its personnel to substantially similar obligations as laid down in Section 3.1 above.

Vendor shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in such third-party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.

Vendor remains responsible to YANFENG for any and all performance by its Sub-Contractors in relation to the protection of YANFENG IA.

3.3 Development of Applications

Vendor applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and shall comply with applicable regulatory and business requirements.
Vendor shall establish a program for the systematic monitoring and evaluation to ensure that standards of quality are met, including but not limited to all outsourced software development. Vendor shall supervise and monitor the development of all software and shall include security requirements, independent security review of the environment by a certified individual, certified security training for software developers, and code reviews. Certification for the purposes of this control shall be defined as either an ISO/IEC 17024 accredited certification or a legally recognized license or certification in the applicable legislative jurisdiction.
At a minimum, the Vendor shall provide a bug list and code analysis at time of release.

4. Technical and Organizational Measures

Vendor shall implement the following technical and organizational measures to secure YANFENG IA:

4.1 Physical access control

Vendor shall implement suitable measures to prevent unauthorized persons from gaining physical access to the data Processing equipment where YANFENG IA are Processed, transferred or used in any manner. This shall be accomplished by, e.g. providing that entries to data Processing facilities (the rooms housing the application servers, computer hardware, database and related equipment etc.) are capable of being locked.

4.2 Admission control

Vendor shall implement suitable measures to prevent its data Processing systems from being used by unauthorized persons.

4.3 Virtual access control

Vendor shall implement suitable measures, including provisioning and de-provisioning processes, to ensure that those persons authorized to use a Processing system are only able to access YANFENG IA within the scope of their need to access (authorization) and in accordance with business, security, compliance and service level agreement (SLA) requirements, and that YANFENG IA cannot be read, copied, modified or deleted without appropriate authorization during Processing and after logging.
Vendor shall implement timely de-provisioning, revocation or modification of user access upon any change in status of employees, contractors, customers, business partners or third parties, including termination of employment, contract or agreement, change of employment or transfer within the organization.

Prior to the Vendor granting access to YANFENG IA's and systems, all identified security, contractual and regulatory requirements shall be remediated where applicable.

4.4 Transmission control

Vendor shall implement suitable measures to ensure that, during electronic transfer, transportation or when being saved to data carriers, YANFENG IA cannot be read, copied, modified or deleted without authorization, and that it is possible to check and establish to which bodies the transfer of YANFENG IA by means of data transmission facilities is envisaged.

Applicable for Vendors providing networks services

Vendor network environments shall be designed and configured to restrict connections between trusted and un-trusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.

4.5 Job / Assignment Control

Vendor shall implement suitable measures to ensure that, in the case of commissioned Processing of YANFENG IA, YANFENG IA are Processed strictly in accordance with the instructions of YANFENG.

4.6 Capacity & Resource Planning / Business Continuity / Availability Control

4.6.1 Capacity & Resource Planning

Vendor shall plan, prepare and measure its systems availability, quality, and adequate current and preventive capacity and resources to deliver the required system performance in accordance with regulatory, contractual and business requirements. Vendor shall provide a copy of the Capacity / Resource Planning Metrics and applicable assessments to YANFENG upon request.

4.6.2 Business Continuity

Vendor shall implement and maintain a Business Continuity Program; ensuring continuity of vendor services (i.e. customer service, technical support, incident management). Vendor shall conduct a business continuity exercise annually and shall

provide YANFENG evidence of business continuity exercise within 30 days of YANFENG's request. Evidence shall include Date and time of exercise, Scope of exercise, Summary and finding.

4.6.3 Availability Control

Vendor shall implement suitable measures to ensure that YANFENG IA are protected from accidental destruction or loss and from denial of service attacks.

Additional Back-up / Disaster Recovery requirements for Vendors providing hosting services YANFENG IA: Vendor shall ensure that all YANFENG IA is regularly backed up to facilitate quick recovery in case of disasters. Application and System architecture(s) shall support YANFENG's Disaster Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Vendor shall implement and maintain a Disaster Recovery Program; ensuring a continuity of technologies, application and software services provided to YANFENG by this agreement. Vendor shall conduct a disaster recovery exercise annually and shall provide YANFENG evidence of disaster recovery exercise within 30 days of YANFENG's request. Evidence shall include:

- Date and time of exercise
- Scope of exercise
- Summary and Findings
- Achieved Recovery Time Objective
- Achieved Recovery Point Objective
- Method used to validate RPO

Specifically, Vendor shall implement measures to ensure that:

- a back-up is performed at least daily;
- tape backup are stored off-site and available for restore in case of failure of SAN infrastructure for database server;
- only YANFENG may authorize the recovery of backups (if any) or the movement of data outside the location where the physical database is held, and security measures will be adopted to avoid loss or unauthorized access to data, when moved;
- backup tapes are only re-used if information previously contained is not intelligible and cannot be re-constructed by any technical means; other removable media is destroyed or made unusable if not used; and
- testing the recovery of backups is carried out at planned intervals

4.7 Input Control and Logging

Vendor shall retain audit logs recording user access activities, modification or deletion of any data, authorized and unauthorized access attempts, system exceptions, and information Security Events, complying with applicable policies and regulations. Vendor shall review audit logs at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents.

4.8 Separation control

Vendor shall ensure a clear separation of YANFENG IA from other customers' data. The separation must be ensured at the logical level which includes the application and preferably at the physical level.
Vendor shall ensure that data collected for different purposes can be Processed separately.

4.9 Other operational security measures

4.9.1 Vulnerability / Patch Management

Vendor shall establish policies and procedures and implement mechanism for Vendor vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.

4.9.2 Anti-Virus / Malicious Software

Vendor shall ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.

4.9.3 Security Checks

Vendor shall provide on-going security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees

4.9.4 Unauthorized Software Installations

Vendor shall establish policies and procedures and implement mechanisms to restrict the installation of unauthorized software. Vendor shall report any exceptions and need to be approved by YANFENG prior to installation.

4.9.5 Production changes

Changes to the Vendor provided YANFENG production environment shall be documented and tested and need approval by YANFENG prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.

5. Information Security Management System

5.1 General Management System

Vendor shall maintain a proper information security management program adequately communicated and published to employees, contractors and other relevant external parties.

5.2 Third Party Management Reports

Vendor shall provide evidence of security controls and their effective operation and provide YANFENG an acceptable annual third-party security report scoped to the specific services YANFENG is procuring from Vendor and all Vendor Sub-Contractors that touch YANFENG data, e.g. SSAE-16 (U.S.), CSAE-3416 (Canada), ISAE-3402 (International) SOC 2 Type 2 Report on an annual basis. This annual security report will follow the AICPA standards for a SOC 2 Type 2 report and will include the tests and effectiveness of Vendor controls as related to the AICPA Trust Services Principles and Criteria associated with security, confidentiality, processing integrity, privacy and availability.

Vendor agrees to remediate any material deficiencies revealed in such report in a commercially reasonable manner and time frame.

Vendor shall also provide an acceptable third-party system / application penetration security report and vulnerability assessment security report on an annual basis

Applicable for Vendors hosting YANFENG IA

Vendor shall develop, document, approve and implement an Information Security Management Program (ISMP) that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction, e.g. ISO 27001:27005.

5.3 Audits / Inspections

In addition, at planned intervals and upon prior written notice, YANFENG may inspect Vendor's operating facilities or conduct an audit to ensure Vendor is compliant with policies, procedures, standards and applicable regulatory requirements and to ascertain compliance with this Standard. YANFENG or an independent audit team may carry out the inspection. Vendor shall fully cooperate with any such audit and investigation procedures initiated by YANFENG.

6. Risk Management

Vendor shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level. Vendor shall perform formal risk assessments at least annually, or at planned intervals, determining the likelihood and impact of all identified risks.

Vendor shall mitigate risks to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.

Vendor will provide evidence of cybersecurity insurance, i.e. Privacy / Network Security (Cyber) liability coverage providing protection against liability for (1) Security Breaches (no matter how it occurs); (2) system breach; (3) denial or loss of service; (4) introduction, implantation, or spread of malicious software code; (5) unauthorized access to or use of computer systems. No condition precedent, including any exclusion/restriction for unencrypted portable devices/media may be on the policy. Minimum required insurance limit - $10,000,000.

7. Event, Incident, Threat and Vulnerability Management / Security Incidents and Breach Notification

Vendor shall establish policies and procedures to triage security related events and ensure timely and thorough incident management.

Vendor shall immediately inform YANFENG in the event of a potential Security Breach. The information should provide the details of YANFENG IA compromised, including

- information on the YANFENG IA, data / persons affected such as categories and number of persons affected;
- a description of the nature of the unlawful disclosure,
- the identity and contact details of a contact person
- the likely consequences of the potential Security Breach, and
- the recommended measures to minimize possible harm.

Vendor shall provide all additional information requested by YANFENG to investigate the potential Security Breach.

In addition, Vendor shall inform YANFENG immediately if (i) Vendor or its Personnel, Affiliates or Sub-Contractors infringe Security Rules or obligations under this Standard, (ii) significant failures occur during the Processing, or (iii) there is reasonable suspicion of the occurrence of an event as defined under (i) and (ii) of this paragraph. In consultation with YANFENG, Vendor shall take appropriate measures to secure YANFENG IA and limit any possible detrimental effect on YANFENG and any persons.

In the event a follow-up action resulting from a Security Breach requires legal action, subject to the relevant jurisdiction, proper forensic procedures including chain of custody shall be carried out by the Vendor and any Sub-Contractor for collection, retention, and presentation of evidence and shall be made available upon request.

8. Return and Deletion of YANFENG IA

Upon termination of these Terms, Vendor, at the discretion of YANFENG, shall return to YANFENG or destroy and delete all YANFENG IA and other materials containing YANFENG IA from YANFENG subject to Processing, unless applicable rules require storage of the YANFENG IA. Additionally, all YANFENG IA should be expunged from any computer, server, media, storage or similar device including backup storage in which it was stored or Processed by Vendor or by its Sub-Contractors. Vendor shall certify that this has been done upon YANFENG's request.

Vendor shall establish policies and procedures and implement mechanisms for the secure disposal and complete removal of YANFENG data from all Vendor storage and certification of proper disposal.