光大控股
EVERBRIGHT LIMITED

China Everbright Limited

Data Security and Privacy Statement

（Version Date: September 2023 ）

I. Scope of Application

This policy is applicable to all business lines of China Everbright Limited (“CEL” or the “Company”).

II. Data Security Management

(I) Framework for Data Security Management

One of the activities of the Risk Management Committee under the Management Decision Committee is to hold IT risk meetings. CEL vice president in charge of IT reports directly to the Board of Directors on data security, information security and other related matters as needed. CEL identifies the IT risks it is exposed to as needed.

(II) Measures to Strengthen Data Security

CEL implements a wide range of data security measures, including:

(1) Separating the production environment from the maintenance environment and the development team from the maintenance team to ensure the safety of production environment and data, and strictly controlling access to data centres; (2) setting up a Demilitarized Zone (DMZ) for application data that have to be exposed to the internet; and (3) during system deployment, putting data on the intranet which, when combined with infrastructure-based access control to server IPs, dual firewalls, intrusion detection system, and other information security systems, can prevent data breach.

CEL specifically mandates that: (1) all data storage media containing internal information must be physically destroyed; (2) prior to decommissioning any computer used to store internal information, a certified data eraser tool must be used to permanently delete all data in the computer system’s disk storage; and (3) any paper document containing internal information must be shredded.

(III) Response to Security Incidents

CEL has in place a fully developed protocol for handling security incidents, covering incident response and follow-up actions to minimize the impact and losses.

1. Incident Response

Response to security incident involves launching procedures to evaluate the incident and to respond in order to restore affected system components and services as soon as possible. The procedures are broadly categorized into five stages: identification, escalation, containment, eradication, and recovery; CEL has established specific steps for each.

2. Follow-Up Actions

After a system is restored to normal operation, CEL will conduct evaluation of the damage caused, system refinement to prevent reoccurrence of the incident, security policies and procedures update and, if necessary, case investigation for subsequent prosecution. Follow-up actions include post-incident analysis, post-incident report, security assessment, review of existing protection, etc.

(IV) Data Security Policy and System Audit

1. Internal Audit

To prevent risks potentially associated with CEL data security rules and procedures, the CEL Operation Centre is tasked with maintaining and updating the CEL IT Security Policy and other data security policies on an annual basis, and the Senior Management is tasked with the periodic review and issuance of those policies.

2. Third-Party/External Audit

CEL takes data and IT system security seriously. Apart from internal audit, CEL engages independent third parties from time to time to audit Company data and information systems, in order to ensure that its information systems meet the standards in terms of data security and system safeguards.

(V) Employee Training on Data Security

To raise CEL staff's security awareness and help them develop a clear understanding of the importance and targets of data security, CEL conducts regular training for all CEL staff including employees and contractors.

CEL has developed the CEL IT Security Policy and other security rules, which, along with related training materials, are accessible by staff members at any time from the OA system and training system. Data security and system usage are also covered by CEL's training program for new hiring. 69 new recruits have received security training in 2022.

III. Customer Privacy Protection

(I) CEL customers are predominantly institutions rather than individuals. As such, it only collects customer information to fulfil “know your customer (KYC)” and anti-money laundering (AML) requirements. This information is mainly collected offline by CEL’s business team and then entered into the Company’s Private Equity Investment Management (PE) system for centralized, online-based management.

CEL has no customer-facing service platform and does not collect private customer information through such channels as apps and websites. Additionally, because CEL’s core business is alternative asset management, its products and services do not involve the collection of privacy information.

(II) CEL does not collect customers’ private information.

(III) To protect the customer information in its PE system, CEL has taken numerous measures to strengthen system security, including:

For secure system login, CEL enforces a strict password policy and the Secure Sockets Layer (SSL) protocol to encrypt data during transmission. A rigorous privilege and access control framework appropriate for CEL’s businesses was planned as early as during the system design phase. The system also keeps access logs.

In terms of system deployment, CEL stores data on its intranet which, when combined with infrastructure-based access control to server IPs, dual firewalls, intrusion detection system, and other information security systems, can prevent data breaches.

VI. Data Security Management at Vendors

CEL’s vendors include providers of software and hardware systems and market data. CEL has taken different measures to ensure its vendors meet its data security requirements.

In selecting vendors, product and service performance and security are paramount considerations. Vendors that do not meet performance and security requirements will not be selected. When providing sample data to a vendor to clarify its needs, CEL would sign confidentiality agreement with the vendor to expressly prohibit it from divulging relevant data and information. This confidentiality agreement also provides the basis for legal action in case of data leak. For vendors admitted into CEL’s data operation system, another confidentiality agreement will be signed to require them maintain data and information security. At the same time, CEL has deployed a remote assistance monitoring system for vendors that provide technical support remotely, in order to keep a record of their activities.

In addition, the Data Security and Privacy Statement is in Chinese and English versions. If there is any inconsistency between the Chinese version and the English version, the Chinese version shall prevail.