# System and Organization Controls (SOC) 3 Report

## Report on the LINE messenger Service System Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

## For the Period January 1, 2018 through December 31, 2018

Ernst & Young Han Young
Taeyoung Bldg.,
111,Yeouigongwon-ro
Yeongdeungpo-gu, Seoul,
Seoul 07241 Korea

Tel: +82 2 3787 6600
Fax: +82 2 3787 4671
ey.com/kr

※ Ernst & Young Han Young is the global network firm of Ernst & Young

# Report of Independent Accountants

To the Management of LINE Corporation

*Scope:*

We have examined management's assertion, contained within the accompanying "Report on the LINE Messenger Service System Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy" (Assertion), that LINE Corporation (LINE)'s controls over the LINE Messenger Service System (System) were effective throughout the period 1 January 2018 to 31 December 2018, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, confidentiality, and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

*Management's Responsibilities*
LINE's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the LINE Messenger Service System and describing the boundaries of the System
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of the system
- identifying, designing, implementing, operating, and monitoring effective controls over the LINE Messenger Service System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

*Our Responsibilities*

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of LINE's relevant security, availability, processing integrity, confidentiality, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating LINE's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program**.**

*Inherent limitations:*
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all

misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve LINE's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

*Opinion:*

In our opinion, LINE's controls over the system were effective throughout the 1 January 2018 to 31 December 2018, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young Han Young

Ernst & Young Korea
30 June 2019

LINE

**Management's Report of its Assertions on the Effectiveness of Its Controls over the LINE Messenger Service System Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy**

June 30, 2019

We, as management of, LINE Corporation (LINE) are responsible for:

- Identifying the LINE Messenger Service System (System) and describing the boundaries of the System, which are presented in the accompanying Description of the LINE Messenger Service System
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 January 2018 to 31 December 2018, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, confidentiality and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

**LINE Corporation**

LINE

# Description of the LINE Messenger Service System

## LINE Overview

LINE Corporation (LINE) is an internet service company that provides the LINE Messenger Service. LINE generally provides its services through smart phone applications and PC programs. To provide the services, LINE uses and operates various IT systems, security devices and service management systems developed by LINE. This system description includes the following service:

- LINE Messenger – one to one chat, group chat, free calls (voice & video calls), image or video-sharing are offered as a main service on mobile devices and/or PCs.

The users of LINE Messenger Service (Users) have the responsibility to abide by the 'Customer's Obligation' section in the "Terms and Conditions of Use" in order to use LINE's service ("the service") securely. The users should identify and perform information security activities, such as changing passwords on a regular basis and not disclosing passwords to others, to protect personal information.

## Infrastructure

LINE operates diverse IT equipment to provide the service as necessary, and operates various IT management systems to manage the IT equipment. The infrastructure necessary to offer service has a physically limited access applied in an independent zone in the data center. LINE also uses automation tools and systems to monitor system components for security, availability, process integrity, confidentiality, and privacy protection of the services**.**

## Data

LINE manages data, which the users provide for the use of services, and information, which is processed for the service, to provide the service. Personal information protection is defined and identified in accordance with the relevant regulations and laws. Internal control processes are established for the collected and processed personal information and for the management systems that process the personal information. We also apply different levels of information security controls by the materiality of personal information. Users' messaging data is encrypted for data confidentiality. When the users withdraw LINE membership, the user's personal information is deleted within the period the user has agreed to and the regulations allow.

## People

IT System relative work, which develops and manages systems, is a major task in offering service. In order to offer stable service, developmental tasks, developing service-related programs, and operational tasks, managing relative system, are separated. The core tasks in supporting, maintenance, monitoring, and supervising services are as follows:

- Service planning – is responsible for planning, designing and operating of the LINE messenger service. Service planning/operating teams cooperate with a software development team, test team, information security team and other teams to make modifications in running services and develop a new service to provide more convenient and secure services.

- Development – develops IT systems for services and maintains software to continuously improve and provide the services and record change logs. Software development and testing is performed in separated environments from the production environment. Development teams continuously communicate the status and issues with relevant teams through a groupware system.

- Test – evaluates the quality of developed services, and makes requests for improvements. Prior to releasing

a developed program and system, a test team confirms that every planning and developing procedure was performed as expected. Also, prior to making the final decision to release a service, a test team reviews the test results of programs and systems to confirm whether data was processed without any problems.

- Infrastructure operation – implements datacenter infrastructures and operates networks, servers, and databases. Also, experts participate in the design, implementation, and operation stages for a provision of seamless service.

- Information security – operates an information security organization that is responsible for the personal information of the users and the stability of service. The information security team is responsible for information security risk management, manages a corporate information security policy and regulation, and audits the LINE's compliance status on a regular basis. Also, each department reviews authorities that need to conduct its task, and terminates unnecessary user access right on a regular basis.

- IT security – performs various activities to assure operational stability and sustainability of server systems and hardware that is required to provide services. Also, information security specialists monitor and examine the IT security status to protect services 24/7. The specialists analyze, prevent and respond to incidents via monitoring any event which may threaten the service.

**Availability**

The datacenter facility is equipped with fire detection and alarm systems and emergency evacuation system to limit loss due to fire. Heating, Ventilation and Air Conditioning (HVAC) systems are in place to protect the datacenter from environmental threats. Uninterruptible Power Supply (UPS) and generators are in place to provide temporary power in the event of a power outage.

An environmental inspection on power, HVAC, fire, and security systems in the datacenter is annually performed.

Service databases are backed up in real time through cluster duplication to continuously maintain copies of the databases. Also, the conditions of database clusters and servers are monitored 24/7 by a cluster monitoring system to ensure that the database clusters are properly duplicated.

LINE annually performs a database availability check including availability requirement analysis, plans and a simulation test for data restoration to prevent operation failure.

**Processing integrity**

LINE maintains system architecture and data architecture standards for system development and alteration.

The data stored in the databases are encrypted to restrict direct modification on the data. Also, access to the database servers are logged and monitored through an IT infrastructure management system.

LINE has established source code review procedures for system development and modification to verify completeness and security of system data.

Types and ranges of input data that can be entered into the service application are defined in the Application Programming Interface (API) reference. There is input validation check applied for the service application, and error response codes are defined in the API reference to return error messages when a data processing failure occurs.

**Confidentiality**

*Confidentiality Policy*

LINE has defined an information classification table containing confidential information classes and disclosure levels and provided to the employees via LINE's knowledge sharing portal.

*Use, Retention, Disposal of Confidential Information*

LINE has in place a policy that defines the definition of confidential information and the retention periods on each class of confidential information. Also, LINE regularly disposes of confidential information that exceeded its retention period.

A feature that restricts internal users to send emails to out of the corporate domain is enabled in the office email system to block emails containing confidential information from being forwarded externally. Additionally, based on the information contained in an email, a retention period for the email should be defined in the office email system. Emails that exceeded its retention period are automatically deleted by the system.

*Technical Security Measures*

Access to both development and production environments is logged and monitored through an IT infrastructure management system.

LINE has defined requirements for secure data communication. According to the requirements, an encryption method through a Secure Sockets Layer (SSL) certificate is used for data exchange in LINE’s internal system and service website.

Full disk encryption is applied on all employees' PCs to prevent confidential information from being disclosed.

*Outsourcing Management*

Outsourcing parties must sign an outsourcing agreement that includes a clause that restricts disclosure of LINE's confidential information. Also, LINE performs a third party information security risk assessment annually or at the point when a new third party contract is made.

LINE regularly reviews any changes in privacy regulations and LINE's confidentiality commitments. The changes identified are updated in the outsourcing contracts if necessary.

**Privacy**

*Notice and Communication of Commitments and System Requirements*

LINE specifies the overall internal policies and procedures for the protection of personal information, including the subject of personal information management, organization and responsibility, handling of personal information, collection, consignment, use, disposal and security in the internal Privacy Policy. Also, the choice, consent, use, retention, disposal, disclosure and security of personal information collection is specified in the Privacy Policy.

LINE annually reviews and updates the Privacy Policy when the service is changed. Any modification made is approved by the CPO. Also, LINE notifies the updated internal Privacy Policy to employees

through LINE's groupware.

LINE documents the current privacy practices and notifies to the users through the Privacy Policy and Terms and Conditions of Use. Also, when the Privacy Policy and the Terms and Conditions of Use are changed, the updates are available to the users through the website and/or the mobile application.

LINE's Privacy Policy and Terms and Conditions of Use are written in seven languages, including Japanese, Korean and English, and posted on the website and mobile application. The Terms and Conditions of Use is first written in Japanese, and the external Privacy Policy is provided to each relevant country that LINE provides service to.

LINE notifies users of the types and methods of collection of personal information about collected cookies or other similar tracking technology, as well as the contents that are restricted through the external Privacy Policy when the collection is refused.

*Choice and Consent*

LINE notifies the users through the Privacy Policy and Term and Conditions of Use posted on the website and the mobile application that the user can selectively consent to the collection, use, retention, disclosure, and disposal of personal information.

LINE communicates regarding selective collection of personal information and communicates the method of refusal when one does not consent to the collection of personal information necessary for the provision of services through the Privacy Policy and Term and Conditions of Use.

LINE collects the consent of the individual for the collection, use, retention, disposal and disclosure of personal information.

*Collection*

LINE notifies the purpose of collecting personal information through the Privacy Policy posted on the website and the mobile application, and reviews whether the personal information is collected only for the purpose specified by the internal audit.

LINE does not collect sensitive information from users.

LINE collects the consent of the individual for collecting personal information through cookies or other similar electronic devices for the purpose of collecting the service. Also, LINE informs that the use of service is restricted if the user refuses to consent.

*Use, Retention, and Disposal*

LINE uses the personal information only for the purposes for which it has been collected unless required by law. The purpose and use of the collected personal information are reviewed by the internal audit.

LINE stores personal information in a hashed value in the server.

LINE has in place a policy that defines the definition of personal information and the retention periods on each class of personal information. LINE regularly disposes of personal information that exceeded its retention period.

*Access*

LINE provides service users with the ability to access and modify their personal information. Access to their personal information is provided and authenticated on the mobile device through the service application.

When the user requests confirmation of their personal information through the customer service center, LINE provides the information through the identity verification process and does not change the personal information on its own.

LINE allows third parties to inquire only through the internal system without sharing the user's personal information externally.

*Disclosure and Notification*

It is stated in the external Privacy Policy that LINE only provides personal information to third parties only with user's consent unless required by law. Also, the user consents to provision of personal information prior to registration of service.

LINE maintains a record of personal information inquiries and monitors the history of internal data loss prevention solutions and service management system access in order to confirm personal information infringement and unauthorized transmission. Also, LINE uses Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor critical security events that could adversely affect the service. If security events are detected, LINE initiates corrective actions for the events according to a security event response policy which defines security event procedures, severity of security events, and security event response personnel. Security event monitoring results are reported to and reviewed by relevant personnel.

LINE has a security incident response policy which defines types of incidents, personnel and procedures for security incident response. If security incidents are identified. Also, LINE initiates corrective actions for the incidents according to the security incident policy.

Employees from the third parties are obligated to sign a Non-disclosure agreement and the incident reporting procedure is present to the third party companies. LINE performs an information security risk assessment of the third parties annually or at the point when a new third party contract is made.

LINE describes accident management and violation management information in incident management regulations and security incident response guidelines. In addition, monitoring is conducted to deal with accidents for its resolutions and notify the information authorities and related organizations to establish appropriate measures to prevent further recurrence.

*Quality*

LINE notifies service users through the Terms and Conditions of Use on the website and mobile application that the service user is responsible for providing accurate and complete personal information to LINE and, if necessary, for informing LINE that the information needs to be modified.

LINE provides services on the mobile devices based on the mobile phone number for the up-to-date of the service user's personal information. When the subscription and re-authentication are necessary, the mobile phone authentication process is performed, and then the subscriber is re-authenticated.

When a service change occurs, LINE reviews the necessary justification for the collection of service user information so that appropriate personal information is collected and maintained. Also, LINE reviews the collected personal information and its appropriateness through the internal audit prior to a report presented to the CEO.

*Monitoring and Enforcement*

LINE informs service users on how to contact the helpdesk for inquiries, complaints and disputes. Also, LINE provides an inquiry function on the website and mobile application for service users to communicate inquiries and complaints.

LINE receives inquiries and service user complaints on the bulletin board of LINE's official website and confirms the inquiries and user complaints through customer information system. If necessary, the relevant personnel in charge reviews and responds to users through the email for resolution.

The Privacy Policy is amended in accordance with change of law that is constantly monitored. The policies are reviewed in the management meetings and approved by the managements and related managers.

LINE monitors the compliance requirements and reviews in accordance with the Privacy Policy through an internal audit, and its audit result is reported to the management. Also, if needed, corrective and disciplinary measures are taken.