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, 2022 through December 31, 2022

Ernst & Young Han Young
Taeyoung Bldg.,
111,Yeouigongwon-ro
Yeongdeungpo-gu, Seoul,
Seoul 07241 Korea
※ Ernst & Young Han Young is the global network firm of Ernst & Young

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

Independent Service Auditor's Report

To the Management of LINE Corporation

Scope:

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over the LINE Messenger Service System Based on the Trust Service Criteria for 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 January 1, 2022 to December 31, 2022, 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 ("applicable trust services criteria") set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy(With Revised Points of Focus – 2022)*.

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 our 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 our 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 January 1, 2022 to December 31, 2022, 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
July 31, 2023

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

July 31, 2023

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 Attachment A
- 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, which are presented in Attachment B
- 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 2022 to 31 December 2022, 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(With Revised Points of Focus – 2022)*.

Very truly yours,

LINE Corporation

(Signature)

Attachment A – Description of 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 Service – 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.

Scope

The scope of this report is only limited to LINE Messenger Service and does not include any other services.

Infrastructure

The company has infrastructure equipment in data centers, related to operating systems, networks, and security facilities of major servers, to provide services. The company owns two data centers("DC"), that one is Tokyo Toyosu DC, which functions as a main DC, and the other is Osaka DC, which functions as a backup DC for emergencies such as disasters. The Company locates its each infrastructure in physically separated, independent areas of DC and applies separate physical access controls. The IT infrastructures, including server's operating system and databases, network, IT security devices and logs, are managed by the Company.

Software

The company is developing/operating applications that manage internal information, customer information, technology information, service information, and IT system software (operating systems, middleware, utilities) supporting them to provide services.

People

The team responsible for Line Messenger services consists of a development team that develops, maintains, and manages applications, a support team responsible for operational support, and a security team responsible for security, and each team includes the following groups:

Development Team

- Line Service Development: Application development and quality improvement planning
- Line Communication Platform Development: Improvement of application communication function and platform development/ function
- Development of Line Content Services Platform: Maximization of content traffic within applications and improvement of service platforms
- Mobile Experience Development: Development improvement activities to optimize mobile experience

Support Team

- Customer Care: Line CS operation planning, CS tool, channel, process improvement

Security Team

- Security Center: Company-wide infrastructure and service security management and regular checks, security management system operations and maintenance to ensure service continuity, prevention and after-care of security-related incidents, game application security check, security software development, security incident correspondence

Process

The Company has established an information security policy and service operation manual to assure security, availability, process integrity, confidentiality and privacy protection of IT systems. The policy and manual are available in the Company's groupware. Internal/external audits and related training are held to strengthen employees' awareness of information security.

The policy and manual cover the following essential security areas:

- Physical access control
- Logical access control
- Availability
- Change management
- Data communication
- Risk assessment
- Data retention
- Vendor management

Data

Users' data is protected in accordance with the related laws and regulations, service use agreement and the Company's information protection regulation.

Attachment B – Principal Service Commitments and System Requirements

LINE Corporation (“LINE”) designs its processes and procedures to meet its objectives for the LINE System. Those objectives are based on the service commitments that LINE makes to user entities (customers), the LINE and regulations that govern the provision of the LINE System, and the financial, operational and compliance requirements that LINE has established for the services. The LINE services are subject to relevant regulations, as well as state privacy security.

LINE and regulations in the jurisdictions in which LINE operates. Security, Availability and Confidentiality, Privacy commitments to customers are documented and communicated in customer agreements, as well as in the description of the service offering provided on the LINE website. Security, Availability and Confidentiality commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the LINE System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.

- Security and confidentiality principles inherent to the fundamental design of the LINE System are designed to safeguard data from within and outside of the boundaries of environments which store a customer’s content to meet the service commitments.

- Availability principles inherent to the fundamental design of the LINE System are designed to replicate critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.

- Integrity principles inherent to the fundamental design of the LINE System are designed to perform complete, accurate and timely processing of data through the establishment of secure system development and operating environment.

- Privacy principles inherent to the fundamental design of the LINE System are designed to protect customers' rights through relevant policies and procedures and by notifying customers of updated Privacy policies in advance.

LINE establishes operational requirements that support the achievement of security, availability and confidentiality, privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in LINE's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

Information security policies include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the LINE Messenger service.

LINE