LINE WORKS

LINE WORKS Corporation

System and Organization Controls 3 Report

On Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy of LINE WORKS Service

January 1, 2023 – December 31, 2023

Table of contents

Deloitte Anjin LLC
9F., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
07326, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

Section I: Independent Service Auditor's Report

English Translation of Independent Auditors' Report Originally Issued in Korean on April 26, 2024

LINE WORKS Corporation

1-5-8 Jingumae, Shibuya-ku, Tokyo, 150-0001

Jingumae Tower Building 11F

Scope

We have examined LINE WORKS Corporation ('LINE WORKS', or the 'service organization')'s accompanying assertion titled "Section II: Management's Assertion" ('assertion') that the controls within the LINE WORKS Service system ('system') were effective and NAVER CLOUD Corporation ('NAVER CLOUD', or the 'subservice organization')'s accompanying assertion titled "Section II: Management's Assertion(Subservice Organization)" ('Subservice Organization's assertion') that the controls designed by LINE WORKS and operated by NAVER CLOUD were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ('applicable trust services criteria') set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in* AICPA, *Trust Services Criteria*.

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LINE WORKS, to achieve LINE WORKS's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the system presents the complementary user entity controls assumed in the design of LINE WORKS's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

LINE WORKS uses NAVER CLOUD to provide system development and operations, IT infrastructure operation service related to LINE WORKS service. The service provided by NAVER CLOUD is part of LINE WORKS service and the controls designed by LINE WORKS and operated by the subservice organization that are necessary for LINE WORKS to achieve its service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

LINE WORKS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved. LINE WORKS has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LINE WORKS is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Subservice Organization's Responsibilities

NAVER CLOUD has provided the accompanying assertion about the effectiveness of the controls designed by LINE WORKS and operated by NAVER CLOUD. When preparing its assertion, NAVER CLOUD is responsible and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls designed by LINE WORKS, which enable LINE WORKS to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve LINE WORKS's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve LINE WORKS's commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA and the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior. We applied the statements on quality control standards established by the AICPA and International Standards on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* and accordingly maintain a comprehensive system of quality control.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within LINE WORKS's LINE WORKS Service system were effective throughout the period January 1, 2023 to December 31, 2023, if complementary user entity controls contemplated in the design of the Service Organization's controls operated effectively, to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte Anjin LLC.

April 26, 2024
Seoul, Republic of Korea

LINE WORKS

Section II: Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within LINE WORKS Corporation ('LINE WORKS' or the 'service organization')'s LINE WORKS Service system ('system') throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that LINE WORKS's service commitments and system were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.* Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved applicable trust services criteria. LINE WORKS's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

LINE WORKS uses NAVER CLOUD Corporation ('NAVER CLOUD') to provide system development and operations, IT infrastructure operation service related to LINE WORKS service. The service provided by NAVER CLOUD is part of LINE WORKS service and the controls designed by LINE WORKS and operated by the subservice organization that are necessary for LINE WORKS to achieve its service commitments and system requirements based on the applicable trust services criteria.

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LINE WORKS, to achieve LINE WORKS's service commitments and system requirements related to system based on the applicable trust services criteria. The accompanying Description of the Boundaries of the system presents the complementary user entity controls assumed in the design of LINE WORKS's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls of LINE WORKS and the controls designed by LINE WORKS and operated by NAVER CLOUD within the system were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved based on the applicable trust services criteria.

NAVER Cloud

Section II: Management's Assertion (Subservice Organization)

NAVER CLOUD Corporation ('NAVER CLOUD' or 'we') provides system development and operation, IT infrastructure operation service related to LINE WORKS service to LINE WORKS Corporation ('LINE WORKS'). The service provided by NAVER CLOUD is part of LINE WORKS service. We are responsible for the operating effectiveness of controls designed by LINE WORKS within LINE WORKS Service system ('system') throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that LINE WORKS's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.*

We assert that the controls designed by LINE WORKS and operated by NAVER CLOUD were effective throughout the period January 1, 2023 to December 31, 2023 based on the applicable trust services criteria.

Section III: Description of the Boundaries of LINE WORKS Service System

1. Overview of Operations

Company Introduction

LINE WORKS Corporation ('LINE WORKS' or the 'Company') was established to provide WORKS MOBILE service targeting Japanese market in June 2015. Starting service provision from January 2016, the Company has set up the business mission "To every personnel working in 47 Dodobu-Hyun and enjoy working" to improve the quality of business operation and communication at work.

The key status of LINE WORKS Corporation is as follows.

COMPANY	LINE WORKS Corporation
FOUNDED	June 3, 2015
CAPITAL	5,520 Million JPY
C.E.O	Masuda Ryuichi
HEADQUARTERS	Jingumae Tower Building 11F, 1-5-8 Jingumae, Shibuya-ku, Tokyo, 150-0001
Reported Telecommunication Business Operator	A-27-14402

LINE WORKS service is a cloud (SaaS) based communication/collaboration service that consists of various features such as business messenger, voice/video call, mail, calendar, bulletin board, address book, cloud storage, monitoring, and so on. LINE WORKS service is accessible from various types of devices like PCs, smartphones, and tablet PCs and enables efficient communication between companies and organizations regardless of location. In addition, LINE WORKS service provides administrators with functions such as member management, security configuration, service statistics, auditing, and monitoring.

Service

LINE WORKS provides services through PC web and mobile for the users' convenience. To deliver such services, LINE WORKS uses various IT systems, security devices, and internally developed service management systems. The system description covers LINE WORKS.

- LINE WORKS – Provides cooperation/communication services such as enterprise-wide instant messenger, e-mail, drive, calendar and contact list for the employees within corporates. Also provides administrative services such as security configuration, service statistics, auditing functions, and e-mail monitoring systems for the management personnel.

User entities of the service are responsible to adhere to the user's obligation in the Terms of Service in order to securely and properly use the LINE WORKS services. User entities should also understand and perform the activities to protect personal information by themselves, including changing passwords on a regular basis and not disclosing passwords to others.

Report Scope Boundary

The objective and scope of this description is limited to the LINE WORKS service and does not include any description related to other services.

2. Service Components

The Company's service components to provide the service consist of infrastructure, software, data, and relevant operating procedures and human resources.

Infrastructure

The Company implements and operates infrastructures such as servers, network, and security systems, which are configured in a separate network for each, to provide the service. The Company restricts unauthorized access (physical / logical) using access controls to infrastructure, and monitors the log of abnormal activities on a regular basis.

The Company also uses automatic vulnerability scanning tools to consistently detect and improve security vulnerabilities which may occur within the infrastructure, and takes remedial actions for identified vulnerabilities. The data center, where the infrastructures are located, is equipped with thermo-hygrostats, Uninterruptible Power Supplies (UPS), water leakage detectors, fire detectors, extinguishers, and so on to get prepared for disasters such as fire, earthquake, flood, and so on.

Software

Relevant functions of the Company for each service are responsible for developing and operating applications. When an application needs additional developments or upgrades to improve service quality provided to users, to remediate failures or to enhance system performance, the security requirements are defined by an agreement between the Service Planning Department and the Development Department and then shared with stakeholders via intranet.

Changes to an application requires preapproval by the person in charge, and the QA (Quality Assurance) team reviews and deploys to the production environment through the automated system to minimize the failures that may arise from the change. When significant changes related to the user's personal information processing are involved, a privacy impact assessment is conducted and remedial actions are taken when deemed necessary.

Human Resources

To ensure service stability, the Company defines and designates such roles as information security and personal information managers, service planners, developers, infrastructure operators, CS (Customer Satisfaction) personnel, and so on. Annual information security and personal information protection trainings are provided to raise the awareness level of information security of the company personnel.

Immediately after being hired or terminated, an employee is informed of his or her confidentiality obligations, and required to sign and submit a security pledge. All employees sign and submit a security pledge every year.

Procedures

The Company established information security regulations such as policies, standards and guidelines to comply with the security, availability, process integrity, confidentiality, and privacy principles. Company policies are periodically reviewed, and revised when deemed necessary, to reflect developments of relevant laws and regulations. Revisions require approval by an appropriate level of management and are announced to all employees through intranet.

Company policies related to protection of user's personal information and privacy are disclosed in the Privacy Policy on the Company's website so that users can refer to at any time.

Data

Important data including user's personal information are protected in accordance with the requirements by relevant laws and regulations such as the Act on Promotion of Information and Communications Network Utilization and information Protection, etc., the Personal Information Protection Act, and so on and the procedures specified in the Terms of Service and security policies of the Company. Such data are managed to be processed only by a limited number of personnel performing relevant duties.

The Company also implements technical measures such as access control, encryption and logging to protect important data.

Complementary User Entity Controls

The complementary user entity controls which are assumed in the design of service organization's controls are as follows. User entities should ensure that adequate control activities are in place in the following areas:

Complementary User Entity Controls
CUEC-01: The user entity is responsible for obtaining a pledge including confidentiality obligation at the time of employment or retirement.
CUEC-02: The user entity is responsible for carrying out periodic awareness programs to prevent unauthorized access to the system by overriding internal controls.
CUEC-03: The user entity is responsible for getting IT assets such as business terminals when an employee retires.
CUEC-04: The user entity is responsible for deactivating or deleting a user account in case of role changes of the employ5e such as internal transfer and resigning.
CUEC-05: The user entity is responsible for executing contracts or agreements which contain clauses related to information security when entrusting certain duties related to use the service to a third party.
CUEC-06: The user entity is responsible for periodically checking whether the information security requirements specified in the contracts, agreements, etc. are being complied with by the third party vendor entrusted with certain duties related to use the service.
CUEC-07: At the termination of the service with the third party vendor, the user entity is responsible for checking whether the third party vendor retains important information, such as personal information, and making sure get such information returned.
CUEC-08: The user entity is responsible for restricting access to its facilities to prevent unauthorized access to business terminals that can access to the service.
CUEC-09: The user entity is responsible for establishing and implementing controls over carrying-in and out of mobile devices and storage media to prevent leakage of important information from protected areas such as offices.
CUEC-10: When creating a user account, the user entity is responsible for assigning a unique ID for each person and not using a shared account.
CUEC-11: The user entity is responsible for restricting use of easily predictable IDs when creating user accounts.
CUEC-12: The user entity is responsible for granting user accounts to a minimum number of individuals upon business needs.
CUEC-13: The user entity is responsible for taking corrective actions against abnormal events such as abusive or misuse of the service account.
CUEC-14: The user entity is responsible for establishing appropriate controls on user accounts, such as limiting the number of login attempt failures.
CUEC-15: The user entity is responsible for periodically reviewing the appropriateness of the accounts assigned to company personnel and deleting any unnecessary privileges identified.

Complementary User Entity Controls
CUEC-16: The user entity is responsible for ensuring that user accounts and passwords are not leaked.
CUEC-17: The user entity is responsible for establishing and implementing measures to secure user passwords such as complexity standards, maximum usage period, and so on.
CUEC-18: The user entity is responsible for installing security programs such as vaccines in business terminals and maintaining the latest patches to minimize service failures through malware infection.
CUEC-19: The user entity is responsible for establishing policies over backup frequency and retention period of important information to ensure service availability and evaluating whether related policies of the service organization conform to its policies.
CUEC-20: The user entity is responsible for notifying the service organization of any problems with or failure of the service.
CUEC-21: The user entity is responsible for notifying the service organization of any issues of system failures regarding the service.

Section IV: Principal Service Commitments and System Requirements

The Company has made service commitments to the user entities and established system requirements for the LINE WORKS service. Some of these commitments are related to the performance of the service and applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements are achieved.

Service commitments to users are documented in such forms as Terms of Service, Privacy Policy, Youth Protection Policy, Spam Mail Policy, Search Result Collection Policy, and so on, and communicated to users through the Customer Center. The Company also provides the description of the service offering through online. Service commitments include, but are not limited to, the following:

- Security: The Company made commitments related to protecting user data from unauthorized access and use. These commitments are addressed through measures including data encryption, authentication mechanisms, access controls, physical security, and other relevant security controls.
- Availability: The Company made commitments related to keeping service continuity without disruptions. These commitments are addressed through measures including performance monitoring, regular data backups and recovery controls.
- Processing Integrity: The Company made commitments related to processing user data completely, accurately and timely. These commitments are addressed through measures including secured system development and production environments, approval of system changes and other relevant controls.
- Confidentiality: The Company made commitments related to maintaining the confidentiality of user data. These are addressed through security controls including encryption mechanisms in transferring and storing users' important data.
- Privacy: The Company made commitments related to protecting personal information. These commitments are addressed through controls relating to collecting, storing, using, entrusting, and disposing of personal information in accordance with relevant laws and regulations and its Privacy Policy.

The Company has established operational requirements that support the achievement of service commitments, requirements by relevant laws and regulations, and other system requirements. Such requirements are specified in the Company's policies and procedures and system design documentation and communicated to users through the service website.

Information security policies of the Company define an organization-wide approach to how systems and data are protected. These include policies over service design and development, system operation, internal business system and network management, and hiring and training of executives and employees. In addition to these policies, standard operating procedures have been documented on how to carry out manual and automated processes specifically required in the operation and development of the LINE WORKS service.