



**WORKS MOBILE**

# **WORKS MOBILE Corporation**

## **System and Organization Controls 3 Report**

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

January 1, 2020 – December 31, 2020

# Table of contents

- Section I: Independent Service Auditor’s Report..... 2**
  - Scope ..... 2
  - Service Organization’s Responsibilities ..... 2
  - Service Auditor’s Responsibilities ..... 2
  - Inherent limitations ..... 3
  - Opinion..... 3
  
- Section II: Management’s Assertion ..... 4**
  - WORKS MOBILE Corporation’s Management Assertion ..... 4
  
- Section III: Description of the Boundaries of NAVER WORKS Service System ..... 5**
  - 1. Overview of Operations ..... 5
    - Company Introduction ..... 5
    - Service ..... 5
    - Report Scope Boundary ..... 5
  - 2. Service Components..... 6
    - Infrastructure ..... 6
    - Software ..... 6
    - Human Resources..... 6
    - Data..... 6
    - Procedures..... 7
  
- Section IV: Principal Service Commitments and System Requirements ..... 8**

## Section I: Independent Service Auditor's Report

### **WORKS MOBILE Corporation**

10F KRAFTON Tower, 117, Bundangnaegok-ro,  
Bundang-gu, Seongnam-si,  
Gyeonggi-do, Korea

### **Scope**

We have examined WORKS MOBILE Corporation ("WORKS MOBILE", the "service organization", or the "Company")'s accompanying assertion titled "Section II: Management's Assertion" ("assertion") that the controls within NAVER WORKS Service system ("system") were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that WORKS MOBILE'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* (AICPA, *Trust Services Criteria*).

### **Service Organization's Responsibilities**

WORKS MOBILE 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 WORKS MOBILE's service commitments and system requirements were achieved. WORKS MOBILE has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, WORKS MOBILE 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.

### **Service Auditor's Responsibilities**

Our responsibility is to express an opinion, based on our examination, on whether 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. 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.

Our examination included:

- 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 WORKS MOBILE'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 WORKS MOBILE'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.

## 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 WORKS MOBILE's NAVER WORKS Service system were effective throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that WORKS MOBILE'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 23, 2021  
Seoul, Republic of Korea



WORKS MOBILE

## Section II: Management's Assertion

### WORKS MOBILE Corporation's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within WORKS MOBILE Corporation ("WORKS MOBILE")'s NAVER WORKS Service system ("system") throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that WORKS MOBILE's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in "Section III: Description of the Boundaries of NAVER WORKS Service System" ("description").

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that WORKS MOBILE'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* (AICPA, *Trust Services Criteria*). WORKS MOBILE'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.

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 within the system were effective throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that WORKS MOBILE's service commitments and system requirements were achieved based on the applicable trust services criteria.

# Section III: Description of the Boundaries of NAVER WORKS Service System

## 1. Overview of Operations

### Company Introduction

WORKS MOBILE Corporation (“WORKS MOBILE” or the “Company”) started providing the “NAVER WORKS” service in 2012, based on the personal NAVER mail domain service that was launched in 2011. In April 2015, the Company was established through spin-off from NAVER Corporation to enter the global enterprise service market and established WORKS MOBILE Japan Corporation targeting Japanese market in June 2015.

NAVER WORKS is the Company's core service to provide the collaboration / communication for the enterprise, which consists of various features such as enterprise-wide instant messenger, voice/video call, e-mail, drive, calendar, home (bulletin board), survey, address book, monitoring, and so on. Customers can build a Smart Office environment by using the Company's cloud-based services. The NAVER WORKS service is accessible from various types of devices like PCs, smartphones, and tablet PCs. In addition to the collaboration / communication services for the employees within an enterprise, the service provides administrative functions such as security configuration, service statistics, auditing functions, and e-mail monitoring systems for managers.

### Service

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

- NAVER 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.

Users 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 WORKS MOBILE services. Users 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 scope of this Description is limited to the NAVER WORKS service. This Description does not include details 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.

### 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.

## 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.



## Section IV: Principal Service Commitments and System Requirements

The Company has made service commitments to the users and established system requirements for the NAVER 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, 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 NAVER WORKS service.