NAVER Corporation

System and Organization Controls 3 Report

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

January 1, 2018 – December 31, 2018

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

NAVER Corporation

NAVER Green Factory, 6, Buljeong-ro,
Bundang-gu, Seongnam-si,
Gyeonggi-do, Korea

Scope

We have examined NAVER Corporation’s (“Service Organization” or “NAVER”) accompanying assertion titled "Section II: Assertion of NAVER Management" (“assertion”) that the controls within BAND Service (“system”) were effective throughout the period January 1, 2018, to December 31, 2018, to provide reasonable assurance that NAVER’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

NAVER 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 NAVER’s service commitments and system requirements were achieved. NAVER has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NAVER 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 NAVER’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 NAVER'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 NAVER's BAND systems were effective throughout the period January 1, 2018, to December 31, 2018, to provide reasonable assurance that NAVER'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 12, 2019
Seoul, Republic of Korea

Section II: Management's Assertion

NAVER's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within NAVER Corporation's ("NAVER") BAND system ("system") throughout the period January 1, 2018, to December 31, 2018, to provide reasonable assurance that NAVER'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 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, 2018, to December 31, 2018, to provide reasonable assurance that NAVER'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*). NAVER'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, 2018, to December 31, 2018, to provide reasonable assurance that NAVER's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section III: Description of the Boundaries of BAND System

1. Overview of Operations

Company Introduction

NAVER Corporation(referred to as 'NAVER' or 'the Company' hereinafter) was incorporated on June 2, 1999 and the Company listed its shares on the KOSDAQ on October 29, 2002, but later transferred its shares to the KOSPI on November 28, 2008.

Based on the search engine technology, a large database processing capability, diverse of contents, NAVER retains 42 million subscribers with approximately 30 million users on average accessing its services via mobile channels daily. This makes the Company the top web portal service in Korea.

Its key services include an integrated search service that provides various information such as news, professional data, images and others, in addition to the Personal Web Environment[1] service including the mail, the cloud and other services. NAVER also provides user-generated content (UGC) platforms including the Knowledge iN, blogs and cafes, as well as contents services such as webtoons, web novels, music and videos, and shopping services including the Shopping Window and Smart Store and many others.

The Company expanded its scope of business to provide easy payment and integrated payment services in June 2015, by launching the NAVER Pay, a service that enables the users to shop at affiliated online stores, pay for digital music, movies, e-books offered by NAVER and to save and transfer credits or money using NAVER ID. The service is generating a synergistic effect through its connection with other existing services. In addition, the Company is expanding its service to the offline sector by supporting Zero Pay which lowers the settlement fee for the small businesses, and raises benefits for consumers. With over 240,000 affiliated online stores as of 2018, NAVER Pay is exhibiting a trend of continued growth.

NAVER is executing Flower Project, a program helping individuals, small businesses and content creators find new opportunities and achieve sustainable growth. In addition, the Company also operates platforms that support content creators, such as the Grafolio. Moreover, NAVER is steadily growing in the global market by offering services such as Line, SNOW, V Live, NAVER Webtoon, BAND and others, which can reach and connect users from all around the world online.

More recently, the Company is making an effort to become a technology platform provider, emphasizing services such as 'Clova', an artificial intelligence platform, Ambient Intelligence based wearable 'phone for KIDS(AKI)', autonomous car technology, robotics (M1), translation application 'Papago', and web browser 'Whale'.

[1] Personal Web Environment (PWE) service: PWE is a NAVER service that allows users to configure and administrate their personal data in the way they want. This includes platforms such as e-mail, calendar, memo, address book, and the like.

Service

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

- BAND – A representative group SNS service that provides invitation-based community service between members. The service allows users to set up a BAND of their passion and share their interest with message board, photos, schedules, and instant messages.

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 NAVER 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 Description is limited to the BAND service. This Description does not include details related to other services.

2. Service Components

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

Infrastructure

The Company implements and operates infrastructures such as server, network, and security systems, which are located at a separate data center for each, to provide the service. The Company restricts unauthorized access (physical / logical) using access controls to infrastructures, 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 in infrastructure, and take remedial actions for identified vulnerabilities. The data center, where the infrastructures are located, is equipped with thermo-hygrostat, UPS, water leakage detector, fire detector, extinguisher, and other security facilities 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 user entities, to remediate failures or to enhance performance, the security requirements are defined by an agreement between the Service Planning Department and the Development Department and shared with stakeholders via intranet.

Changes to an application requires preapproval by the person in charge, and the QA 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 analysis is conducted to evaluate its impact 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, and CS (Customer Satisfaction) personnel. Annual information security and personal information protection trainings are provided to raise the awareness level of information security of the individuals.

Upon an employee is hired or terminated, he or she is informed about the confidentiality obligations, and required to sign off on a security pledge immediately after his or her employment and termination.

Data

Important data including user's personal information are protected in accordance with relevant laws and regulations such as the Act on Promotion of Information and Communications Network Utilization and information Protection, etc. (the "Act on Information and Communications Network" hereinafter), the Personal Information Protection Act, 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 applies 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. The regulations are monitored and revised periodically to reflect developments of relevant laws. Revisions require approval by a responsible person and are announced to all employees through intranet.

Regulations related to protection of user's personal information and privacy are disclosed as 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

NAVER makes service commitments to its customers and has established system requirements as part of the BAND system. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. NAVER 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 NAVER's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in Terms of Service, Privacy Policy, Youth Protection Policy, Spam Mail Policy, Search Result Collection Policy, and Customer Center as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: NAVER made commitments related to protecting customer 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: NAVER 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: NAVER made commitments related to processing customer actions completely, accurately and timely. These commitments are addressed through measures including secured system development and production environments, management approval of system changes and other relevant controls.
- Confidentiality: NAVER made commitments related to maintaining the confidentiality of customers' data. These are addressed through measures including encryption mechanisms and other security controls to transfer and store users' important data.
- Privacy: NAVER 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.

NAVER establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in NAVER'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. These 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 BAND service.