NAVER Cloud

NAVER CLOUD Corporation

System and Organization Controls 3 Report

On Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy of NAVER Cloud Platform Service for Private Sector Organizations

January 1, 2021 – December 31, 2021

Table of contents

Deloitte.

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 CLOUD Corporation
11F KRAFTON Tower, 117, Bundangnaegok-ro,
Bundang-gu, Seongnam-si,
Gyeonggi-do, Korea

Scope

We have examined NAVER CLOUD Corporation ('NAVER CLOUD', or the 'service organization')'s accompanying assertion titled "Section II: Management's Assertion" ('assertion') that the controls within the NAVER Cloud Platform Service for Private Sector Organizations system ('system') were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that NAVER CLOUD'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 CLOUD 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 CLOUD's service commitments and system requirements were achieved. NAVER CLOUD has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NAVER CLOUD 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 (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.

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 CLOUD'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 CLOUD'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 CLOUD's NAVER Cloud Platform Service for Private Sector Organizations system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that NAVER CLOUD'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.

March 25, 2022
Seoul, Republic of Korea

Section II: Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within NAVER CLOUD Corporation ('NAVER CLOUD')'s NAVER Cloud Platform Service for Private Sector Organizations system ('system') throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that NAVER CLOUD'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, 2021 to December 31, 2021, to provide reasonable assurance that NAVER CLOUD'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 CLOUD'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, 2021 to December 31, 2021, to provide reasonable assurance that NAVER CLOUD's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section III: Description of the Boundaries of NAVER Cloud Platform Service for Private Sector Organizations System

1. Overview of Operations

Company Introduction

NAVER CLOUD Corporation ('NAVER CLOUD', the 'Company', or the 'service organization') was incorporated on May 1, 2009 as a specialized IT service company being named as NHN BUSINESS PLATFORM Corporation through business split from NAVER Corporation. The Company changed its name to NAVER BUSINESS PLATFORM Corporation on August 1, 2014, and then to the current name effective October 15, 2020.

The Company operates and supports overall IT infrastructures including infrastructure, enterprise information, Ncloud, and relevant services for NAVER Corporation, NAVER FINANCIAL Corporation, WORKS MOBILE Corporation, SNOW Corporation, NAVER Webtoon Corporation, LINE Corporation, and other NAVER affiliates. Leveraging such experiences, NAVER CLOUD has acquired the systems for operation, development and management of cloud business to provide the NAVER Cloud Platform service for customers. The major services provided by the Company are as follows:

- IT Infrastructure Service
  The Company provides a stable and efficient IT environment which belongs to an IaaS (Infrastructure as a Service) area so that a customer's IT infrastructure such as Internet Data Center (IDC), networks, storages, databases (DB), and so on can be operated 24/7 without interruption. The environment is also provided by using the broadband network and is supported by professional technicians. Furthermore, the Company offers high quality consulting services on overall infrastructure design/implementation/operation, reflecting customer requirements.
- Data Center Operation Service
  The IDC service is a key competitive advantage of infrastructure for the NAVER Cloud Platform service launched in 2017 by making the Company respond with flexibility not only to around 3,900 services and products provided by NAVER and NAVER affiliates but also rapidly growing data demands due to advanced technology, such as AI, self-driving cars, and so on. More specifically, the Company provides such services as Co-location, server hosting, NAS (Network Attach Storage) / SAN (Storage Area Network), Owner-based File System (OwFS) services, and backup/recovery.
- Security Service
  The Company provides seamless security services using tens of solutions and thousands of robust detection/blocking policies in addition to CERT (Computer Emergency Response Team) and security monitoring services, to provide safe and reliable services. Further, the Company proposes optimal security designs customized for each service and has know-how to prevent and respond to globally evolving intelligent attacks such as phishing, ransomware, and so on.
- Enterprise Information Service
  With the one-stop enterprise system, the Company provides optimized business tools to maximize productivity of customers. Especially, the global office care program provides a stable information system in a same IT environment for any affiliated company's office around the world.

- Ncloud Service
  With the cloud service for NAVER affiliates using its integrated knowhow to operate large scale IT infrastructure, the Company adaptably supplies IT infrastructures anytime, at any place and as much as needed in a short period of time. The experience acquired through running Ncloud on numerous services has become a foundation for the NAVER Cloud Platform.
- NAVER Cloud Platform
  The Company provides IaaS, PaaS, and SaaS to customers, leveraging its world-class infrastructure technology and service operation capacity that has led NAVER to become the largest portal site in Korea and LINE messenger to be used in more than 200 countries around the world.

With the experience built up through operating IT infrastructure since the start of NAVER service in 1999 and the continuous challenges to lead the rapidly changing industry, the Company has accumulated IT expertise that is optimized for a wide variety of service needs. And through these efforts, 'GAK', its own data center established in Chuncheon of Gangwon province in June 2013, received the LEED (Leadership in Energy and Environmental Design) Platinum certification, the highest level for the first time among data centers in the world. Data center 'GAK' maintains stable services with 24-hour integrated monitoring and real-time management.

Since 2017, the NAVER Cloud Platform service has been providing various cloud services such as Compute, Storage, Networking, Database, Management, Security, Artificial Intelligence Service (AI Service), Application Service, Analytics, Global, Business Application, Development Tools (Dev Tools), and so on leveraging its cloud technology and service experiences accumulated through services provided to NAVER and LINE services. The Company was certified with CSA (Cloud Security Alliance), STAR (Security, Trust Assurance and Risk), which is an international agency certification for cloud service, for the first time in Korea, and is qualified to provide services to public sector entities in Korea by acquiring the CSAP (Cloud Security Assurance Program) certification, which is a local certification for cloud service. The Company has infrastructure bases in 10 global major locations and networks around the world and is expanding its cloud service regions.

Service

NAVER CLOUD provides services through PC web and mobile for the users convenience. To deliver such services, NAVER CLOUD uses various IT systems, security devices, and internally developed service management systems. The system description covers NAVER Cloud Platform Service for Private Sector Organizations service.

NAVER Cloud Platform Service for Private Sector Organizations – Provides stable IT service infrastructure, along with IT Platform, enterprise information service, and cloud services based upon the optimal conditions for a cloud service such as professional technicians, security technology, and continuous customer support service.

User entities are responsible to adhere to the user's obligation in the Terms of Service in order to securely and properly use the NAVER CLOUD 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 NAVER Cloud Platform Service for Private Sector Organizations provided by the data center in Korea, Western United States (San hose), Germany (Frankfurt), Japan (Tokyo), Singapore and Hongkong, and does not include descriptions related to other services.

Product Category	NAVER Cloud Platform Service for Private Sector Organizations
Compute	HDD Server SSD Server GPU Server CPU Intensive Virtual Dedicated Server Bare Metal Server Auto Scaling Application Server Launcher Cloud Functions HPC (High Performance Computing) Container Registry Kubernetes Service
Storage	Object Storage Archive Storage Block Storage NAS Backup
Networking	Virtual Private Cloud (VPC) Load Balancer DNS Global DNS CDN+ Global CDN IPsec VPN NAT Gateway Global Route Manager
Database	Cloud DB for MySQL Cloud DB for Redis Cloud DB for MSSQL MSSQL MySQL CUBRID Redis PostgreSQL MariaDB Tibero
Security	Basic Security Secure Zone (Firewall) App Safer Site Safer File Safer App Security Checker Web Security Checker System Security Checker SSL VPN Security Monitoring Compliance Guide

Product Category	NAVER Cloud Platform Service for Private Sector Organizations
	Private CA Key Management Service Certificate Manager Webshell Behavior Detector
AI Service	CLOVA Speech Recognition (CSR) CLOVA Speech Synthesis (CSS) CLOVA Face Recognition (CFR) CLOVA Premium Voice (CPV) CLOVA Speech CLOVA Voice CLOVA Dubbing CLOVA Chatbot CLOVA OCR CLOVA AiCall Papago Translation Papago Korean Name Romanizer TensorFlow Server TensorFlow Cluster Pose Estimation Object Detection CLOVA Sentiment CLOVA Summary AiTEMS
Application Service	GeoLocation MAPS CAPTCHA nShortURL SENS (Simple & Easy Notification Service) API Gateway Search Trend RabbitMQ Simple RabbitMQ Service Cloud Outbound Mailer Pinpoint JEUS WebtoB
Media	VOD Transcoder Image Optimizer Live Station VOD Station Video Player
Game	GAMEPOT Game Chat Game Report
Management	Monitoring Cloud Insight Web service Monitoring System Network Traffic Monitoring

Product Category	NAVER Cloud Platform Service for Private Sector Organizations
	Sub Account Cloud Activity Tracer Resource Manager Tools Pinpoint Cloud Cloud Advisor
Analytics	Cloud Log Analytics Real User Analytics (RUA) Effective Log Search & Analytics Cloud Hadoop Cloud Search Search Engine Service Data Analytics Service Cloud Data Streaming Service Cloud Data Box
Dev Tools	Jenkins SourceCommit SourceBuild SourceDeploy SourcePipeline
Business Application	WORKPLACE WORKBOX NAVER WORKS RPA Service
Hybrid & Private Cloud	Hybrid Cloud Hosting Cloud Connect VMware on NCloud
IoT	Cloud IoT Core
Blockchain	Blockchain Service
Migration	Data Teleporter Object Migration

Locations Covered by this Report

The production infrastructure for the systems of NAVER Cloud Platform Service for Private Sector Organizations is located in the datacenters situated in Korea, Western United States (San hose), Germany (Frankfurt), Japan (Tokyo), Singapore and Hongkong. These datacenters deliver the core physical infrastructure that includes physical hardware asset management, security, data protection, networking services.

2. Service Components

The Company’s service components to provide the service consists 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.

Section IV: Principal Service Commitments and System Requirements

The Company has made service commitments to the user entities and established system requirements for the NAVER Cloud Platform Service for Private Sector Organizations. 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 and shared with them through contracts such as Terms of Service (including SLA, Service Level Agreement), Privacy Policy, and so on. The Company also provides online descriptions of the service offerings. Service commitments include, but are not limited to, the following:

- Security: The Company made commitments related to protecting user entities 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 entities 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 entities data. These are addressed through security controls including encryption mechanisms in transferring and storing user entities' 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 user entities 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 Cloud Platform Service for Private Sector Organizations.