NAVER

Information Protection Policy

Date of Revision	2024.06.07
Monitored by	Security

1. Purpose and Objectives

NAVER Corporation (hereinafter referred to as "NAVER" or the "Company") has not only fulfilled the expectations of its stakeholders – including users, shareholders, and business partners – by adhering to relevant laws and compliance standards both domestically and internationally, but has also ensured stable service delivery by prioritizing the security and privacy of users' personal information. As a leading global ICT company, NAVER continuously explores and develops new technologies to shape emerging internet cultures and trends in a rapidly evolving IT landscape. On the other hand, the global landscape of security threats is becoming increasingly advanced and sophisticated. These threats pose significant risks, including personal information breaches, service disruptions, and large-scale denial-of-service attacks, as shown in recent security incidents both domestically and abroad. Consequently, protecting data is no longer optional but essential for survival, and thus NAVER considers achieving the following objectives for data protection imperative.

Objectives of Information Protection

① NAVER guarantees confidentiality, integrity, and availability of information assets.

② NAVER provides stable services while prioritizing the protection of personal information and privacy of users.

③ NAVER supports its businesses to create new value through data protection activities.

④ NAVER fulfills its social responsibility for data protection so that the values created by data protection are not limited to NAVER but are shared with various stakeholders including users, shareholders, and business partners.

2. Scope of Application

All individuals employed by NAVER, as well as employees of its subsidiaries, subcontractors, service providers, and part-time workers who handle NAVER's information assets or have access to the Company's information systems, must adhere to the Information Protection Policy (hereinafter the "Policy"), guides, and guidelines outlined in the NAVER Information Protection Policy System[1]. To this

[1] Refers to a set of policy, guides and guidelines on data protection developed by NAVER; see "4. Management and Policies" of this Policy for more information

end, all employees must familiarize themselves with the Information Protection Policy System that are relevant to their work. Also, when a possibility of conflict with other policies and standards of NAVER is present, they are expected to seek advice from the data protection department. Additionally, if any security incidents during specific tasks occur due to violations of data protection policies, individuals in charge of the tasks are held primarily responsible for the incidents. Also, the individuals' department heads overseeing the tasks share partial responsibility. For corporate or individual entities in a contractual relationship, data protection responsibilities must be included in the contract to establish each party's accountability clearly. In principle, the Information Protection Policy Systems of NAVER's subsidiaries and other entities that are in contractual relationships with NAVER must be applied and operated in alignment with the NAVER Information Protection Policy System. If there is a conflict between the data protection policies of subsidiaries or other entities and the NAVER Information Protection Policy, the NAVER Information Protection Policy shall take precedence and be considered the superior standard.

3. Roles and Responsibilities

NAVER's information protection organization consists of information security department, which handles data protection policies and technical tasks, and a data protection/privacy department, which is responsible for personal information and privacy related policies and rights assurance. The head of the organization overseeing the two departments is responsible for analyzing the causes of various security issues and developing fundamental countermeasures. The head must also formulate mid- to long-term data protection plans in response to changes in the new service environment and regularly report to management. To this end, a cooperative system must be established and maintained with related departments such as service planning, development, and operations. Furthermore, to maintain consistent policy implementation and an immediate response system in accordance with management system, a close cooperation system must be established and operated with the data protection departments of subsidiaries and other related entities. Effective communication channels with external organizations must also be maintained. To facilitate this, the head of the organization responsible for overseeing data protection and personal information security shall be appointed as executive, ensuring that these organizations operate more smoothly and efficiently.

4. Management System

The NAVER Information Protection Policy System is comprised of three components – 1) the **Information Protection Policy**, which serves as the top-level policy document outlining NAVER's management approach; 2) **data protection guides**, which are tailored to specific business areas based on the data protection policy; and 3) **data protection guidelines**, which explain the practical measures for those who are responsible for final business operations. Each policy document is operated and managed by data protection policy department and the personal information security policy department in accordance with area of responsibility. However, given the specialized nature of subsidiaries and the need for efficient management, subordinate documents beneath the data protection guides may be delegated to the data protection departments of each subsidiaries. All documents within the NAVER Information Protection Policy System must be systematically and logically consistent, written in a clear and understandable manner for all employees, and designed to be easily accessible for immediate reference during their work. To this end, the information security guides are structured as follows to ensure that employees can easily access and refer to them according to their jobs:

① Company-wide

② By service stage

③ For global expansion

④ Security and infrastructure

The departments responsible for data protection and privacy protection policies shall establish and maintain an integrated management system. This system oversees the creation and revision of procedures for policies, guides, and guidelines within the NAVER Information Protection Policy System, ensuring that they are consistently updated and distributed in their most current versions.

5. Core Principles

All employees of NAVER must perform their duties according to the following principles for data protection that are aligned with the Company's Objectives for Data Protection.

① Employees shall correctly understand and practice the basic security requirements related to handling user personal information, managing work devices, and responding quickly to security incidents.

② Employees shall comply with relevant laws and standards to ensure the safe protection of user personal information, carefully managing the personal information they handle to prevent loss, theft, leakage, alteration, and misuse.

③ Employees shall manage data to meet security requirements at each stage of service development, from the planning stage to the transfer stage.

④ Employees shall manage data to meet security requirements during service operation, including the sustaining stage of public services, internal systems, and service management systems.

⑤ Employees shall ensure that infrastructure operations, such as servers, networks, and databases, are securely managed to prevent illegal acts and incidents such as leakage, misuse, damage, and destruction due to security vulnerabilities.

⑥ The data protection department shall establish, review, and implement policies and guidelines to ensure the confidentiality, integrity, and availability of information assets. These efforts shall align with the Company's strategy, goals, and business needs, and the department must regularly verify that these measures are being correctly implemented.

Soo-yeon Choi
CEO
NAVER Corporation


NAVER