NHK SPRING Group Information Security Management Policy

President and Representative Member of the Board　Kazuhisa Uemura

It has long been said that we live in an information and IT-driven society. Today, information assets are considered to have a value equal to, or even greater than, the traditional corporate assets of people, goods, and capital. It is no exaggeration to say that timely and accurate information holds the key to the future of NHK SPRING and its Group companies (hereinafter referred to as “NHK SPRING Group ”). With the advancement of IT, it has become possible for anyone to easily access the information they need, anytime and anywhere. At the same time, however, many companies are facing issues such as the destruction or falsification of data through malware and unauthorized access, as well as the leakage of confidential information. Once such problems occur, they not only result in the direct loss of information assets but also cause a loss of trust, which may ultimately jeopardize the very survival of the company. The NHK SPRING Group is no exception.
In such an environment, the purpose of the NHK SPRING Group Information Security Management Policy (hereinafter referred to as “the Policy”) is to establish the fundamental principles, framework, and rules for protecting NHK SPRING Group’s information assets and ensuring the smooth execution of business operations. By implementing appropriate security measures and thoroughly enforcing the Policy, NHK SPRING Group aims to enhance its overall level of information security while strengthening the trust of its stakeholders.

(1) Management Framework

NHK SPRING Group regards information security initiatives as a key management priority. To this end, each department director is designated as an Information Security Manager, supported by the NHK SPRING Computer Security Incident Response Team (NHK Spring-CSIRT), under a structured management framework.

(2) Scope of Application

The information assets to be protected under this Policy encompass all information, IT assets, and services handled by NHK SPRING Group, regardless of their form. These constitute critical assets of NHK SPRING Group, and ensuring their confidentiality, integrity, and availability is essential to the conduct of its business. In line with this recognition, NHK SPRING Group will establish a robust security management framework and implement appropriate protective measures.
Furthermore, the scope of application of this Policy extends to all NHK SPRING Group personnel, including executive officers, employees, part-time staff, and all others with an employment relationship with the Group, as well as temporary staff and employees of external contractors.

(3) Confidentiality Levels

The information assets held by NHK SPRING Group shall be assessed and classified according to their degree of confidentiality and content, and managed appropriately to prevent destruction, falsification, leakage of confidential information, and unauthorized use.

(4) Compliance Requirements

NHK SPRING Group shall ensure the security of confidential information by adhering to the various regulations, guidelines, and other rules that constitute this Policy. In addition, NHK SPRING Group shall not improperly acquire or use confidential information belonging to others.

(5) Education

NHK SPRING Group shall provide planned and ongoing education and training to ensure that all employees are thoroughly informed of and comply with information management practices.

(6) Auditing

The Audit Department shall verify and confirm that each department is complying with this Policy. Based on the results of such audits, the audited departments shall regularly and continuously review their security measures to maintain a secure environment.

(7) Disciplinary Action

If NHK SPRING Group employees, etc., neglect their obligation to comply with this Policy and engage in malicious conduct, etc. that has, or could have, a significant impact on NHK SPRING Group's security, they shall be subject to disciplinary action or other penalties in accordance with the Rules of Employment.

(8) Response to Information Security Breaches

In the event that an incident occurs which is determined to constitute an information security breach at NHK SPRING Group, the Group shall respond promptly in accordance with the relevant regulations, guidelines, and procedures.

＊In this Policy, the terms "Confidentiality," "Integrity," and "Availability" are used with the following meanings:

1. Confidentiality: Being accessible only to specifically authorized persons.
2. Integrity: Being free from alteration or falsification, and completely accurate.
3. Availability: Being accessible and usable when required.

Established: December 1, 2003
Revised: April 1, 2010
Revised: November 1, 2017
Revised: January 1, 2025
Revised: March 3, 2026