

October 8, 2026

ENFORCEMENT OF THE AMENDED NETWORK ACT: ENHANCED INFORMATION SECURITY, INCIDENT RESPONSE, AND REGULATION OF ILLEGAL SPAM

I. ENFORCEMENT OF THE AMENDED NETWORK ACT AND ENFORCEMENT DECREE

The amendment to the "Act on the Promotion of the Use of Information and Communications Networks and Information Protection, etc." (hereinafter the "Network Act"), which passed the National Assembly plenary session on March 12, 2026, was promulgated on March 31, 2026, and has been in effect since October 1, 2026. As a follow-up measure, Presidential Decree No. 36735, "Decree Partially Amending the Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." (hereinafter the "Enforcement Decree"), was promulgated on September 30, 2026, and took effect on October 1, 2026.

[In our March newsletter](#), we introduced the key provisions of the legislation, including the expansion of the powers and responsibilities of the Chief Information Security Officer (CISO) introduced by the amended Act, the establishment of an Information Security Committee, the notification and investigation of security breaches, enforcement fines and administrative penalties, and strengthened regulations on illegal spam. The Enforcement Decree promulgated now specifies the scope of application and operational methods of these systems, standards for user notifications, and criteria for calculating administrative fines and enforcement penalties. Therefore, companies now need to review their actual internal systems and incident response procedures based not only on the direction of the amended Act but also on the finalized detailed standards.

II. KEY PROVISIONS

CATEGORY	KEY PROVISIONS OF THE ENFORCEMENT DECREE
CISO and Information Security Committee	Specifies CISO qualification requirements and additional duties; mandates that certain businesses establish an Information Security Committee, convene it at least once a year, and establish a reporting system to the CEO and the board of directors
Differentiated Application of ISMS	Specifies the scope of application for the enhanced Information Security Management System (ISMS) certification based on factors such as revenue, business type, and recent history of security incidents, and conducts both written and on-site audits
Incident Notification and Response	Requires immediate notification to users in cases of service disruptions lasting two hours or longer or breaches of user information, and stipulate the content and method of notification as well as follow-up notification procedures

Manuals and Remedies	Requires certain businesses to prepare and submit manuals for managing and responding to security incidents, and must submit a report on the results of remedial measures within 14 days of reporting the incident
Sanctions and Illegal Spam	Establishes specific calculation standards for compliance enforcement fines and penalties for repeated security incidents, and further specifies the criteria for restrictive measures and penalties regarding violations related to the transmission of advertising information

1. Specifies Standards for CISO Qualifications, Duties, and the Operation of the Information Security Committee

The amended law requires telecommunications service providers to designate a Chief Information Security Officer (CISO) as an executive officer, thereby strengthening the CISO's authority and responsibilities, including the management of information security personnel, budget allocation, and reporting to the board of directors. The Enforcement Decree specifies that a CISO may be a business owner, representative, director, executive officer, de facto director, or executive officer. Furthermore, for medium-sized enterprises as defined by the Framework Act on Small and Medium-Sized Enterprises—specifically telecommunications service providers, entities required to obtain information security management system certification, personal information processors, and e-commerce sellers—the head of the department overseeing information security-related operations may also be designated as the CISO.

Furthermore, the CISO's duties include conducting security reviews upon the introduction, launch, or modification of telecommunications systems or services, as well as regularly inspecting and supervising the security levels of entities entrusted with the construction, operation, and management of information and communications systems, information processing contractors, and cloud computing service providers. It is important to note that security reviews regarding the supply chain and cloud usage have been explicitly included in the CISO's statutory scope of duties (Enforcement Decree Article 36-7, Paragraph 7).

The entities required to establish an Information Security Committee are specified as telecommunications service providers falling under Items 2 through 4 of Paragraph 1 of Article 36-7 of the Enforcement Decree. The committee shall be chaired by the CISO and composed primarily of the heads of departments related to information security, personal information processing, IT operations and development, compliance and legal affairs, finance, and human resources; it must meet at least once a year. The results of deliberations must be reported to top management, and matters having a significant impact on information security must also be reported to the board of directors (Enforcement Decree, Articles 36-10 and 36-11).

2. Determination of Entities Subject to Enhanced Information Security Management System (ISMS) Certification Requirements

The Enforcement Decree stipulates that ISMS certification audits must combine document reviews with on-site inspections, while also specifying the entities subject to enhanced certification standards and procedures, taking into account the scale of

information and social impact. The entities subject to these enhanced requirements are as follows (Enforcement Decree Article 55-7, Paragraph 3).

- Major telecommunications service providers or operators of integrated information and communications facilities whose revenue for the previous fiscal year was 1 trillion won or more
- Telecommunications service providers with revenue of 3 trillion won or more in the previous fiscal year
- Telecommunications service providers that have experienced a security breach within the last three years, and were investigated by a joint public-private investigation team, or that have been levied administrative fines due to repeated security breaches

Furthermore, regulations stipulate that if a provider is assessed a penalty for repeated security breaches and the severity of the breach is classified as a “very serious security breach” or a “serious security breach,” this may constitute grounds for revocation of ISMS certification; thus, sanctions for security breaches can directly affect the maintenance of certification (Enforcement Decree Article 52-2).

3. Specification of Standards for Notifying Users of Data Breaches and Investigation Procedures

The amended Act requires that users be notified without delay when certain security incidents occur, and the Enforcement Decree specifies the scope of such incidents and the notification methods. The scope of user notifications includes the following security incidents (Enforcement Decree Article 58-9).

- Incidents in which a disruption or interruption of telecommunications services persist for two hours or longer
- Incidents in which user information has been lost, stolen, leaked, altered, damaged, or misappropriated, or where there is a possibility of such occurrence
- Incidents equivalent to the above which pose a risk of significantly affecting the protection of user information

The notification must include (i) the date and time of the incident, its cause, and details of the damage; (ii) the status of the response, including measures taken regarding the security incident; (iii) information on steps users can take to minimize potential damage resulting from the security incident; (iv) details of measures taken to remedy user damage; and (v) the department responsible for handling complaints related to damage remediation and its contact information. If the cause of the incident or the details of the damage have not yet been specifically confirmed, the provider must first notify users of the fact that the security incident occurred, the details confirmed up to that point, and the information listed in items (ii) through (v) above; any additional details confirmed thereafter must be notified immediately upon confirmation. Notification may be provided in writing, by telephone, email, fax, or text message; if there is a valid reason,

such as the user's contact information being unknown, it may be substituted by posting the notice on the website for at least 30 days.

Meanwhile, the Security Incident Investigation Deliberation Committee shall consist of no more than 15 members, including the chairperson, with due consideration given to gender balance; it shall deliberate on the scope and methods of investigation when an investigation into whether a security incident has occurred is necessary. Accordingly, it is important to note that not only when a security incident has already been confirmed, but also at the stage where its occurrence is suspected, an investigation by the regulatory authority and measures to prevent the spread of damage may be carried out following a review of the necessity for such an investigation (Enforcement Decree Articles 58-2 and 58-3).

4. Specification of the Security Incident Management and Response Manual and Obligations for User Remedies

The obligation to prepare and submit a security incident management and response manual applies to: ① telecommunications service providers with total assets of 5 trillion won or more as of the end of the previous fiscal year; ② telecommunications service providers subject to mandatory Information Security Management System (ISMS) certification that have total assets of 500 billion won or more as of the end of the previous fiscal year; ③ medium-sized enterprises that are telecommunications operators; those subject to mandatory ISMS certification, telecommunications service providers that are personal information processors required to disclose a privacy policy, or e-commerce businesses; and ④ all other telecommunications service providers, excluding those with capital of 100 million won or less, small enterprises, or medium-sized enterprises that do not fall under the categories listed above (i.e., telecommunications operators, entities subject to mandatory ISMS certification, personal information processors required to disclose a privacy policy, or e-commerce businesses). These businesses must prepare a management and response manual (hereinafter referred to as the "Manual") for the prevention of data breaches and rapid response in the event of an incident, and submit it to the Minister of Science and ICT (the "MSIT"). The Manual must include: a) the organizational structure, designated personnel, and methods for information sharing to prevent security breaches and limit the spread of damage; b) measures to remedy user harm and minimize damage in the event of a security breach; c) an inspection and response system for preventing security breaches; d) plans for the regular review and updating of the Manual, and e) any other matters deemed necessary by the MSIT to enhance the efficiency and expertise of inspections regarding the preparation and operation of the Manual. The MSIT may inspect the preparation and operation of the Manual through written or on-site investigations, taking into account compliance with information security disclosure requirements, recent history of security incidents, and the number of service users. When conducting an inspection of the preparation and operation of the manual, the MSIT must notify the party obligated to prepare the manual in writing of the purpose, scope, method, and duration of the inspection at least 7 days

prior to the start of the inspection; however, in cases where an urgent inspection is necessary, such as when a security incident occurs, the MSIT may provide written notice or give oral notification at the same time the inspection begins. (Enforcement Decree Article 60-15).

Furthermore, regarding redress for user damages resulting from security incidents, telecommunications service providers must submit details regarding the content, scope, and results of the redress measures to the MSIT within 14 days of the date the security incident was reported. If unavoidable circumstances are recognized, this deadline may be extended once, provided the extension does not exceed 14 days (Article 60-16 of the Enforcement Decree).

5. Establishment of Calculation Standards for Enforcement Fines and Penalties for Recurring Security Incidents

Enforcement fines imposed for failure to comply with a re-order—such as failure to submit or submission of false information during an investigation, obstruction of an on-site investigation, or failure to comply with a corrective order—are set at 2 ten-thousandths (0.02%) of the average daily sales under the Enforcement Decree as the base amount per day. This amount may be increased or reduced by up to 50%, considering the efforts made to comply with the order and the degree of non-compliance. However, the amount may not exceed the upper limit prescribed by law. If compliance is not achieved within 90 days after the expiration of the re-order compliance period, additional penalties may be imposed and collected every 90 days thereafter (Enforcement Decree Article 60-10 and Appendix 5-2).

If a security incident occurs two or more times within five years due to the willful misconduct or gross negligence of a telecommunications service provider, the penalty surcharge shall be calculated based on the amount obtained by subtracting revenue unrelated to the security incident from the revenue calculated for the fiscal year in which the most recent security incident occurred. The Enforcement Decree classifies the imposition rates according to the severity of the security incident as follows: “very serious security incident” (2.1% or more but not exceeding 2.7%); “serious security incident” (1.5% or more but less than 2.1%); “moderate security incident” (0.9% or more but less than 1.5%); and “minor security incident” (0.03% or more but less than 0.9%). Subsequently, adjustments (increases or reductions) are made based on information security efforts, such as cooperation with investigations, recovery from damage and prevention of further spread, allocation of personnel and budget for information security, committee operations, and the development of manuals; however, the amount cannot exceed the statutory maximum (Enforcement Decree Article 60-11 and Annex 5-3).

6. Specification of Restrictive Measures and Fines for Illegal Spam

The Enforcement Decree specifies the measures that service providers must take and the criteria for calculating penalty surcharges when telecommunications services are used to transmit illegal advertising information.

If an telecommunications service provider becomes aware that its service is being used to transmit unlawful advertising information, it must immediately cease such transmission; if the cause is a vulnerability in the security system, it must inspect and improve the system; and if the cause is a deficiency in the user agreement or terms of service, it must amend the relevant provisions and establish and review a plan to prevent recurrence (Enforcement Decree, Appendix 6-2). Administrative fines are calculated based on revenue excluding amounts unrelated to the violation. For general violations of regulations governing the transmission of promotional information, a penalty rate of 1% to 4% applies, depending on the severity of the violation. However, a penalty rate of 3% to 6% applies in cases where prohibited acts¹ are committed during the transmission of promotional information (violation of Article 50, Paragraph 5 of the Act) or where promotional information is transmitted for the purpose of illegal acts (violation of Article 50-8) (Enforcement Decree Article 64-2 and Appendix 6-3).

III. EFFECTIVE DATE AND TRANSITIONAL MEASURES

The amended Network Act and this Enforcement Decree have been in effect since October 1, 2026. Therefore, businesses subject to the above obligations should note that they are no longer in the preparatory phase but are now required to comply with the law.

However, the system for periodic evaluation of information security levels (Article 45-5 of the Act) and the related administrative fine provisions will take effect one year after promulgation; thus, they are scheduled to apply starting April 1, 2027. The Enforcement Decree also stipulates that the administrative fine standards for refusing to submit or submitting false materials related to information security level evaluations will take effect on April 1, 2027.

Furthermore, among businesses that designated and reported the head of the department overseeing information security-related operations as the CISO in accordance with the previous regulations at the time of enforcement, those falling under Article 36-7(1)(4) of the Enforcement Decree must re-designate and report a CISO who meets the new qualification requirements within six months from the effective date.

¹ ① Acts that circumvent or obstruct a recipient's opt-out or withdrawal of consent to receive commercial messages; ② Acts that automatically generate a recipient's contact information—such as a phone number or email address—by combining numbers, symbols, or characters; ③ Acts that automatically register phone numbers or email addresses for the purpose of transmitting commercial messages for profit; ④ Any act intended to conceal the identity of the sender of commercial messages or the source from which the advertisement is sent; ⑤ Any act intended to deceive recipients into replying for the purpose of transmitting commercial messages for profit

IV. IMPLICATIONS

In light of the implementation of the Network Act, companies need to review the following matters to ensure compliance with the law:

- Verify whether the current CISO meets the qualification requirements under the amended Enforcement Decree, and revise the composition, operating regulations, and annual meeting schedule of the Information Security Committee, as well as the reporting procedures to the CEO and the board of directors
- Determine whether the strengthened ISMS applies based on revenue, business type, and the history of security incidents over the past three years, and prepare a certification response system that takes into account both written and on-site audits
- Incorporate user notification triggers, including service disruptions lasting two hours or more and the potential for user data breaches, into the incident response manual, and specify procedures for initial notification, follow-up notifications, and website announcements
- Incorporate the mandatory items specified in the Enforcement Decree into the security incident management and response manual, and standardize in advance the records of regular inspections and updates, as well as the materials to be submitted within 14 days of reporting, including remedial measures and damage relief actions
- Separately manage revenue data required for calculating enforcement fines and administrative penalties, and systematically accumulate internal records that can substantiate mitigating factors such as cooperation with investigations, prevention of damage spread, and investment in information security
- When outsourcing the transmission of promotional information to external service providers, verify whether they hold transmission qualification certification, and review contracts, terms of service, and service suspension and restoration processes to ensure they comply with the restriction criteria set forth in the Enforcement Decree

* * *

Bae, Kim & Lee LLC has extensive advisory experience regarding the establishment of CISO and Information Security Committee frameworks under the Network Act, the review of entities subject to ISMS requirements, the development of incident response manuals and user notification and damage relief processes, responding to investigations by regulatory agencies, and addressing compliance fines, administrative penalties, and illegal spam regulations. Please feel free to contact us at any time if you have any questions regarding the application of the amended Act and its Enforcement Decree.

For any inquiry or questions regarding the content of this newsletter, please contact us.

Related Professionals

Jiyeon Park

Partner

T 82.2.3404.0655

E jiyeon.park@bkl.co.kr**Taeuk Kang**

Partner

T 82.2.3404.0485

E taeuk.kang@bkl.co.kr**Juho Yoon**

Partner

T 82.2.3404.6542

E juho.yoon@bkl.co.kr**Kanghye Lee**

Partner

T 82.2.3404.7454

E kanghye.lee@bkl.co.kr**Sean Jeong**

Senior Foreign Attorney (New York)

T 82.2.3404.1036

E sean.jeong@bkl.co.kr

Please note that the content and opinions published in the Bae, Kim & Lee LLC newsletter are provided solely for general informational purposes and do not constitute the official views of Bae, Kim & Lee LLC or legal advice regarding any specific matter. If you have any questions regarding the newsletter, please contact us using the information above.