SEOUL METROPOLITAN GOVERNMENT ORDINANCE ON CYBERSECURITY

Enactment No. 9889, Sep. 29, 2025

Article 1 (Purpose)

The purpose of this Ordinance is to prescribe the matters required to strengthen cybersecurity and to improve and enhance the systems of cooperation between the relevant institutions so as to enable the latter to respond systematically and effectively to cyber-attacks and threats, and to prescribe the matters delegated by the Regulations on Cybersecurity Services.

Article 2 (Definition of Terms)

The definitions of the terms used in this Ordinance shall be as follows:

1. "Cyber-attacks and threats" refers to acts involving intrusions into disturbance, paralysis or destruction of information and communications devices, information and communications networks, or related information systems, etc. by electronic means such as hacking, computer viruses, distributed denial of services (DDoS), electronic waves, or forgery, alteration, damage, or theft of information, and threats related thereto.
2. "Agencies at various levels" refers to organizations under the direct control of the Seoul Municipal Government, offices, collegiate administrative agencies, the Secretariat of the Seoul Metropolitan Council, and autonomous Gu's public corporations and public agencies under the Local Public Enterprises Act; and invested or funded institutions under the Seoul Metropolitan Government Ordinance on the Operation of Invested or Funded Institutions.
3. "Information system" refers to an information system as specified under subparagraph 13 of Article 2 of the Electronic Government Act.
4. "Information protection system" refers to an information protection system as specified under subparagraph 15 of Article 2 of the Framework Act on Intelligent Informatization.
5. "Information and communications device" refers to a device, facility, software, or information and communications service relating to the collection, processing, storage, search, transmission, reception, or utilization of information.
6. "Information and communications chamber" refers to a place where information systems, information protection systems, etc. such as servers, switches, firewalls, or intrusion blocking systems are installed and operated, regardless of the name, such as the computer room, communications room, data center, etc.

Article 3 (Responsibility)

(1) The Seoul Metropolitan City Mayor (hereinafter referred to as the "Mayor") and the heads of agencies at various levels shall make efforts to protect cyberspace from cyber-attacks and threats.
(2) The Mayor and the heads of agencies at various levels shall form and operate organizations, personnel, and budgets, then guide and oversee them to facilitate the performance of cybersecurity services at the main office of the Seoul Metropolitan Government and agencies at various levels (hereinafter referred to as "agencies at various levels, etc.").
(3) The Mayor and the heads of agencies at various levels shall protect the affairs under their jurisdiction as prescribed by other statutes such as Local Autonomy Act from cyber-attacks and threats.
(4) The heads of agencies at various levels shall make efforts to ensure the level of cybersecurity corresponding to the cybersecurity policies formulated and implemented by the Mayor.

Article 4 (Applicability)

This Ordinance shall apply to the cybersecurity services of the agencies at various levels, etc. of the Seoul Metropolitan Government.

Article 5 (Scope of Public Institutions Subject to Cybersecurity Duties)

"Institutions prescribed by Municipal Ordinance" in Article 7 (2) 2 of the Regulations on Cybersecurity Services refers to invested or funded institutions established by the investment or funding of Seoul Metropolitan Government and designated and publicly notified under Article 5 of the Act on the Operation of Local Government-Invested or -Funded Institutions.

Article 6 (Operation of a Cybersecurity Managing Officer)

(1) To ensure the efficient and systematic performance of cybersecurity duties and the safe protection of the affairs under his or her jurisdiction, the Mayor shall secure appropriate personnel with expert knowledge in cybersecurity to form and operate a dedicated cybersecurity organization.

(2) The Mayor shall appoint a cybersecurity management officer to take exclusive charge of the following duties:
1. Formulation and implementation of cybersecurity policies and plans, and guidance and oversight of cybersecurity duties.
2. Management of the dedicated cybersecurity organization and fostering of expert personnel.
3. Review of informatization project security and verification of security suitability.
4. Security management and oversight of information and communications chambers, information and communications networks, etc.
5. Implementation of cyber-attack and threat response training and inspections of the actual state of cybersecurity.
6. Security control, accident analysis and response, and information-sharing with the relevant institutions.
7. Formulation and implementation of cybersecurity education and cybersecurity diagnostic days.
8. Cybersecurity audits of agencies at various levels, etc.
9. Formulation, operation, and security management of restoration countermeasures for information protection systems.
10. Oversight of the duties of the assistant cybersecurity management officer.
11. Other cybersecurity matters determined by the relevant rules.
(3) The heads of agencies at various levels shall appoint cybersecurity management officers to take exclusive charge of the following services, and designate cybersecurity officers to assist them:
1. Guidance and oversight of the cybersecurity services under jurisdiction.
2. Security management and oversight of information and communications chambers, information and communications networks, etc. under jurisdiction.
3. Cooperation with cyber-attack and threat response training and inspections of the actual state of cybersecurity.
4. Cooperation with security control, accident analysis and response, and information-sharing with the relevant institutions.
5. Formulation and implementation of cybersecurity education and cybersecurity diagnostic days.
6. Formulation, operation and security management of restoration countermeasures for information protection systems under jurisdiction.
7. Oversight of the duties of the agency's assistant cybersecurity management officer.
8. Other cybersecurity matters determined by the relevant rules.
(4) When necessary to perform the duties provided under the foregoing paragraph (3), the heads of agencies at various levels may request administrative and financial support from the Mayor.

Article 7 (Operation of Assistant Cybersecurity Management Officers)

(1) To ensure the cybersecurity management officer's efficient performance of his or her duties, the Mayor shall appoint and assign an assistant cybersecurity management officer to each department and appoint assistant cybersecurity officers to assist them. Matters necessary for the foregoing - such as the assistant cybersecurity management officer's qualifications, appointment procedures, and scope of duties - shall be determined by the relevant rules.
(2) When necessary to ensure the efficient performance of the duties of the cybersecurity management officers and cybersecurity officers, considering the size of agencies at various levels and the nature of their duties, etc., the heads of agencies at various levels may recruit appropriate personnel capable of performing each department's cybersecurity duties and appoint assistant cybersecurity officers to assist them.

Article 8 (Formulation of Basic Plans)

To ensure the efficient implementation of cybersecurity duties, the Mayor shall formulate and implement a Seoul Metropolitan City Cybersecurity Basic Plan (hereinafter the "Basic Plan") every five years, which shall include the following matters:
1. Cybersecurity goals and directions for their implementation;
2. Matters concerning domestic and international trends, the adoption of new technology, and responses;
3. Countermeasures to prevent cyber-attacks and threats;
4. Promotion of cybersecurity education;
5. Fostering of experts to ensure stronger cybersecurity;
6. Ways to enhance systems of cooperation with the relevant institutions;
7. Matters otherwise necessary for stronger security, as determined by the relevant rules.

Article 9 (Formulation of Implementation Plans)

(1) The Mayor shall formulate and implement annual implementation plans for cybersecurity duties in keeping with the Basic Plans under Article 8.
(2) The heads of agencies at various levels shall formulate and implement annual implementation plans for cybersecurity duties at their agencies and submit the plans to the Mayor.

Article 10 (Establishment and Functions of the Cybersecurity Advisory Committee)

The Mayor may establish the Seoul Metropolitan Government Cybersecurity Advisory Committee (hereinafter referred to as the "Committee") to advise on implementing the following cybersecurity services:

1. Establishment and modification of the Basic Plans.
2. Assessment of the implementation of major services.
3. Ways to respond to changes in domestic and international cybersecurity conditions.
4. Other matters determined by the relevant rules.

Article 11 (Committee Composition)

(1) The Committee shall be composed of 15 or fewer members including one Chairperson and two Vice-Chairpersons, and the gender balance shall be considered in the composition.

(2) Members shall be appointed or commissioned from among the following persons by the Mayor, while the Chairperson shall be elected by and from among the commissioned members; one of the two Vice-Chairpersons shall be an ex officio member, while the other shall be elected by and from among the commissioned members.

1. Ex officio member: The head of the office, headquarters, or bureau to which the dedicated cybersecurity organization belongs.
2. Commissioned members: Any of the following persons who have extensive knowledge and/or experience of cybersecurity:

(a) A cybersecurity-related expert.
(b) The chief information security officer of an enterprise located in Seoul Metropolitan City.
(c) A member of the standing committee over which the office, headquarters, or bureau to which the dedicated cybersecurity organization belongs has jurisdiction.
(d) Other persons as determined by the relevant rules.

(3) The Chairperson shall represent the Committee and oversee its work; if the Chairperson is unable to perform their duties due to an unavoidable cause, the Vice-Chairperson (the commissioned member shall have priority) shall perform the Chairperson's duties by proxy, followed by a member designated in advance by the Chairperson.

(4) There shall be a secretary to handle the Committee's affairs, and an official of the dedicated cybersecurity organization shall serve as the secretary.

(5) The Committee shall be composed as and when an agenda arises and shall be dissolved as a matter of course after deliberation and advice.

(6) A meeting of the Committee shall be opened by the attendance of the majority of the members, and it shall reach a result by the affirmative vote of a majority of the attending members.

(7) The duration of the Committee shall be until five years after the date of enforcement of this Ordinance.

(8) Other matters on the decommissioning, exclusion, challenge, recusal, compensation, etc. of members shall be governed by the Seoul Metropolitan Government Ordinance on the Establishment and Operation of Various Committees.

Article 12 (Data Submission)

The Mayor may request the heads of agencies at various levels to submit data if necessary for the performance of cybersecurity services, such as self-diagnostics and inspections under Article 15, investigation of accidents under Article 19, cybersecurity audits under Article 25, and assessments of the actual state of cybersecurity under Article 13 of the Regulations on Cybersecurity Services. The heads of agencies at various levels who receive such requests shall comply in the absence of a justifiable cause for not doing so.

Article 13 (Cybersecurity Education)

(1)The Mayor and the heads of agencies at various levels shall implement at least one educational course per year as necessary to raise affiliated public officials' (including civil servants and fixed-term employees; hereinafter the same shall apply) and employees' awareness of the necessity and importance of cybersecurity and to enhance the work capabilities of affiliated public officials and employees who perform cybersecurity duties.

(2) In the absence of a compelling reason for not doing so, affiliated public officials and employees shall complete at least one course per year of the training provided under paragraph (1).

(3) The Mayor and the heads of agencies at various levels shall encourage the completion of educational courses at expert institutions, participation in academic conferences, etc. in order to enhance the work-related expertise of cybersecurity management officers and cybersecurity officers and to cultivate the cybersecurity knowledge of affiliated public officials.

(4) The Mayor may provide administrative and financial support to encourage affiliated public officials to complete the educational courses provided under the foregoing paragraph (1) and to complete educational courses at expert institutions

and participate in academic conferences, etc., as provided under paragraph (3).

Article 14 (Preventative Cybersecurity Measures, Etc.)

(1) To prevent cyber-attacks and threats, the Mayor may review the security of informatization projects implemented at agencies at various levels, etc., and verify whether the results of such review are implemented by agencies at various levels, etc.
(2) The Mayor and the heads of agencies at various levels shall designate and periodically implement “cybersecurity diagnostic days” appropriate to each agency’s circumstances.
(3) The Mayor and the heads of agencies at various levels shall formulate and implement security countermeasures when implementing informatization projects; the specific scope and means, etc. thereof shall be determined by the relevant rules.
(4) The Mayor shall perform the following prevention and countermeasure activities for the comprehensive management of cyber-attacks and threats:
1. Periodic preventive inspection and training.
2. Adoption and utilization of safe information and communications devices.
3. Establishment and operation of protective systems, such as cyber-attack and threat detection systems, information sharing systems, and accident reporting systems.
4. Securing of expert personnel and implementation of job training.
5. Other activities determined by the relevant rules.

Article 15 (Cybersecurity Self-Diagnostics and Inspections)

(1) The Mayor shall implement, on an annual basis at the very least, self-diagnostics and inspections of the following, in order to prevent and respond to cyber-attacks and threats against agencies at various levels, etc.:
1. Information systems such as servers and network equipment.
2. Public-facing and work websites.
3. Information protection systems such as firewalls and intrusion prevention systems.
4. Other subjects determined by the relevant rules.
(2) In addition to the self-diagnostics and inspections under the foregoing paragraph (1), the Mayor may inspect the actual state of cybersecurity if necessary to ensure stronger cybersecurity at agencies at various levels, etc.
(3) In the event that a self-diagnostic and inspection under paragraph (1) or an inspection of the actual state of cybersecurity under paragraph (2) reveals a vulnerability, the Mayor may request the heads of agencies at various levels to take all necessary corrective measures; and the heads of agencies at various levels who receive such requests shall comply with them in the absence of a justifiable reason for not doing so.

Article 16 (Strengthening Security for the Use of New TechnologiesSuch as Artificial Intelligence)

(1) When agencies at various levels, etc. seek to implement the following policies, they shall formulate security countermeasures and consult with the Mayor to identify security threats in advance and remove security vulnerabilities:
1. Projects that utilize or incorporate new technologies such as artificial intelligence or autonomous driving systems.
2. Projects that are built and operated on areas separate from internal networks, such as cloud computing, wireless LAN, visual data processing devices, and the internet of things.
3. Other projects determined by the relevant rules.
(2) Matters necessary for consultation under paragraph (1) shall be determined by the relevant rules.

Article 17 (Establishment and Operation of Security Control Centers)

(1) The Mayor shall establish and operate the Security Control Center to detect and respond immediately to cyber-attacks and threats against agencies at various levels, etc. (hereinafter referred to as “security control”)
(2) The Security Control Center shall perform the following duties:
1. Collection and storage of logs generated by the information protection systems of agencies at various levels, etc.
2. Detection and analysis of cyber-attacks and threats against agencies at various levels, etc.
3. Response to cyber-attacks and threats against agencies at various levels, etc., and initial measures.
4. Investigation of accidents due to cyber-attacks and threats against agencies at various levels, etc.
5. Training to respond to cyber-attacks and threats against agencies at various levels, etc.
(3) For the security control of agencies at various levels, the heads of agencies at various levels shall establish and operate security control centers linked to the Security Control Center under paragraph (1): Provided that, where it is more efficient to utilize a security control center operated by another agency in light of the agency’s size and the nature of its duties, etc., the head of the agency may utilize another agency’s security control center without establishing one directly.

(4) To ensure security control under paragraph (1), the Mayor may request the necessary cooperation or support from cloud computing service providers under subparagraph 4 of Article 2 of the Act on the Development of Cloud Computing and the Protection of Its Users.

Article 18 (Issuance of Warnings)

(1) Where a warning has been issued under Article 15 of the Regulations on Cybersecurity Services, the Mayor and the heads of agencies at various levels shall take necessary measures according to the corresponding warning level, such as strengthening readiness against cyber-attacks and threats.
(2) Measures to be taken by the Mayor and the heads of agencies at various levels by warning level shall be determined by the relevant rules.

Article 19 (Accident Investigation and Reporting)

(1) In the event of accident caused by a cyber-attack or a threat against agencies at various levels, etc., the Mayor may investigate the accident in order to identify the perpetrator of the attack, analyze the cause, and confirm the details of any damages, etc.
(2) In the event of an accident under the foregoing paragraph (1), the Mayor may request the heads of agencies at various levels to take all measures necessary to ensure the continuity of work performance and the provision of the services provided by agencies at various levels, and to minimize the impact of the accident. The heads of agencies at various levels who receive such request shall comply in the absence of a justifiable reason for not doing so.
(3) The heads of agencies at various levels, upon learning that an accident has occurred due to a cyber-attack or threat, shall report the facts to the Mayor without delay.
(4) In the event that personal information is divulged due to an accident caused by a cyber-attack or threat, the Mayor shall fully cooperate with the personal information controllers at agencies at various levels, etc. in order to minimize the damages.

Article 20 (Cybersecurity Restoration System)

(1) Depending on the severity of an accident, the Mayor may form and assign a Cybersecurity Emergency Countermeasures Team to minimize the damages resulting from an accident under Article 19.
(2) If necessary, the heads of agencies at various levels may request the Mayor to form a Cybersecurity Emergency Countermeasures Team under paragraph (1).
(3) Matters necessary for the composition and operation of a Cybersecurity Emergency Countermeasures Team under paragraph (1) shall be determined by the relevant rules.

Article 21 (Cyber-Attack and Threat Response Training)

(1) The Mayor and the heads of agencies at various levels shall implement, on an annual basis at the very least, training on how to respond to cyber-attacks and threats.
(2) The Mayor may implement joint training in preparation for cyber-attacks and threats against agencies at various levels, etc.
(3) When seeking to implement joint training under paragraph (2), the Mayor shall give advance notice of the training schedule, etc. to the heads of the agencies at various levels concerned, unless there is a compelling reason not to do so.
(4) If the Mayor deems it necessary, as a result of the joint training under paragraph (2), he or she may request the heads of agencies at various levels to implement corrective measures.
(5) The scope and detailed substance of the training under paragraph (1) and the joint training under paragraph (2) shall be determined by the relevant rules.

Article 22 (Sharing of Information on Cybersecurity Threats)

(1) To ensure the prevention of and rapid response to cyber-attacks and threats, the Mayor and the heads of agencies at various levels may share the following information (hereinafter referred to as “threat information”) between agencies:
1. Information on the means of, and response measures to, cyber-attacks and threats.
2. Software used in cyber-attacks and threats, and related information.
3. Information on security vulnerabilities in information and communications networks, information protection systems, information and communications devices, etc.
4. Information that is otherwise necessary for the prevention of and response to cyber-attacks and threats, as determined by the relevant rules.
(2) The Mayor and heads of agencies at various levels shall devise security countermeasures to prevent any forgery,

alteration, damage, divulgence, etc. of threat information in the course of sharing such information as provided under paragraph (1).

Article 23 (Cooperation Systems)

The Mayor may implement the following matters in order to enhance cybersecurity levels and strengthen the systems for domestic and international cooperation:

1. Establishment of a crisis response system through cybersecurity cooperation and information sharing with central administrative agencies.
2. Cybersecurity information sharing and joint research with international institutions and private institutions.
3. Holding of seminars, conferences, forums, etc. concerning paragraphs (1) and (2);
4. Other matters determined by the rules for enhancing systems of cooperation.

Article 24 (Consultative Council)

(1) The Mayor may participate in a consultative council under Article 169 of the Local Autonomy Act in order to coordinate cybersecurity policies and promote information-sharing.

(2) The Mayor may form a public-private cooperation consultative council, etc. at the Seoul Metropolitan Government level to promote stronger cybersecurity or participate as necessary in consultative councils administered by the relevant institutions.

(3) The Mayor may offer the necessary administrative and financial support to facilitate the operations of consultative councils under paragraphs (1) and (2).

Article 25 (Cybersecurity Audits)

(1) The Mayor shall implement, on an annual basis at the very least, cybersecurity audits to investigate and inspect the cybersecurity services and activities of agencies at various levels, etc.; the standards and procedures for which shall be determined by the Mayor with reference to the guidelines presented in Article 3-2 (1) 2 of the Regulations on Cybersecurity Services.

(2) If necessary as a result of a cybersecurity audit under paragraph (1), the Mayor may request an internal audit from an internal audit body under the Act on Public Sector Audits.

(3) When performing self-diagnostics and inspections under Article 15, the Mayor may utilize the data submitted by agencies at various levels in cybersecurity audits under paragraph (1).

Article 26 (Handling of Persons who Infringe the Cybersecurity Regulations)

The Mayor shall enact and implement standards for the handling of persons who have infringed the cybersecurity regulations.

Addendum <No. 9889, Sep. 29, 2025>

Article 1 (Enforcement Date) This Ordinance shall enter into force on the date of its promulgation.

Article 2 (Transitional Measures on the Standards for the Handling of Violators) Standards for the handling of violators enforced under the Seoul Metropolitan Government Information and Communications Security Services Handling Rule prior to the enforcement of this Ordinance shall be deemed to have been implemented under this Ordinance.

Article 3 (Transitional Measures on Appointments) Any information security management officer appointed under the Seoul Metropolitan Government’s Regulations on the Administration of Information and Communications Security Affairs prior to the enforcement of this Ordinance shall be deemed to have been appointed as a cybersecurity management officer under Article 6 of this Ordinance.

Article 4 (Amendment of Other Ordinances) An article of the Seoul Metropolitan Government Ordinance on Smart Cities and Informatization shall be amended as follows:

Article 21 (2) shall be as shown below, while each of paragraphs (3) to (5) of that Article shall be deleted.

(2) Other matters on information protection shall be governed by the Seoul Metropolitan Government Ordinance on Cybersecurity.