Chapter 1 General Rules

(Purpose)

Article 1 This outline is based on the provisions of Article 28, Paragraph 1 of the Nerima Ward Informatization Management Regulations (Nerima Ward Instruction No. 24, November 2004; hereinafter referred to as the "Management Regulations"). A system for promoting information security management and information security management in the ward (hereinafter referred to as "ward") while defining basic matters for ensuring and maintaining the confidentiality, completeness and availability of information assets owned by the ward. It shall define necessary matters regarding "security management system") and information security management operation.

(Information security management)

Article 2 According to the provisions of this outline, information security management (measures related to information security stipulated in Article 9 (hereinafter, in order to ensure the confidentiality, completeness and availability of information assets and contribute to the safe life of residents) It means to set up a person who has the authority and responsibility to implement (referred to as "security measures") according to the role, and to implement, maintain and improve security measures according to the importance of information assets. .) Is carried out.

2. In implementing the information security management (hereinafter referred to as "security management") prescribed in the preceding paragraph, establish a security management system, and plan (Plan), implementation (Do), evaluation (Check), and review (Action). Activities at the stage should be defined, these activities should be reviewed regularly and repeated.

3. The Chief Information Security Officer (hereinafter referred to as the "Chief Information Security Officer") stipulated in Article 11, Paragraph 1 shall carry out management reviews (plans) in accordance with the provisions of Article 11, Paragraph 6 when implementing security management. It means to confirm from the viewpoint of the effectiveness of the security measures whether the security measures are implemented based on the above and whether the results specified in the plan are obtained. The same shall apply hereinafter).

4 In order to handle information assets appropriately, information security management operation (education and enlightenment on information security, self-inspection, audit,

risk management, management of security accidents, etc. The management of persons, etc. The same shall apply hereinafter.)

(Definition)
Article 3 The meaning of the terms in this outline shall be as stipulated in the Nerima Ward Personal Information Protection Ordinance (March 2000 Nerima Ward Ordinance No. 79) and the management regulations, as well as the following.

(1) Confidentiality This means ensuring that only those who are authorized to use information assets can use the information assets.
(2) Integrity This means ensuring that information assets have not been leaked, destroyed, falsified or erased.
(3) Availability It means ensuring that a person who is authorized to use information assets can use information assets without interruption when necessary.

(4) Department Nerima Ward Organization Ordinance (April 1965 Nerima Ward Ordinance No. 4) Room and Department stipulated in Article 1, Nerima Ward Accounting Management Office Establishment Regulations (June 2007 Rule No. 74) No. Room prescribed in Article 1, Nerima Ward Board of Education Secretariat Organization Regulations (March 1992 Nerima Ward Education Committee Regulation No. 1) Department prescribed in Article 2, Nerima Ward Election Management Committee Regulations (Showa 39) July 1964 Nerima Ward Election Administration Committee Instruction A No. 1) Secretariat stipulated in Article 14 and Nerima Ward Audit Committee Ordinance (April 1964 Nerima Ward Ordinance No. 3) stipulated in Article 6 , Nerima Ward Agricultural Committee Secretariat Administrative Regulations (December 1973 Nerima Ward Agricultural Committee Decision) Article 2 Secretariat and Nerima Ward Assembly Secretariat Ordinance (March 1973 Nerima Ward Ordinance No. 9) ) The secretariat stipulated in Article 1.
(5) Organization Refers to the department specified in the previous item and the section specified in Article 2, Item 1 of the Management Regulations.
(6) General manager means the general manager of the department specified in No. 4 and the person specified in Article 4 of the Nerima Ward Organization Regulations (Rule 33, December 1973).
(7) Employees General and special employees who belong to the organization stipulated in Employee No. 5 and employees who are approved by her curity officer.
(8) Consignment business, etc. Refers to those who handle information assets of the ward

among those approved by the consignment business, designated manager, or chief information security officer.
(9) Person in charge of clerical work Among the staff and employees of consignment businesses, etc., the person in charge of clerical work that handles the management specific personal information, etc. prescribed in Item 10.
(10) Management Specific Personal Information, etc. Law Concerning the Use of Management Specific Personal Information and Numbers for Identifying Specific Individuals in Administrative Procedures stipulated in Article 2, Item 4 of the Nerima Ward Personal Information Protection Ordinance (2013 Law) No. 27. Hereinafter referred to as "numbering method") Refers to the personal number specified in Article 2, Paragraph 5.
(11) Implementation procedure This shows the implementation procedure of security management related to information assets under the jurisdiction of the section, and is created by each information security officer.
(12) Threats Leakage, destruction, falsification, erasure, etc. of information assets due to intrusion by outsiders, unauthorized access, virus attacks, and taking out of information assets.
(13) Information security accidents, etc. Refers to the following cases.
A. When a threat has occurred or is likely to occur
B. When the fact that the staff or the consignment business violates the laws and regulations stipulated in Article 8 or the Nerima Ward Information Security Policy (hereinafter referred to as "security policy") or signs of these are found.

(14) Emergency response plan Created by each information security officer and managed by the chief information security officer as an accident response procedure that shows individual and specific response methods when an information security accident occurs in each section. It means something that does.
(15) Special notes on the protection and management of personal information and information security "Special notes on the protection and management of entrusted information", "Special notes on the protection and management of information in designated management", "Protection of information in worker dispatch contracts" And "Special notes on management", "Special notes on information protection and management in finance leases", "Special notes on information protection and management in maintenance leases" and "Special notes on protection and management of specific personal information" It means the one specified by the general information security manager.

(16) General education This refers to education and enlightenment of staff and contractors regarding basic matters required for the implementation of security management pursuant to the provisions of Article 23.
(17) Workplace education This refers to education and enlightenment of staff and contractors regarding matters required for handling information assets in each section pursuant to the provisions of Article 23.

(Scope of application)
Article 4 The scope of application of the security policy shall be as follows.
(1) Information assets that require management to be protected from leakage, destruction, falsification, erasure, etc.
(2) Organization
(3) Staff and consignment businesses, etc.

(Obligation to comply with staff)
Article 5 Employees must have a common understanding of the importance of information security and comply with security policies, implementation procedures and emergency response plans in carrying out their duties.
2. Of the staff, the person in charge of clerical work must handle the managed specific personal information, etc. strictly based on the security policy, implementation procedure, other related rules, and instructions of the information security officer.
3 Employees must take general education and, if deemed necessary, take workplace education.
4 Employees must carry out self-inspection (hereinafter referred to as "self-inspection") regarding information security prescribed in Article 24.
5 Employees must cooperate in the implementation of information security audits (hereinafter referred to as "audits") prescribed in Article 25 and information security risk management (hereinafter referred to as "risk management") prescribed in Article 26. It doesn't become.
6. When an employee becomes aware of an information security accident, etc. (hereinafter referred to as "security accident, etc."), he / she must respond in accordance with the provisions of the separately stipulated procedure and the description of the emergency response plan.
7. Employees must manage the consignment business operators, etc. prescribed in Article 28.

(Business consignment)
Article 6 When the ward consigns (including the case where the designated manager in the designated manager system manages it. The same shall apply hereinafter), the consignment business operator, etc. manages the safety of information assets equal to or higher than the ward. After confirming in advance that the measures will be taken, the contractor must be selected appropriately.
When the two wards outsource, they have a common understanding of the importance of information security among the outsourced businesses, etc., and when carrying out their business, they have a security policy and implementation procedures, as well as "special notes on the protection and management of personal information and information security. It must be stipulated in contracts, agreements, etc. that compliance with "matters" (hereinafter referred to as "special notes").
3 When the ward outsources, if the outsourcer subcontracts, unless it is confirmed in advance that the subcontractor will take safety management measures equal to or higher than the ward, the subcontractor will be subcontracted. Do not approve. The same shall apply to consignment acts after subcontracting.
4 When subcontracting or consignment after subcontracting (hereinafter referred to as "subcontracting, etc.") is performed pursuant to the preceding paragraph, the consignment company, etc. is the subcontractor and the consignee after subcontracting (hereinafter, "subcontractor, etc."). It is necessary to supervise whether necessary and appropriate supervision is being carried out.

(Consignment of business from Tokyo and the national government)
Article 7 When entrusted by the Tokyo Metropolitan Government and the national government, we request the Tokyo Metropolitan Government and the national government to implement security measures equal to or higher than the security policy of the ward, and shall stipulate in contracts and agreements. ..

(Legal compliance)
Article 8 Employees must comply with and comply with the following laws and regulations when handling information assets in their duties.
(1) Local Public Service Law (Law No. 261 of 1950)
(2) Copyright Law (Law No. 48 of 1970)
(3) Law Concerning Prohibition of Unauthorized Access Act (Law No. 128 of 1999)
(4) Law Concerning Protection of Personal Information (Law No. 57 of 2003)
(5) Number method

(6) Nerima Ward Personal Information Protection Ordinance

When the 2nd ward is entrusted with business from Tokyo, the national government, etc., the staff must comply with and comply with the following laws and regulations when handling information assets.
(1) Local Civil Service Law
(2) Copyright law
(3) Law Concerning Prohibition of Unauthorized Access
(4) Law Concerning Protection of Personal Information
(5) Number method
(6) Other laws or ordinances regarding the protection of personal information stipulated by the Tokyo Metropolitan Government and the national government, etc.

3. If an employee violates the security policy and other related regulations, he / she will be subject to disciplinary action, etc., based on the Local Public Service Law and other related laws and regulations, depending on the seriousness of the violation and the situation of the incident that occurred.

(4) When handling information assets in the outsourced business, the consignment business operator, etc. must comply with and comply with the following laws and regulations as well as related laws and regulations.
(1) Copyright law
(2) Law Concerning Prohibition of Unauthorized Access
(3) Law Concerning Protection of Personal Information
(4) Number method
(5) Nerima Ward Personal Information Protection Ordinance

5 If the outsourced business operator violates the security policy, strict measures shall be required based on relevant laws and contracts, contracts, etc., depending on the seriousness of the violation and negligence.

(Information security measures)
Article 9 In order to protect information assets from threats, the following information security measures will be implemented as specified separately.
(1) Physical security measures Physical security measures such as management of information system equipment, restrictions on controlled areas, and clarification of areas

where office work for handling managed specific personal information (hereinafter referred to as "handling areas") are carried out.
(2) Human security measures Human measures by staff compliance, user management, consignment management, etc.
(3) Technical security measures Technical measures such as computer virus countermeasures and unauthorized access countermeasures
(4) Operational measures for information systems Operational measures required from the development stage to the operation stage of information systems
2. In implementing the information security measures prescribed in the preceding paragraph, the level of security required for information assets from the viewpoint of confidentiality, integrity and availability must be determined and classified according to their importance, as specified separately. Must be. (Collection of information related to information security, etc.)

Article 10 In order to prevent security accidents and implement effective and efficient operation of security measures, information on threats, etc. must be collected and shared.

Chapter 2 Security Management Promotion System
(Chief Information Security Officer)
Article 11 A chief information security officer shall be appointed to comprehensively implement security management.
2 The Chief Information Security Officer has the ultimate authority and responsibility for information security.
3 The Chief Information Security Officer shall be the Deputy Mayor in charge of the Planning Department (hereinafter referred to as the "Deputy Mayor").
4 The Chief Information Security Officer shall make comprehensive coordination of the organization in implementing security management.
5 The Chief Information Security Officer conducts and approves management reviews on the following matters.
(1) Annual operation plan for security management
(2) Report on the measurement of results and effects related to general education
(3) Report of self-inspection results and measurement of effects
(4) Report of audit results
(5) Implementation status of risk management related to risks confirmed by the results of audits
(6) Results of risk management

(7) Report on security accidents, etc.
(8) Report on management of consignment companies, etc.
(9) Implementation status of security management

6 The Chief Information Security Officer shall respond to security accidents, etc., and manage the formulation of emergency response plans in the ward in accordance with the provisions of the guidelines specified separately.
7. The Chief Information Security Officer shall provide guidance and advice in conducting the management review pursuant to the provisions of Paragraph 5.

(Highest Information Security Advisor)
Article 12 A Chief Information Security Advisor may be appointed as a person who assists the duties of the Chief Information Security Officer from a professional standpoint.
2 The Supreme Information Security Advisor is commissioned by the ward mayor from among those who have specialized knowledge and experience in security management.
3. Notwithstanding the provisions of the preceding paragraph, when the highest information security advisor business is outsourced to a corporation or other organization (hereinafter referred to as "corporation, etc."), the corporation, etc. entrusted with the business has excellent insight into security management. The person who reported as is the highest information security advisor.
4 The Supreme Information Security Advisor can give advice, etc. from a professional standpoint regarding the security management of the ward.

(Information security auditor)
Article 13 An information security audit manager shall be appointed as a person who has the authority and responsibility for conducting audits.
2. The information security audit manager shall be appointed by the chief information security officer from the department manager or section manager who can ensure the fairness of the audit.
3. The information security audit manager shall carry out the following matters regarding the audit.
(1) To formulate an audit plan
(2) Approve the result of the audit.
(3) Report the results of the audit to the Chief Information Security Officer.

(General Information Security Manager)
Article 14 A general information security manager shall be appointed as a person to assist the chief information security officer.
2 The person in charge of general information security management shall be the general manager of the planning department.
3 The general information security manager will provide general education.
4. The general information security manager shall report the following matters to the chief information security officer.
(1) Results of general education
(2) Results of self-inspection
(3) Results of risk management
(4) Management status of consignment companies, etc.

5 The general information security manager shall respond to security accidents, etc. in accordance with the provisions of the separately established guidelines and the description of the emergency response plan.
6 The general information security manager cooperates with the information security audit manager to carry out audit-related duties.

(General information system administrator)
Article 15 The general information system administrator (hereinafter referred to as "general information system administrator") stipulated in Article 10, Paragraph 1 of the Management Regulations assists the general information security manager from a professional perspective on information systems. ..
2. The general information system administrator shall implement the following matters regarding the information security of the resident information system, the in-house infrastructure system and the common infrastructure stipulated in Article 10, Paragraph 3, Item 3 of the Management Regulations.
(1) Thing about workplace education.
(2) Risk management related to risks confirmed by the results of audits
(3) Respond to security accidents, etc. in accordance with the provisions of the guidelines specified separately.
(4) Regularly check the status of compliance with the security policy.
(5) Responsible for the practice of formulating and reviewing emergency response plans.

3. The general information system administrator must take necessary measures to

improve and correct the guidance and improvement requests and the matters recommended for correction regarding the information security management operation (hereinafter referred to as "security management operation"). ..

(General information security manager)

Article 16 A general information security manager shall be appointed to assist the general information security manager from a professional perspective on information security.

2 The general information security manager shall be the information policy section chief.

3 The general information security manager gives guidance and advice on security management operations and security measures.

4 The general information security manager compiles reports on the results and effects of general education and reports them to the general information security manager.

5 The general information security manager summarizes the results of the self-inspection and reports it to the general information security manager.

6 The general information security manager responds to security accidents, etc. that occur in each section in accordance with the provisions of the guidelines specified separately and the description of the emergency response plan.

7. The general information security manager must collect information on security accidents, etc. and disseminate it to the relevant organizations as necessary.

8. The general information security manager summarizes the management status of the consignment business operator, etc., and reports it to the general information security manager.

9 The general information security manager is in charge of the affairs related to auditing.

(Information security manager)

Article 17 An information security manager shall be appointed to carry out security management in each department.

2 The person in charge of information security management shall be the general manager.

3 The information security manager has the authority and responsibility for the security measures of the department.

4. The information security manager must direct and supervise the information security manager to properly manage information assets and implement appropriate security measures when handling information assets.

5. The information security manager shall direct and supervise the following matters regarding security management in the department.

(1) Thing about security measures of the staff to which it belongs.
(2) Development, setting change, operation, update, etc. of the information system under the jurisdiction.
(3) Regularly grasp the compliance status of the security policy of employees and contractors.
(4) Management of clerical staff To regularly grasp the handling status of specific personal information, etc.

6. The information security manager shall direct and supervise the following matters in order to properly implement the security management operation in the department.
(1) To grasp the attendance status of general education and workplace education, and to implement workplace education regarding the handling of information assets under the jurisdiction as necessary.
(2) To secure opportunities for staff and contractors to take general education.
(3) To grasp the implementation status of self-inspection.
(4) If you are subject to an audit, cooperate in conducting the audit.
(5) To understand the implementation status of risk management regarding risks confirmed by the results of audits.
(6) Approve the results of risk management and report to the general information security manager on a regular basis.
(7) Respond to security accidents, etc. in accordance with the provisions of the guidelines specified separately and the description of the emergency response plan.
(8) To understand the management status of outsourced businesses.

7. The information security manager shall take necessary measures to improve and correct the matters for which guidance and improvement requests and correction recommendations regarding security management operations have been made.

(Information security officer)
Article 18 An information security officer shall be appointed to carry out security management in each section.
2 The person in charge of information security shall be the section chief. However, in the case of a section that has a section chief in charge, the section chief in charge may be the person in charge of information security for the part related to the office work in charge, as determined by the section chief.
3. The information security officer has the authority and responsibility to implement

security measures when developing, changing, operating, and updating the information system under the jurisdiction of the section.

4. The information security officer must take responsibility for managing information assets in the section and implement appropriate security measures when handling information assets.

5 The information security officer must confirm the following matters regarding security management in the section.

(1) Thing about creation, maintenance and management of implementation procedure to affect management specific personal information, etc. under the jurisdiction of section.

(2) Create, maintain and manage implementation procedures for information assets other than those specified in the previous item.

(3) Create, maintain and manage an emergency response plan.

(4) Thing about security measures of the staff to which it belongs.

(5) Development, setting change, operation, update, etc. of the information system under the jurisdiction.

(6) Thing about compliance situation of security policy such as staff and consignment business.

(7) Management of clerical staff To regularly grasp the handling status of specific personal information, etc.

6. The information security officer must implement the following matters in order to properly implement the security management operation in the section.

(1) To grasp the attendance status of general education and workplace education, and to implement workplace education regarding the handling of information assets under the jurisdiction as necessary.

(2) To secure opportunities for staff and contractors to take general education.

(3) To grasp the implementation status of self-inspection.

(4) If you are subject to an audit, cooperate in conducting the audit.

(5) Thing about risk management about risk confirmed by the result of audit.

(6) Periodically report the implementation status of risk management to the person in charge of information security management.

(7) Respond to security accidents, etc. in accordance with the provisions of the guidelines specified separately and the description of the emergency response plan.

(8) To understand the management status of outsourced businesses.

7. The information security officer shall take necessary measures to improve and correct

the matters for which guidance and improvement requests and correction recommendations regarding security management operations have been made.
8. When dealing with managed specific personal information, etc. among important information, the information security officer must implement the following matters.
(1) Clarify the person in charge of clerical work (excluding consignment businesses, etc.).
(2) Nerima Ward Personal Information Protection Ordinance Enforcement Regulations (March 2000 Nerima Ward Regulation No. 42) Personal Information Business Registration Form stipulated in Article 3, Paragraph 1 and stipulated in Article 4, Paragraph 1 of the same Regulation The previous issue so that the affairs can be properly executed within the scope shown in the personal information file registration slip and the Nerima Ward Personal Number-related affairs specific personal information handling guidelines (Nerima Ward, November 4, 2015, Nerima General Affairs No. 1325). To direct and supervise the person in charge of clerical work prescribed in.
(3) When the ward consigns or when the consignment is subcontracted, it is necessary to confirm in advance that the consignment company, etc. and the subcontractor, etc. will take safety management measures for information assets equal to or higher than the ward. ..
(4) When the ward consigns, make the consignment business, etc. clarify the person in charge of clerical work, and supervise the consignment business, etc. so that proper clerical work is performed.
(5) In the case of the previous item, when subcontracting, etc. is carried out, the person in charge of clerical work should be clarified at the subcontracting party, etc. To supervise.
(6) Clarify the handling area and manage it appropriately.

(Information security officer)
Article 19 In each section, one or more information security officers shall be assigned to each section as persons responsible for the implementation of security management under the direction of the information security officer, and one of the information security officers concerned. Will be the general affairs chief.
(2) In the case of the preceding paragraph, if two or more information security officers are assigned, the following persons shall be assigned in addition to the general affairs chief in the same paragraph.
(1) In the section where the chief-level staff is assigned as the head of the facility, etc., the chief-level staff concerned. However, if multiple chief-level staff are assigned to the facility, etc., the person in charge of information security shall be appointed from among them.

(2) In addition to the persons listed in the previous item, persons appointed by the information security officer (IT Promotion Headquarters) Article 20 The IT Promotion Headquarters shall be based on the provisions of Article 6, Paragraph 6 of the Management Regulations, Item 4 of the same paragraph. The following matters will be investigated and deliberated as matters deemed necessary by the general manager of the headquarters prescribed in.
(1) Review of this outline and countermeasure standards, and approval of the review
(2) Review of matters necessary for implementing security management and approval of the review
(3) Thing about proposal from security committee.

(Information Security Committee)
Article 21 An Information Security Committee will be established to formulate and promote measures related to security measures.
2 The Security Committee shall consist of a chairman, a vice chairman and members.
3 The chairman shall be the director of the planning department, and the vice chairman shall be the director of the information policy section.
4 Committee members shall be those in the positions listed in the attached table.
(5) When the chairman finds it necessary, he / she may request the security committee to attend, hear opinions, or request explanations from persons other than the members listed in the preceding paragraph.
6. The chairperson shall promptly report the results of the investigation and deliberation by the Security Committee to the Chief Information Security Officer, and seek judgment and instructions as necessary.
7. The Security Committee shall implement the following matters.
(1) Thing about review of this outline and measures standard.
(2) Thing about review of matters necessary for implementation of security management.
(3) Preparation of draft security management operation plan
(4) Examination of proposals to the IT Promotion Headquarters
(5) Examination of security accidents, etc.
(6) Deliberation on the proposal from the CSIRT
(7) Deliberation on classification of information systems
(8) Other matters related to information security.

8 The general affairs of the committee will be handled by the Information Policy Division.

(CSIRT)
Article 22 Nerima Ward CSIRT Installation Guidelines (2017) as an emergency response system to accurately grasp and analyze the situation when a security accident occurs, prevent the spread of damage, and perform recovery promptly and accurately. March 1st, 28th, CSIRT will be established by Nerima No.).

Chapter 3 Security Management Operation
(Education and enlightenment on information security)
Article 23 In order to raise awareness and understanding of information security while recognizing the authority and responsibility for implementing security management, information security is provided to staff and contractors on a regular or necessary basis. To carry out education and enlightenment.

(Self-inspection regarding information security)
Article 24 In order to ensure the effectiveness of security measures by measuring the effects of education and enlightenment prescribed in the preceding article, grasping the status of own security measures and promoting self-improvement, regularly or as necessary. , Carry out self-inspection regarding information security.

(Audit on information security)
Article 25 In order to ensure the effectiveness of security measures by evaluating the implementation status of security measures and ordering corrections, the implementation status of security measures in each section is audited regularly and as necessary regarding information security. To carry out.

(Risk management related to information security)
Article 26 For risks identified by the results of audits, risk management related to information security will be implemented in order to implement appropriate security measures according to the risks.

(Management of information security accidents, etc.)
Article 27 In the event of a security accident, etc., we will respond promptly, prevent the occurrence and spread of damage, record and save the history of security accidents, etc., and share it with the organization to prevent its recurrence. Therefore, we will manage security accidents.
2 Specific matters related to the management of security accidents, etc. shall be specified

separately and described in the emergency response plan.
3 In the event of a security accident, etc., the use of information assets can be restricted as necessary by taking into consideration the response to the accident, the content of the accident, the scope of responsibility, etc.

(Management of consignment companies, etc.)
Article 28 To confirm the security policy and implementation procedure of the consignment business operator handling the information assets of the ward and the compliance status of the special notes, the consignment business operator, etc. will be managed.

Chapter 4 Supplementary Provisions
(Review of security management, etc.)
Article 29 The security management and security management operation plan must be reviewed so that they can be implemented effectively and efficiently, reflecting the changes in the situation surrounding information security in the ward and the following matters.
(1) Operational status of security management operation
(2) Compliance with security policy
(3) Appearance of new threats
2. In the case of a review pursuant to the provisions of the preceding paragraph, the security policy and related regulations shall be reviewed as necessary.

(Delegation)
Article 30 In addition to what is stipulated in this outline, necessary matters shall be stipulated separately.