Appendix 5 Matters for Implementation by Government Agencies with Level C Cyber Security Responsibility

Institutional Aspect	Item	Sub-Item	Content to be Implemented
Management	Classification and security baselines of information and communication systems		The government agency shall classify information and communication systems developed by itself or through outsourcing in accordance with Appendix 9 and implement the control measures set out in Appendix 10; thereafter, the government agency shall review the appropriateness of the classification and security baselines of such systems at least once a year.
	Implementation of information security management systems		All core information and communication systems shall implement information security management system standards, such as CNS 27001 or ISO 27001, other systems or standards with equal or greater effect, or other standards developed by government agencies and recognized by the competent authority, and shall continuously maintain the implementation.
	Dedicated cyber security personnel		Appoint at least one person.
	Internal cyber security audits		Conduct once every two years.
	Business continuity plan drill		Conduct once every two years for all core information and communication systems.
Technology	Security testing	Vulnerability scanning	Conduct once every two years for all core information and communication systems.
		Penetration testing	Conduct once every two years for all core information and communication systems.
	Cyber security health check	Review of network architecture	Conduct once every two years.
		Review of malicious network activities	
		Review of malicious activities on user endpoint computers	
		Review of malicious activities on server hosts	
		Review of directory service system settings and firewall connection settings	
	Cyber security vulnerability management		1. When becoming aware of a cyber security vulnerability, the government agency shall

			carry out timely patching or take mitigation measures. 2. The government agency shall implement vulnerability management operations in the manner designated by the competent authority and continue to operate and maintain them.
	Cyber security protection	Anti-virus software	The government agency shall enable the various cyber security protection measures, continue to use them, and timely carry out the necessary software and hardware updates or upgrades.
		Network firewalls	
		A government agency with email servers shall have email filtering mechanisms	
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each person shall receive at least 12 hours of cyber security professional training or cyber security competency training each year.
		Information personnel other than dedicated cyber security personnel	Each person shall receive at least three hours of cyber security professional training or cyber security competency training every two years, and at least three hours of general cyber security education each year.
		General users and supervisors	Each person shall receive at least three hours of general cyber security education each year.
	Cyber security professional certificates and competency training certificates		Each dedicated cyber security person shall hold at least one professional certificate and at least one competency training certificate, and shall continuously maintain the validity of both.

Notes:

1. Where an information and communication system is of a shared nature, the government agency primarily in charge of the establishment, maintenance, or development of such system shall determine whether it is a core information and communication system.
2. “Dedicated cyber security personnel” refers to personnel who shall perform cyber security duties on a full-time basis; that is, cyber security is their primary core duty and shall be handled with priority. “Information personnel other than dedicated cyber security personnel” refers to other personnel who actually engage in cyber security duties or information affairs.
3. In conducting “cyber security health check” of this Appendix, in addition to implementation of the items, contents, and timeframes specified in this Appendix, the government agency may take other measures which have equal or better effects as recognized by the competent authority.
4. “Cyber security vulnerability management” refers to operations that integrate information asset

management and vulnerability management, comprehend the overall risk landscape, and assist agencies in implementing the required matters under the Act concerning asset inventory and risk assessment.

5. “Cyber security professional certificates” refers to cyber security professional certificates announced by the competent authority.
6. “Cyber security competency training certificates” refers to certificates issued to persons who have passed the cyber security competency assessment conducted by the competent authority.
7. Implementation Deadlines for Required Matters
   (1) Classification and security baselines of information and communication systems: This matter shall be completed in accordance with Appendix 9 within one year after initial approval or a change in cyber security responsibility level, and the control measures set out in Appendix 10 shall be completed within two years; the same shall apply when an information and communication system is added, when the system classification is modified, or when the applicable security baselines are updated.
   (2) Implementation of information security management systems: Within two years after initial approval or a change in cyber security responsibility level, information security management systems shall be implemented for all core information and communication systems.
   (3) Cyber security vulnerability management: The implementation shall be completed within two years after initial approval or a change in cyber security responsibility level.
   (4) Cyber security protection: Activation shall be completed within one year after initial approval or a change in cyber security responsibility level, and the protective measures shall continue to be used.
   (5) Appointment of dedicated cyber security personnel, cyber security education and training, and cyber security professional certificates and competency training certificates: These matters shall be completed within one year after initial approval or a change in cyber security responsibility level; the same shall apply when there are personnel changes.
   (6) Other required matters shall be handled in accordance with this Appendix starting from the year following initial approval, a change in cyber security responsibility level, or a change to a core information and communication system.