Appendix 4 Matters for Implementation by Specific Non-Government Agencies with Level B Cyber Security Responsibility

Institutional Aspect	Item	Sub-Item	Content to be Implemented
Management	Classification and security baselines of information and communication systems		The specific non-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 specific non-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 and certification by an impartial third party		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; certification by an impartial third party shall be completed, and the validity of such certification shall be continuously maintained.
	Dedicated cyber security personnel		Appoint at least two personnel
	Internal cyber security audits		Conduct once a year.
	Business continuity plan drill		Conduct once every two years for all core information and communication systems.
	Cyber security governance maturity assessment		The critical infrastructure provider shall conduct it once a year.
Technology	Security testing	Vulnerability scanning	Conduct once a year 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	

		Database security review of core information and communication systems	
	Cyber security monitoring and management mechanism		The specific non-government agency shall establish a cyber security monitoring and management mechanism, continuously maintain and operate it, and submit monitoring and management data in the manner designated by the competent authority. The monitoring scope shall include the implementation contents of the "Endpoint Detection and Response Mechanism" and "Cyber Security Protection" specified in this Appendix, as well as the log records of directory service systems and core information and communication systems, and records of information and communication equipment.
	Cyber security vulnerability management		1. When becoming aware of a cyber security vulnerability, the specific non-government agency shall carry out timely patching or take mitigation measures. 2. The critical infrastructure provider shall implement vulnerability management operations in the manner designated by the competent authority and continue to operate and maintain them.
	Endpoint Detection and Response (EDR) mechanism		The specific non-government agency shall complete implementation of the Endpoint Detection and Response (EDR) Mechanism, continue to operate and maintain it, and submit detection data in the manner designated by the competent authority.
	Cyber security protection	Anti-virus software	The specific non-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 specific non-government agency with email servers shall have email filtering mechanisms	
		Intrusion detection and prevention mechanism	

		A specific non-government agency with core information and communication systems providing external services shall have web application firewalls	
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 or competency training certificates		Each dedicated cyber security person shall hold at least one professional certificate or competency training certificate, and shall continuously maintain the validity of the certificate.

Notes:

1. Where an information and communication system is of a shared nature, the 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. "Third party" as used in "certification by an impartial third party" refers to an institution accredited by a body commissioned by the competent authority under the Standards Act of the Republic of China; the certificate issued by such third party shall bear the accreditation mark of the aforementioned commissioned body.
3. "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.
4. In conducting "cyber security health check" of this Appendix, in addition to implementation of the items, contents, and timeframes specified in this Appendix, the specific non-government agency may take other measures which have equal or better effects as recognized by the central competent authority in charge of the relevant sector.
5. "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.
6. "Endpoint Detection and Response (EDR) mechanism" refers to protective operations that provide proactive endpoint scanning and detection, vulnerability protection, analysis of suspicious programs or anomalous activities, and presentation of the severity of related threats.
7. "Cyber security professional certificates" refers to cyber security professional certificates announced by the competent authority.
8. "Cyber security competency training certificates" refers to certificates issued to persons who have

passed the cyber security competency assessment conducted by the competent authority.

9. The central competent authority in charge of the relevant sector of a specific non-government agency may, as required by actual needs and within the scope of these Regulations, separately prescribe the cyber security required matters for the specific non-government agencies under its jurisdiction.
10. Implementation Deadlines for Required Matters
    (1) Classification and security baselines of information and communication systems: This matter shall be completed within one year after initial approval or a change in cyber security responsibility level; 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 and certification by an impartial third party: 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, and certification by an impartial third party shall be completed within three years.
    (3) Cyber security monitoring and management mechanism, cyber security vulnerability management, and endpoint detection and response mechanism: The implementation shall be completed within one year 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 or 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.