

Schedule 2: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A

| System aspect | Items conducted | Sub-items conducted | Contents conducted |
|-------------------|---|------------------------|---|
| Management aspect | Classification of levels and defense standards of the information and communication system | | Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year. |
| | The importation of the information security management system and verification by a impartial third party | | Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification. |
| | Dedicated cyber security personnel | | Within one year after receipt of initial approval or change of levels, the specific non-government agency shall deploy four persons. |
| | Internal cyber security audits | | Conduct twice a year |
| | Business sustainable operation rehearsal | | Conduct once a year for all core information and communication systems |
| Technical aspect | Security detection | Vulnerability scanning | Conduct twice a year for all core information and communication systems |

| | | | |
|--|---|---|--|
| | | Penetration test | Conduct once a year for all core information and communication systems |
| | Cyber security health diagnosis | Inspection of network frameworks | Conduct once a year |
| | | Inspection of malicious cyber activities | |
| | | Inspection of malicious activities in user terminal computers | |
| | | Inspection of malicious activities in servers | |
| | | Inspection of settings of directory servers and settings of firewall connection | |
| | Cyber security threat detection management mechanism | | Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof. The monitoring scope shall include the contents conducted for “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application. |
| | Vulnerability alert and notification system mechanism | | 1. Within one year after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory |

| | | | |
|---------------|------------------------|--|---|
| | | | <p>data of information assets in the manner designated by the competent authority.</p> <p>2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the critical infrastructure provider shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.</p> |
| | Cyber security defense | Anti-virus software | <p>Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.</p> |
| | | Network firewalls | |
| | | If the specific non-government agency has email servers, it should have email filtering mechanisms | |
| | | Intrusion detection and defense mechanism | |
| | | If the specific non-government agency has core information and communication systems for external services, it should have the application firewalls | |
| | | Defense measures for advanced persistent threat attacks | |
| Awareness and | Cyber | Dedicated cyber | Each personnel shall receive the |

| | | | |
|----------|--------------------------------------|---|--|
| training | security education and training | security personnel | cyber security professional program training or the cyber security competence training for not less than twelve hours each year. |
| | | Information personnel other than dedicated cyber security personnel | Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year. |
| | | General user and officer | Each year, each person shall receive the general cyber security education training for not less than three hours |
| | Cyber security professional licenses | | <ol style="list-style-type: none"> 1. Within one year after receipt of initial approval or change of levels, at least four dedicated cyber security persons shall each hold one or more licenses, and shall continually maintain the validity of licenses. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments. |

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the

grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.

5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
6. The central authority in charge of relevant industry of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.