Schedule 10: Defense standards of cyber systems

Defense requirements of systems Levels Control measures		High	Medium	Common
Dimension	Contents of the measures			
Access control	Account management	1. The agency shall define the idle time or usable duration of each system and the use status and condition of information and communication system. 2. When the permitted idle time prescribed by the agency or usable time is exceeded, the system should automatically logout the users. 3. Use the information and communication system according to the circumstances and conditions prescribed by the agency. 4. Monitor the information and communication system accounts; report to the administrator if any abnormal use by an account is found 5. All control measures for the level of "medium".	1. The temporary or emergent accounts which have expired should be deleted or prohibited. 2. The idle accounts of information and communication system should be prohibited. 3. Periodically review the application, establishment, revision, activation, suspension and deletion of accounts of information and communication systems. 4. All control measures for the level of "common".	Establish the account management mechanism, including the procedure for application, establishment, revision, activation, suspension and deletion.
	Least privilege	The principle of least privilege is adopted. The users(or the procures for acts on behalf of users)are granted authorized access required for the completion of duties only, depending on the duties and business functions of the		No requirement

		agencies .	
	Remote access	1. Any remote connection with the cyber system should be monitored. 2. The cyber system should adopt encryption mechanisms. 3. The source of remote access to the cyber system should be the access control point as pre-defined and managed by the agencies. 4. All control measures for the level of "common".	1. For each kind of permitted remote access, the authorization should be obtained in advance; the use restriction, configuration requirement, connection requirement and documentation should be established. 2. The inspection operation of users' privilege should be completed at the server terminal. 3. The remote access to intranet of the agency or the connection to the information and communication system back office should be monitored. 4. Encryption mechanism should be adopted.
Event log and accountability	Record events	1. The log generated by the information and communication system which is retained by the agency should be reviewed periodically. 2. All control measures for the level of "common".	1. Stipulate the time cycle of records in the logs and retention policy and retain the logs for at least six months. 2. Assure that the information and communication system has the function of record of specific events, and determine the specific information and communication system incidents to be recorded. 3. Should record various functions

				executed by the administrator account of the information and communication system.
	Content of log record	The log generated by the information and communication system shall include the type of incidents, dates of occurrence, places of occurrence, and the information about the identification of the users relating to the incidents; the single log mechanism should be adopted to assure the consistency of the formats of output, and other relevant information shall be included in accordance with the cyber security policy and requirements of laws and regulations.		
	Storage capacity of the log	Storage capacity required for the log shall be equipped depending on the requirement of the storage of the log.		
	Response to failure in log process	1. Upon occurrence of the event of failure in log process which should be reported immediately as required by the agency, the information and communication system should give warnings to the specific personnel within the timeframes prescribed by the agency. 2. All control measures for the levels of “medium” and “common”.		In case of failure in log process, the information and communication system should take appropriate actions.
	Time stamp and time calibration	1. The internal clock of the system should periodically synchronize with the time cycle specified by the agency and the source of standard times. 2. All control measures for the level of “common”.		The information and communication system should use the internal clock of the system to generate time stamps required for the log, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).
	Protection of log information	1. Periodically back up the log to the physical system different from the original audit system. 2. All control measures for the level of “medium”	1. Should use the integrity of the hashing or other proper methods to assure the mechanism. 2. All control measures for the level of “common”.	The access management of the log is limited to the users with privileges.
Business continuity plan	Backup of system	1. Should take the backup and restore as a part of the testing of the business continuity plan. 2. Should store the important software	1. Should periodically test the backup information to verify the reliability of the backup media and the integrity of the information. 2. All control measures	1. Set the requirement for tolerable time of information loss of the system. 2. Execute the system source codes and the data backup.

		of the information and communication system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 3. All control measures for the level of "medium".	for the level of "common".	
	System rescue	1. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 2. When the original service interrupts, the service is provided by the rescue equipment or other method in lieu thereof within the tolerable time.		No requirement
Audits and accountabilities	Audit events	1. Audit events should be reviewed periodically. 2. All control measures for the level of "common".		1. Retain audit records according to the prescribed time cycle and the policies of record retention. Assure that the cyber system has the function of audit of specific events, and determine the specific cyber system incidents to be audited. 2. Should audit various functions executed by the administrator account of the cyber system.
	Contents of audit records	1. Audit records generated by the cyber systems shall include other relevant information as required. 2. All control measures for the level of		Audit records generated by the cyber system shall include the type of incidents,

		“common”.		date of occurrence, place of occurrence, and information about the identification of the users relating to the incidents; single journal recording mechanisms should be adopted to assure the consistency of the formats of output.
	Storage capacity for the audits	Storage capacity required for the audit records shall be equipped depending on the requirement of the storage of audit records.		
	Response to failure in audit process	1. Upon occurrence of audit failure events, which should be reported immediately as required by the agencies, the cyber systems should give warnings to the specific personnel within the timeframes prescribed by the agencies. 2. All control measures for the levels of “medium” and “common”.		In case of failure in the audit process, the cyber systems should take appropriate actions.
	Time stamp and time calibration	1. The internal clock of the system should synchronize with the time cycle specified by the agencies and the source of standard times. 2. All control measures for the level of “common”.		The cyber systems should use the internal clock of the systems to generate time stamps required for audit records, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).
	Protection of log information	1. Periodically back up the log to the physical system different from the original audit system. 2. All control measures for the level of “medium”	1. Should use the integrity of the hashing or other proper methods to assure the mechanism. 2. All control measures for the level of “common”.	The access management of the log is limited to the users with privileges.
Business continuity plan	Backup of system	1. Should take the backup and restore as a part of the testing of	1. Should periodically test the backup information to verify the reliability	1. Set the requirement for tolerable time of information loss of the system.

		the business continuity plan. 2. Should store the important software of the information and communication system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 3. All control measures for the level of "medium".	of the backup media and the integrity of the information. 2. All control measures for the level of "common".	2. Execute the system source codes and the data backup.
	System rescue	1. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 2. When the original service interrupts, the service is provided by the rescue equipment or other method in lieu thereof within the tolerable time.		No requirement
Identification and authentication	Identification and authentication of internal users	1. Adopt multiple authentication technologies for the access to the information and communication system. 2. All control measures for the level of "medium" and "common".		The information and communication system should have the function of identification and authentication of sole agency users(or the program of act on behalf of agency users); common accounts are prohibited.
	Identity verification management	1. Identity verification mechanism should prevent from the logon by automatic program or the trials of change of password. 2. The password resetting mechanisms have verified identities of users again, and then send one-time and time-based tokens. 3. All control measures for the level of "common".		1. When using the preset password to login the system, should immediately change the password after logon. 2. Information relating to identity verification may not be transmitted by plain text. 3. Have the account lockout mechanism; if the identity verification for

			account logon fails for five times, disallow such account to continue the trial of logon at least within fifteen minutes, or use the failure verification mechanisms built by the agencies themselves. 4. While the password is used to conduct authentication, the least complexity of password should be imposed; and the restriction on the shortest and longest validity of passwords should be imposed. 5. In the event of change of password, at least the password may not be same as those used for previous three times. 6. The measures specified in points 4 and 5 may be conducted for non-internal users according to the regulations formulated by the agencies themselves.
	Authentication information feedback	The information and communication system should shield the information in the course of authentication.	
	Encryption module authentication	When the information and communication systems use the passwords for authentication, such passwords should be encrypted, or stored after hashing process.	No requirement
	Identification or authentication of non-internal users	The information and communication systems should identity and authenticate non-internal users (or the program of act on behalf of agency users).	
Access to systems and services	Requirement phase of system development life circle	Use the method of checklist to confirm system security requirements(including confidentiality, availability and integrity).	
	Design phase of system development life circle	1. Depending on the system functions and requirements, identify the threats that might impact on the system, to conduct risk analysis and assessment. 2. Feedback the risk assessment results	No requirement

<table>
<tr><td></td><td></td><td colspan="2">to the screening items of the requirement phase and submit the revision of security requirements.</td><td></td></tr>
<tr><td></td><td>Development phase of system development life circle</td><td colspan="2">1. Execute “source code scanning” security testing.
2. The system should have the notification mechanisms when serious error occurs.
3. All control measures for the level of “medium” and “common”.</td><td>1. Should practice necessary control measures for the security requirements.
2. Should pay attention to the avoidance of common software vulnerabilities, and practice necessary measures.
3. When errors occur, the user’s pages display short error message and code only, without detailed error message.</td></tr>
<tr><td></td><td>Testing phase of system development life circle</td><td colspan="2">10. Execute “penetration testing” security testing.
11. All control measures for the level of “medium” and “common”.</td><td>Execute “vulnerability scanning” security testing.</td></tr>
<tr><td></td><td>Deployment and maintenance operation phase of system development life circle</td><td colspan="2">1. In the maintenance operation phase of system development life circle, the version control and change management shall be implemented.
2. All control measures for the level of “common”.</td><td>1. Under the deployment environment, should conduct update and fixing of relevant cyber security threats, and close unnecessary services and ports.
2. Not to use preset passwords for information and communication system.</td></tr>
<tr><td></td><td>Outsourcing phase of system development life circle</td><td colspan="3">If the development of the information and communication system is outsourced, the security requirements by level (including confidentiality, availability, integrity) for each phase of system development life circle shall be included in the outsourcing contract.</td></tr>
<tr><td></td><td>Obtaining programs</td><td colspan="2">Development, testing, and formal operation environments should be separated.</td><td>No requirement</td></tr>
<tr><td></td><td>System documents</td><td colspan="3">Should store the documents relating to the management system development life circle.</td></tr>
<tr><td>Protection of systems and</td><td>confidentiality and integrity of</td><td>1. The information and communication system</td><td>No requirement</td><td>No requirement</td></tr>
</table>

communications	transmission	should adopt encryption mechanism, to prevent from unauthorized disclosure of information or to detect the change of information; unless there are substitutive physical protection measures in the course of transmission. 2. Use public, international institution verified and not cracked algorithms. 3. Support the maximum length key of algorithms. 4. Periodically change the encryption key or certification. 5. Should formulate the management regulations on the custody of key at server terminal, and implement security defense measures that should exist.		
	Securities of data storage	The important configuration setting file of the information and communication system and other relevant confidential information required for protection should be encrypted or stored by other appropriate method.	No requirement.	No requirement.
Integrity of systems and information	Vulnerability fixing	1. Periodically confirm the status of fixing of relevant vulnerabilities of the information and communication system. 2. All control measures for the level of "common".		The vulnerability fixing of the system should be tested for the effectiveness and potential impact, and should be updated periodically.
	Monitoring of information and communication system	1. The information and communication system should adopt automatic tools to monitor the access communication flows; if unusual or unauthorized activities are found, conduct the analysis of such activity. 2. All control measures for the level of "medium".	1. Monitor the information and communication system to detect the attack and unauthorized connection and to identify the unauthorized users of the information and communication system. 2. All control measures for the level of "common".	If a sign of hacking to the information and communication system is found, should notify the specific personnel of the agencies thereof.

	The integrity of software and information	1. Should conduct the inspection of the integrity of software and information. 2. All control measures for the level of “medium”.	1. Use the integrity verification tools to detect the unauthorized change of specific software and information. 2. The examination of the legitimacy of input data of users should be placed on the server terminal of the application system. 3. If any violation to the integrity is found, the information and communication system should implement the security defense measures designated by the agency.	No requirement

Notes: 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 information and communication system defense standards of its regulated specific non-government agency.