Appendix 10 Security Baselines for Information and Communication Systems

Protection Requirement Levels for Information and Communication Systems / Control Measures		High	Medium	Basic
Dimension	Control Measures			
Access Control	Account management	1. Use information and communication systems in accordance with the circumstances and conditions prescribed by the agency. 2. Monitor information and communication system accounts and report any abnormal account use to the administrator. 3. All control measures for the “Medium” level.	1. The agency shall define the allowable idle time or period of use for each system, as well as the conditions governing the use of information and communication systems. 2. When the allowable idle time or period of use prescribed by the agency is exceeded, the system shall automatically log out the user. 3. All control measures for the “Basic” level.	1. Establish an account management mechanism, including procedures for account application, creation, modification, activation, deactivation, and deletion. 2. Expired temporary or emergency accounts shall be deleted or disabled. 3. Inactive accounts of information and communication systems shall be disabled. 4. Periodically review the application, creation, modification, activation, deactivation, and deletion of information and communication system accounts.
	Least privilege	The principle of least privilege shall be adopted, permitting only the authorized access necessary for users (or processes acting on behalf of users) to perform assigned duties in accordance with the agency’s mission and business functions.		
	Remote access	1. For each permitted type of remote access, prior authorization shall be obtained, and use restrictions, configuration requirements, and connection requirements shall be established and documented. 2. Authorization checks for user privileges shall be performed on the server side. 3. Connections involving remote access to the agency’s internal network segments or the backend of information and communication systems shall be monitored. 4. Encryption mechanisms shall be adopted. 5. The source of remote access shall be a pre-defined and managed access control point of the agency.		
Event Logging and Accountability	Record events	1. Logs generated by information and communication systems and retained by the agency shall be reviewed periodically. 2. All control measures for the “Basic” level.		1. Establish log recording intervals and a retention policy, and retain logs for at least six months. 2. Ensure that information and communication systems are capable of recording specified

				events and determine which specified information and communication system events shall be recorded. 3. The functions executed by administrator accounts of information and communication systems shall be recorded.
	Content of Log Records	Logs generated by information and communication systems shall include the event type, time of occurrence, location of occurrence, and any user identifiers related to the event. A single logging mechanism shall be adopted to ensure consistency of output formats, and other relevant information shall be included in accordance with cyber security policies and legal requirements.		
	Log Storage Capacity	Allocate the storage capacity required based on log storage requirements.		
	Response to Log Processing Failures	1. When a log processing failure event that the agency requires to be reported immediately occurs, the information and communication system shall alert designated personnel within the timeframe prescribed by the agency. 2. All control measures for the "Medium" and "Basic" levels.	When log processing fails, the information and communication system shall take appropriate action.	
	Time Stamps and Time Synchronization	1. Information and communication systems shall use their internal clocks to generate the time stamps required for logs, and such time stamps shall correspond to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). 2. The internal clocks of systems shall be periodically synchronized with a reference time source.		
	Protection of Log Information	1. Periodically back up logs to a physical system other than the original system. 2. All control measures for the "Medium" level.	1. Use hashing or other appropriate methods as an integrity assurance mechanism. 2. All control measures for the "Basic" level.	Access to logs shall be restricted to authorized users.
Business Continuity Plan	Data backup	1. Restoration from backups shall be included as part of business continuity plan drills. 2. An off-site data backup mechanism shall be established.	1. Backup data shall be tested periodically to verify the reliability of backup media and the integrity of information. 2. All control measures for the "Basic" level.	1. Define the tolerable period of data loss. 2. Perform data backup.

		3. All control measures for the "Medium" level.		
	System Redundancy	1. Activation of redundancy shall be included as part of business continuity plan drills. 2. All control measures for the "Medium" level.	1. Periodic tests shall be conducted so that, when the original service is interrupted, redundant equipment or other means can take over and provide the service within the maximum tolerable interruption time. 2. All control measures for the "Basic" level.	Define the maximum tolerable interruption time for restoring service after an interruption of an information and communication system.
Identification and Authentication	Identification and Authentication of Users	1. Multi-factor authentication technologies shall be adopted for access to information and communication systems. 2. All control measures for the "Medium" and "Basic" levels.	Information and communication systems shall identify and authenticate users, and shared accounts shall be prohibited.	
	Authentication Management	1. Authentication mechanisms shall prevent login attempts or password-change attempts by automated programs. 2. Password reset mechanisms shall, after re-verifying the user's identity, issue one-time and time-limited tokens. 3. All control measures for the "Basic" level.		1. When a default password is used for the first login to the system, it shall be changed immediately after login. 2. Authentication-related information shall not be transmitted in plaintext. 3. An account lockout mechanism shall be established so that, when account login authentication fails five times, the account shall be prevented from attempting to log in again for at least 15 minutes, or the agency's own failed-authentication mechanism may be used. 4. When passwords are used for authentication, minimum password complexity requirements shall be enforced, and

				passwords shall be changed in accordance with the agency's password validity policy. 5. When a password is changed, the new password shall not, at a minimum, be identical to any of the previous three passwords. 6. For external users, the agency may prescribe its own rules for implementing the measures specified in Items 4 and 5.
	Protection of Authentication Information	1. Where information and communication systems use passwords for authentication, such passwords shall be hashed or otherwise appropriately processed before storage. 2. All control measures for the "Basic" level.		Information and communication systems shall mask information during the authentication process.
System and Service Acquisition	Requirements Phase of the System Development Life Cycle	Confirm system security requirements (including confidentiality, availability, and integrity).		
	Design Phase of the System Development Life Cycle	1. Based on system functions and requirements, identify threats that may affect the system and conduct risk analysis and assessment. 2. Incorporate the risk assessment results into the review items for the requirements phase and propose revisions to the security requirements.		No requirements.
	Development Phase of the System Development Life Cycle	1. Perform source code scanning. 2. The system shall have a notification mechanism for the occurrence of serious errors. 3. All control measures for the "Medium" and "Basic" levels.	1. Necessary control measures shall be implemented to satisfy security requirements. 2. Attention shall be paid to preventing common software vulnerabilities, and necessary control measures shall be implemented. 3. When an error occurs, the user-facing page shall display only a brief error message and code, and shall not include detailed error information.	
	Testing Phase of the System Development Life Cycle	1. Perform penetration testing. 2. All control measures for the "Medium" and "Basic" levels.	Perform vulnerability scanning.	
	Deployment and Operation and Maintenance Phase of the	1. During the operation and maintenance phase of the system development life cycle, version control and change management shall be implemented. 2. All control measures for the "Basic" level.		1. In the deployment environment, relevant cyber security threats shall be addressed through updates and patching.

	System Development Life Cycle			2. Identify and disable unnecessary services and ports. 3. Information and communication systems shall not use default passwords. 4. Back up system source code.
	Outsourcing Phase of the System Development Life Cycle	Where the development of an information and communication system is outsourced, security requirements for each phase of the system development life cycle, by level and including confidentiality, availability, and integrity, shall be incorporated into the outsourcing contract.		
	Acquisition Procedures	1. Development, testing, and production environments shall be segregated. 2. All control measures for the “Basic” level.		Identify third-party software, services, libraries, or other components used in information and communication systems.
	System documents	Documents related to the system development life cycle shall be properly retained and managed.		
System and Communication Protection	Confidentiality and integrity of transmission	1. Information and communication systems shall adopt encryption mechanisms to prevent unauthorized disclosure of information or detect changes to information, unless alternative physical protection measures are in place during transmission. 2. Use publicly available algorithms that have been validated by recognized international bodies and remain uncompromised. 3. Encryption keys or certificates shall be changed periodically. 4. Management rules shall be established for the custody of keys on the server side, and necessary security protection measures shall be implemented.	No requirements.	No requirements.
	Security of data storage	Important configuration files of information and communication systems	No requirements.	No requirements.

		and other information requiring protection shall be encrypted or stored by other appropriate means.		
System and Information Integrity	Vulnerability Remediation	1. Periodically confirm the status of remediation of vulnerabilities relevant to information and communication systems. 2. All control measures for the “Basic” level.		System vulnerability patches shall be tested for effectiveness and potential impact, and shall be applied periodically.
	Monitoring of information and communication systems	1. Information and communication systems shall adopt automated tools to monitor inbound and outbound communications traffic and, when unusual or unauthorized activities are detected, analyze such events. 2. All control measures for the “Medium” level.	1. Monitor information and communication systems to detect attacks and unauthorized connections, and identify unauthorized use of information and communication systems. 2. All control measures for the “Basic” level.	When signs of intrusion into an information and communication system are detected, designated agency personnel shall be notified.
	Integrity of software and information	1. Conduct periodic integrity checks on software and information. 2. All control measures for the “Medium” level.	1. Use integrity verification tools to detect unauthorized changes to specified software and information. 2. When an integrity violation is detected, the information and communication system shall implement the security protection measures designated by the agency. 3. All control measures for the “Basic” level.	Input validation of user-provided data shall be performed on the application server side.

Note: The central competent authority in charge of the relevant sector for a specific non-government agency may, depending on actual needs and within the scope permitted by these Regulations, separately prescribe information and communication system security baselines for the specific non-government agencies under its jurisdiction.