Schedule 9: Principles of classification of levels of defense requirements of information and communication system

Defense requirements Levels Dimension	High	Medium	Common
Confidentiality	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to limited impact on the operation, asset or reputation of the agency.
Integrity	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to limit impact on the operation, asset or reputation of the agency.
Availability	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to very serious or disastrous impact on the operation, asset or	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to limit impact on the operation, asset or reputation of the agency.

	reputation of the agency.		
Regulatory compliance	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the personnel of the agencies to be subject to criminal liabilities.	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the agencies or their personnel to be subject to administrative punishments, disciplines or penalties.	Other status of establishment or operation of information and communication system under relevant regulatory requirements.

Note: The defense requirement levels of the information and communication system shall be the highest ones as determined in any of the dimensions of confidentiality, integrity, availability and regulatory compliance relating to such systems.