Tourism Administration, Ministry of Transportation and Communications Cyber Security Management Agreement for Contracted Suppliers

(Revised on 9.20.2023)

All suppliers that undertake this procurement project and involve operations such as information and communication system/website, set up, maintenance of information and communication software and hardware, and provision of information and communication service, shall strictly observe the following rules and regulations:

1. Setup and maintenance

(1) Newly set up external service system shall adopt responsive web design (RWD) technology at least for the front end, capable of adapting to different screen sizes of various mobile devices without distorting images. If responsive web design (RWD) cannot be adopted due to special requirements, an exemption may be granted after explaining the reasons and obtaining approval from the Administration.

(2) Newly set up external service system shall comply with various website construction specifications of the Ministry of Digital Affairs, including “Web Content Accessibility Guidelines” and “Government Website Service Management Specifications”, etc., and pass the AA-level accessibility web page testing to obtain the certification label. If the AA-level accessibility web page testing certification label cannot be obtained due to special requirements, an exemption may be granted after explaining the reasons and obtaining approval from the Administration.

(3) If the system has adopted responsive web design (RWD) or obtained the AA-level accessibility web page testing certification label, the supplier shall continuously maintain relevant functions and operations.

(4) In the event of webpage replacement or abnormality in the external service system, it should switch to a standby static service screen within 10 minutes, and vulnerabilities should be detected, repaired, and follow-up response measures prepared.

(5) Both the front and back ends of the system shall adopt https encryption, and their protocols shall comply with internationally recognized secure transmission standards to maintain data transmission security and ensure security control management.

(6) The supplier shall regularly review the accuracy of graphic and textual information and link settings on web pages and rectify any related issues.

(7) If the system does not use the Administration’s domain, the supplier shall provide relevant information regarding domain leasing (including the information of the company applying for the domain, applicant information, account username and

password, lease expiration date, etc.) to the Administration. The domain leasing fees during the contract and warranty period shall be borne by the supplier.

(8) Before the system goes online or after the completion of functional expansion/revision, the supplier shall submit vulnerability scanning and program source code security testing reports for web application, stress testing reports, and cooperate with the Administration's cyber security detection operation to rectify any related vulnerabilities.

(9) For various types of cyber security detection results submitted by the Administration or the supplier, severe, high, medium, and OWASP TOP 10 or above risk vulnerabilities must be patched by the supplier within 10 days. Low-risk vulnerabilities should be patched by the supplier to the best of their ability within the contract period. If a vulnerability cannot be patched, the supplier must provide a "Vulnerability Handling Report Form" or include details in the report, specifying the reasons for inability to patch, response methods, or relevant cyber security protection measures. After review and approval by the Administration, the time for patching may be extended.

(10) **The defense requirements level is: ___ level** (if not specified, medium). During the performance period, the supplier shall fill out the "Defense standards of cyber systems Form" (if the system contains personal data, the "Outsourced Supplier Self-Assessment Form" shall be filled out separately) and submit it to the Administration for review. The Administration may inspect and confirm at the supplier's website or system development location as required. The supplier shall complete the control measures specified in Schedule 10 of the "Regulations on Classification of Cyber Security Responsibility Levels" in accordance with the system protection level determined by the Administration (Common, medium, high).

2. Environment and Services

(1) The Administration can provide a virtual hosting environment for the operation system (Windows Server 2019), database (SQL Server 2019 or 2022) for the project, for the winning tenderer to use. (if the supplier needs to use other operating systems and databases, it shall provide and install copyrighted software itself, and the installed software shall be the latest version and regularly updated). The supplier may provide a cloud environment for the project system, but shall provide sufficient external network and hardware resources during the project and warranty period; basic information security protection such as antivirus software, firewall (WAF), IPS, DDoS attack

prevention services, and system and data backup services. The related fees of which shall be borne by the supplier.

(2) If it is necessary to apply for the shared co-location room virtual hosting environment or domain of the Administration, the “Information Technology Service Request Form” shall be filled out. After approval by the responsible unit of the Administration, an application shall be submitted to the information management unit of the Administration.

(3) Hardware and software equipment, network environment, and systems shall comply with IPv6 specifications (support IPv6 protocol) and provide IPv6 services.

(4) If the system is placed in the shared co-location room of the Administration, the supplier shall cooperate with the Administration’s information security requirements, such as installing agent programs to perform security monitoring, and cooperate with the Administration’s operating system and database upgrades, hardware and software equipment replacement and update, virtual environment adjustments, and complete relevant migration and configuration operations.

(5) If it is necessary to apply for the shared co-location room virtual hosting environment or domain of the Administration, and if there are changes in web pages or URLs (including additions, removals, or modifications of names and URLs), the “Information Service Application Form” shall be filled out. After approval by the responsible unit of the Administration, an application shall be submitted to the information management unit of the Administration.

(6) If the project involves information and communication software, hardware, or services, team members executing the project for the supplier shall not be mainland Chinese nationals, and mainland Chinese information and communication products (including system software, apps, IoT devices, mobile devices and phones, computers, servers, monitors, remote control drones, hardware with data processing or control functions) shall not be provided or used.

(7) If this procurement belongs to the category of “Business Areas with Sensitive or National Security (Including Information Security) Concerns” announced by the Investment Review Committee, Ministry of Economic Affairs, the supplier shall not be mainland Chinese companies, third-party companies with mainland investment components, and information service providers with mainland Chinese capital announced by the Investment Review Committee, Ministry of Economic Affairs. (The above-mentioned business areas and list of information service providers with mainland

Chinese capital are publicly available on the website of the Investment Review Committee, Ministry of Economic Affairs http://www.moeaic.gov.tw).

(8) During the contract period, the supplier shall be responsible for the maintenance of the system and equipment provided for the project to ensure that they remain in good and usable condition at all times. In case of a malfunction, the supplier shall arrive for service or commence repairs within 2 hours and complete repairs **within ___ hours** (if not specified, 8 hours) after notification by the same phone call, email, or SMS. If it is unable to provide service or complete repairs within the specified time due to justifiable reasons, the supplier shall provide replacement equipment of the same (or higher) grade until the malfunctioning equipment or system is restored to normal operation.

3. System Design Security

(1) When system design involves authentication mechanisms, priority shall be given to integrating with other security authentication mechanisms, and more rigorous mechanisms shall be given priority, such as certificate authority (CA) mechanisms, lightweight directory access protocol (LDAP), operating system account integration (such as SSO or AD), etc.

(2) When adopting the account and password identity authentication mechanism, the password shall consider including password length restrictions, password combination restrictions, password error count restrictions, and password change history management, etc., and comply with the relevant items specified in the Government Configuration Baseline (GCB). If it is unable to comply with the GCB requirements due to special requirements, an exemption may be granted after explaining the reasons and obtaining approval from the Administration.

(3) If the system information involves the transmission and reception of sensitive information, an encrypted transmission mechanism shall be designed, and relevant information such as transmission source, destination address, transmission time, and transmission success or failure shall be recorded. Sensitive data shall be encrypted, and the program of the database shall have a SQL Injection filtering mechanism.

(4) Relevant electromagnetic records of the system shall be retained for at least the last 6 months, including OS event, web log, AP log, and logon log.

(5) When designing various exception handling mechanisms, avoid directly displaying the original complete error information to the users.

(6) When a program fails, the error code that may be generated shall be handled by exception handling.

(7) Appropriate idle time shall be planned for system construction. When a user logs in for more than 30 minutes without any action, its account shall be automatically logged out.

(8) When encoding system applications, avoid writing insecure source code issues such as Cross Site Scripting, Injection Flaw, Malicious File Execution, Insecure Direct Object Reference, and Cross-Site Request Forgery. These shall be explained in the vulnerability scanning and program source code security detection report before the web page application goes online.

(9) The software, hardware and documents delivered by the supplier shall be inspected in advance for hidden malicious programs (such as viruses, worms, Trojans, spyware, etc.) and covert channels, and security testing certificates shall be submitted before going online, Additionally, test data and accounts in the production environment and management data and accounts shall be cleared.

(10) The system development operations environment shall have security protection measures in place. Development, testing, and production environments shall be segregated, and data testing shall not be conducted in the system's production environment. If real data is necessary for testing purposes due to business requirements, authorization shall be obtained from the authority before proceeding. Additionally, sensitive data or fields should be virtualized or obfuscated.

(11) For services provided by the supplier, such as software or system development, version management shall be carried out for each version, and permission control and access record preservation shall be provided in accordance with relevant cyber security management specifications.

(12) A complete executable version of the program and the program source code shall be provided, managed, and controlled by the person in charge of the business. Any subsequent changes should be managed by submitting relevant program versions and source code as backups or for emergency recovery purposes. If unable to provide due to special circumstances, an exemption may be granted after explaining the reasons and obtaining approval from the Administration.

(13) When the supplier performs system maintenance operations such as version updates, data file modifications, or configuration changes, it shall submit change requests and fill out a "Program Requirement Application Form." These requests shall be approved

by system administrators or competent business units before any changes can be made. Relevant records should be retained for future reference.

(14) The supplier shall comply with the Administration's cyber security requirements, conduct regular backup data recovery tests and business continuity plan recovery drills, and establish emergency response plans for outsourced contracts.

(15) The supplier shall fulfill its responsibility for the safekeeping of the system account. The system account shall not be arbitrarily shared with non-operation-related personnel. Access permissions shall only be granted to personnel from the Administration and supplier as necessary for their duties. Regular reviews of access permissions shall also be conducted to ensure appropriateness.

(16) If the supplier's personnel need to remotely access the Administration's system due to operational requirements, they shall submit a "Network Service Connection Application Form." Remote access shall only be granted after approval from the head of the responsible unit of the Administration.

(17) The software used by the supplier during the contract period shall be legal and shall not violate the provisions of intellectual property rights. If any violation occurs, the supplier shall bear the corresponding legal responsibilities.

(18) The Administration has the right to audit and review the tools, software and execution records of processing operations used by the supplier. The supplier shall cooperate by providing relevant information.

4. Database Security Measures

(1) Important system services shall consider having a dedicated database and shall be designed to prevent users from directly accessing the database. Any changes to the database shall be requested by filling out the "Information Service Application Form" and can only be implemented after approval by the head of the responsible unit of the Administration.

(2) After the database is set up, user passwords for all management permissions shall be changed immediately to prevent illegal connections to the database. Additionally, the database management system shall evaluate the activation of audit functions without affecting system performance, save the special permissions of the database management system, and retain records of changes, user account additions and deletions, and the creation, modification, and deletion of objects for at least six months.

5. Information Service Security

(1) Supplier responsible for the establishment, maintenance, or provision of information and communication systems for the Administration, and outsourced to process data on behalf of the Administration through outsourcing and subcontracting (including subcontracting, contract assignment, etc.), shall comply with the Administration's contracts and related security requirements and possess information security maintenance measures. However, without the Administration's permission, data processing shall not be further subcontracted or outsourced.

(2) Supplier service personnel who access data from the Administration shall be required to sign a "Confidentiality Agreement (Supplier, Personnel)" in accordance with the Administration's cyber security management system. During the project execution period, if there are any changes in supplier personnel, relevant data shall be supplemented accordingly.

(3) Upon completion of performance or termination of the contract, the supplier shall deliver the final executable version of the complete program, including program source code, system databases, etc., and data collected during the contract period (including original data from public participation activities, personal data of the public, etc.). If the website or system is assessed by the Administration as no longer needed, the supplier shall assist in the removal and deletion of data. The supplier shall also delete any personal data collected, processed, or used in executing the contract, and shall not retain any backups.

(4) The supplier shall diligently implement Configuration Management to ensure the integrity and consistency of the system, in order to meet the Administration's requirements for system quality and cyber security.

(5) When the supplier becomes aware of any violation of relevant cyber security laws pertaining to this project or incidents of cyber security within the system, it shall promptly report to the responsible personnel or designated contact point of the Administration in the specified manner, propose emergency response measures, implement remedial actions, and cooperate with the Administration for follow-up processing.

(6) The supplier shall have comprehensive cyber security management measures in place or be verified by a third party when conducting outsourced business-related procedures and environments.

(7) The supplier shall allocate sufficient and appropriately qualified personnel who have received adequate training and possess professional certifications in cyber security, or have similar business experience in cyber security.

(8) If the outsourced business involves classified national security information, personnel executing the outsourced business shall undergo competency audit, and their departure shall be controlled in accordance with the provisions of the Classified National Security Information Protection Act.

(9) If the outsourced business includes customized development of information and communication system, the supplier shall provide security testing certificate of such information and communication system; if such information and communications system is the core system of the Administration, or the outsourcing amount exceeds NT$10,000,000, the supplier shall contract third party to conduct the security testing (related costs to be borne by the supplier).

(10) If the use of system or resource other than those developed by the supplier is involved (e.g., external components or software), the supplier shall provide a list indicating non-self-developed content, versions, sources, and provide the certification of authorization, and pay attention to security vulnerability notices and regularly assess and update them.

(11) Upon completion, termination, or cessation of the contract, the supplier shall return, hand over, delete, or destroy all relevant data in its possession for the performance of the contract, or return it in accordance with the instructions of the Administration, and retain the execution records.

(12) The Administration shall, periodically, or whenever it becomes aware of the occurrence of cyber security incident of the supplier that might affect the outsourced business, confirm the implementation status of the outsourced business by audit or other appropriate method.

(13) The supplier shall comply with the Cyber Security Management Act and its sub-laws, and the various cyber security norms and standards issued by the Executive Yuan, as well as adhere to the Administration's cyber security management and confidentiality regulations. Furthermore, the Administration reserves the right to conduct audits on the supplier and its subcontractors by dispatching personnel for auditing, commissioning project teams organized by the competent authority of the Cyber Security Management Act for audit or other appropriate method. If the audit results do not meet the requirements of the contract, the Cyber Security Management Act, its related sub-laws, the various cyber security norms and standards issued by the Executive Yuan, the

supplier shall complete the improvements within the time limit upon receiving notification from the Administration.

(14) The supplier hereby guarantees that, for works completed by its employee or contracted party within the scope of employment, in accordance with Article 11, Paragraph 1, Proviso and Article 12 of the Copyright Act, where an agreement is made between the employee or contracted party which stipulates that the supplier is the author, such agreement shall govern. If it is agreed with its employees or contractors that the supplier shall be the author, the economic rights to such work shall be enjoyed by the supplier (a written agreement signed by the author must be submitted). However, this agreement is only applicable between the supplier and its employee or contracted party. The rights and responsibilities between the supplier and the Administration shall still be governed by the terms of the contract for this project.

6. Personal Data Protection

(1) If the data entrusted to the supplier or subcontractor involves personal information, both the supplier and subcontractor shall strictly adhere to the requirements of the "Personal Data Protection Act" and the "Enforcement Rules of the Personal Data Protection Act". They shall ensure that the processing and use of data are appropriate, relevant, and not excessive. Additionally, they shall include a confidentiality statement regarding personal data and specify the matters subject to supervision under the Personal Data Protection Act and related regulations, and submit appropriate "File Security Maintenance Plan" and "Rules Governing the Handling of Personal Data Following A Business Termination."

(2) When the supplier collects, processes, or uses personal data and files entrusted by the Administration for this project (that is, "personal data" as defined by the Personal Data Protection Act, which refers to a natural person's name, national identification Card number, occupation, contact information, social activities and any other information that may be used to directly or indirectly identify a natural person), the supplier shall adhere to the following agreements:

1. Obligations during collection, processing, or use:

(1) When the supplier collects, processes, or uses personal data for this project, it shall comply with the requirements of Article 19 or Article 20 of the Personal Data Protection Act, and the provisions of the Enforcement Rules of the Personal Data

Protection Act, and adhere to the scope, categories, specific purpose, and time period commissioned by the Administration.

(2) The supplier shall only collect, process, or use personal data within the scope of the execution of this project. (The supplier is prohibited from using the personal data and files provided by the Administration or collected during the execution of this project for marketing or commercial promotion activities, or in any way or method delivering them to third parties unrelated to the performance of the contract. Furthermore, the supplier shall not collect, process, or use personal data for purposes beyond the scope of this project, including combining personal data and files originally held by the supplier for further processing or use.)

(3) If the supplier believes that the instructions from the Administration violate the Personal Data Protection Act or other laws, it shall immediately notify the Administration and cease executing the relevant operation upon consent.

2. Security Management Measures

The supplier, within the scope of executing its business, shall implement security management measures as stipulated in Article 27 of the Personal Data Protection Act and Article 12 of the Enforcement Rules of the Personal Data Protection Act to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed. These security management measures may include the following and shall be proportionate to the intended purposes of personal data protection:

(1) allocating management personnel and reasonable resources;
(2) defining the scope of personal data;
(3) establishing a mechanism of risk assessment and management of personal data;
(4) establishing a mechanism of preventing, giving notice of, and responding to a data breach;
(5) establishing an internal control procedure for the collection, processing, and use of personal data;
(6) managing data security and personnel;
(7) promoting awareness, education and training;
(8) managing facility security;
(9) establishing an audit mechanism of data security;
(10) keeping records, log files and relevant evidence; and
(11) implementing integrated and persistent improvements on the security and maintenance of personal data.

3. If there is a need for second-tier subcontract in the execution of business activities, which involves the collection, processing, or use of personal data, the supplier shall obtain prior written consent from the Administration and a written undertaking from the second-tier subcontractor regarding the confidentiality of personal data. The Administration shall also be notified in writing of the name, address, and scope of the collection, processing, or use of personal data by the second-tier subcontractor. The supplier shall restrict the scope of the second-tier subcontractor's collection, processing, or use of personal data and appropriately supervise the second-tier subcontractor in accordance with relevant regulations such as the Personal Data Protection Act. The supplier shall bear the same responsibility for the second-tier subcontractor's collection, processing, or use of personal data.
4. Obligations When Exercising the Rights of Data Subject

   When the supplier performs the business for this project and receives the exercise of rights by the data subject under the Personal Data Protection Act, it should respond in accordance with relevant regulations and make records for the Administration's reference.
5. Obligation to Provide Data

   When the Administration requests the supplier to provide relevant information such as the collected personal data files, the basis and specific purpose for retaining these personal data files, the categories of personal data, and related information on their collection, processing, and use, the supplier shall not refuse.
6. Obligation to Notify in Case of Emergency Incidents

   If, during the execution of this project, personal data is stolen, disclosed, altered, or otherwise infringed upon, the supplier shall immediately notify the Administration and take appropriate response measures upon discovery. After investigating, the supplier shall report the nature of the violation, the scope of the affected personal data, and the remedial measures taken and planned. With the Administration's consent, the supplier shall notify the data subject in an appropriate manner as required by law.
7. Regular Verification

   The Administration shall have the right to audit and verify the implementation of the supplier's personal data security management measures and record the verification results. If necessary, the Administration may send personnel for on-site inspections or commission professionals to conduct audit, and the supplier shall cooperate. If

flaws are identified during the inspections or audit, the Administration may provide written notice detailing the reasons and request the supplier to implement improvements within the time as designated by the Administration.

8. Deletion or Return of Data During Contract Performance or Termination

(1) During the performance of the contract, the Administration shall have the right at any time to request the supplier and personnel handling personal data to return or delete the personal data collected, processed, and used in the execution of business for this project, and demand that no backups are retained.

(2) Upon termination or cessation of the contract, the supplier and personnel handling personal data shall delete or destroy the personal data held in the course of performance of the contract and return the personal data carriers and also provide records of the time, method, and location of the deletion, destruction, or return of the personal data.

(3) For the aforementioned return, the supplier shall have the right to deliver the personal data to a third party designated by the Administration. If necessary, the Administration may conduct on-site inspections of the supplier's deletion and destruction operations, and the supplier shall cooperate.

9. Liability for Damages

(1) If the supplier violates Article 6, Paragraph 2, Items 1 to 8 of this Affidavit and fails to implement improvements within the time as designated by the Administration, the Administration, depending on the severity of the situation, shall have the right to take the following actions:

A. Notify the supplier in writing to terminate or partially or fully rescind the contract.

B. Require a reduction in part or all of the contract price.

C. Charge liquidated damages of 2‰ (two thousandths) of the total contract price.

(2) If the supplier in the execution of the business of this project, violates the Personal Data Protection Act, the Enforcement Rules of the Personal Data Protection Act or other related regulations, resulting in the unlawful collection, processing, use, or other infringement of personal data, the supplier shall be liable for damages. If the Administration suffers damage due to the supplier's violation of the Personal Data Protection Act or the Enforcement Rules of the Personal Data Protection Act while executing this project, the Administration shall have the right to seek compensation from the supplier. If a third party claims damages

as a result, the supplier shall be responsible for handling and bearing all legal liabilities (such as assisting the Administration in necessary defenses and providing relevant information during litigation, and bearing any resulting litigation costs, attorney fees, and other related expenses, and be responsible for repaying the liability of the Administration for damages to third parties).

7. Confidentiality and Copyright Signing

(1) If the supplier undertakes this procurement project, and if it involves operations related to information and communication systems/websites, information and communication software and hardware setup, maintenance, and provision of information and communication services, the supplier or team members shall sign and submit the following documents:

1. Confidentiality Agreement/ Non-disclosure Affidavit (supplier): 1 copy.
2. Confidentiality Agreement/ Non-disclosure Affidavit (Personnel): Each participating personnel in this project shall sign 1 copy.
3. Authorship Agreement: Each participating personnel in this project shall sign 1 copy.
4. List of supplier's service team members: 1 copy.
5. Supplier personnel's acceptance of competency audit agreement: For outsourcing projects involving important business and classified national security information: Each participating personnel in this project shall sign 1 copy.

(2) If there are changes in team members, new personnel shall submit the Confidentiality Agreement/ Non-disclosure Affidavit (Personnel) and Authorship Agreement on the day of appointment or before taking office.

The Company fully understands the above cyber security-related provisions and pledges to comply with them diligently. In the event of any violations, the Company is willing to accept the relevant penalties stipulated in the contract for this project.

Name and Seal of Supplier:
Name and Signature of the Person-In-Charge of the Supplier:
Address of Supplier:
Contact Phone Number of Supplier:
Unified Number:

Dated MM____DD____2024

Confidentiality Agreement/ Non-disclosure Affidavit (Supplier)

The company (hereinafter referred to as "the Supplier") is entrusted by the Tourism Administration of the Ministry of Transportation and Communications (hereinafter referred to as the "Administration") to handle the project ○○○○○○○○ (hereinafter referred to as "the Project"). During the execution of the Project, the Supplier may become aware of or have access to government confidential information and business secrets (including personal data), and in order to maintain their confidentiality, the Supplier hereby agrees to abide by the following provisions of this Affidavit:

Article 1 The Supplier hereby undertakes that during the validity period of this contract and after its expiration or termination, all government confidential information not marked for public disclosure by the Administration, as well as business secrets for which the Administration has confidentiality obligations to third parties under the contract or the law, shall be properly safeguarded and kept confidential with the care of a prudent manager. Such secrets shall only be used within the scope of this contract and within the premises designated by the Administration. Without the prior written consent of the Administration, the Supplier shall not copy, retain, or use such secrets for personal or any third-party's needs, nor disclose, inform, deliver them to a third party, or in any other way make such secrets known or utilized by a third party, or publish or release them externally, nor shall they be taken to places other than those designated by the Administration or outside of the designated premises.

Article 2 The Supplier's knowledge or acquisition of the Administration's official secrets and business secrets shall be limited to what is necessary for the execution of this contract and only during the validity period of this contract. The Supplier hereby agrees that official secrets and business secrets shall be provided and disclosed only to members of the contract performing Contractor's team who need to know the secrets for the performance of the contract.

Article 3 The Supplier's shall be relieved from its confidentiality obligations under the following circumstances:

Information that was originally subject to confidentiality obligations was legally held or known without the need for confidentiality before being provided by the Administration.

Information that was originally subject to confidentiality obligations has been declassified in accordance with the law, the Administration is no longer responsible for confidentiality obligations under the contract, or the information has become public knowledge.

The information that was originally subject to a confidentiality obligation was obtained or acquired from a third party, and the third party has confidentiality obligations regarding such information.

Article 4 If the Supplier violates the provisions of this Affidavit, resulting in damage or compensation to the Administration or a third party, the Supplier hereby agrees to unconditionally bear all responsibilities, including all expenses and compensation required for litigation involving the Administration or a third party. In the event that a third party makes a claim or initiates litigation against the Administration, upon written notice from the Administration requesting relevant information, the Supplier shall cooperate and provide the necessary assistance.

Article 5 The Supplier hereby guarantees to fulfill confidentiality obligations and responsibilities regarding any confidential or sensitive business files, personal data, and information system operations known or held during the course of work. The Supplier shall adhere to relevant regulations such as the “Trade Secrets Act” , “Copyright Act”, “Trademark Act”, “Patent Act”, “Personal Data Protection Act”, and the “Enforcement Rules of the Personal Data Protection Act”. Without the written approval of authorized personnel from the Administration, the Supplier shall not extract, hold, transmit, or provide such information to any third party not related to the business. In case of violation, the Supplier hereby agrees to compensate for all resulting damages and bear relevant civil and criminal liabilities. Additionally, upon termination or completion of the contract, the Supplier shall delete or destroy any personal data obtained during the contractual relationship, return the media containing personal data, and provide records of the time, method, and location of such deletion, destruction, or return. The Administration reserves the right to audit these actions.

1. Without approval, the Supplier shall not remove the Administration’s information equipment, media files, and official documents.
2. Information equipment brought in shall not be connected to the Administration’s network without verification and approval from relevant personnel. If connection to the Administration’s network is approved, the use of modems or

wireless transmission devices to connect to external networks is strictly prohibited.

3. Approved information equipment intended to be brought in for connection to the Administration's network or other information equipment shall be tested for viruses, vulnerabilities, or backdoor programs by designated personnel in the computer mainframe room. If it passes the inspection, an inspection certificate and label shall be issued which shall be affixed to a conspicuous location on the equipment for inspection.
4. In principle, the Supplier on-site service and dedicated maintenance personnel shall use the personal computers and peripheral equipment provided by the Administration and are only allowed to use the Administration's internal network. If business needs require the use of the Administration's email or directory services, it shall be confirmed and approved by relevant personnel. Additionally, internet connection hall also be confirmed and approved by relevant personnel.
5. The Administration shall have the right to periodically or randomly send personnel to check or audit compliance with the above work regulations by the signatory of this Affidavit.
6. This Affidavit remains effective regardless of the signatory's resignation.
7. For any damages arising from the breach of confidentiality obligations and responsibilities outlined in this Affidavit, the Company of the signatory or the Supplier shall bear joint liability for compensation.

Article 6: If the Supplier violates the provisions of this Affidavit, the Administration may request the Supplier to compensate for any damages suffered by the Administration and pursue criminal liability for the Supplier's breach of confidentiality. If a third party suffers damages as a result, the Supplier shall also bear the responsibility for compensation.

To: Tourism Administration of the Ministry of Transportation and Communications

Signatory:
Name and Seal of Supplier:
Name and Signature of the Person-In-Charge of the Supplier:
Address of Supplier:

Contact Phone Number of Supplier:

Unified Number:

The Administration collects the personal data listed on this form to identify you as the signatory of this Affidavit and to trace any violations of the related provisions of this Affidavit. This data will not be used beyond these purposes and will be handled in accordance with the Personal Data Protection Act and the Administration’s data protection requirements.

Dated MM____DD____2024

Confidentiality Agreement/ Non-disclosure Affidavit (Personnel)

The company_____ (hereinafter referred to as "the Supplier") and the company's personnel (hereinafter referred to as Party A) are entrusted by the Tourism Administration of the Ministry of Transportation and Communications (hereinafter referred to as the "Administration") to handle the project ○○○○○○○○ (hereinafter referred to as "the Project"), During the execution of the Project, Party A may become aware of or have access to government confidential information and business secrets (including personal data), and in order to maintain their confidentiality, Party A hereby agrees to abide by the following provisions of this Affidavit:

Article 1 Party A hereby undertakes that during the validity period of this contract and after its expiration or termination, all government confidential information not marked for public disclosure by the Administration, as well as business secrets for which the Administration has confidentiality obligations to third parties under the contract or the law, shall be properly safeguarded and kept confidential with the care of a prudent manager. Such secrets shall only be used within the scope of this contract and within the premises designated by the Administration. Without the prior written consent of the Administration, the Supplier shall not copy, retain, or use such secrets for personal or any third-party's needs, nor disclose, inform, deliver them to a third party, or in any other way make such secrets known or used by a third party, or publish or release them externally, nor shall they be taken to places other than those designated by the Administration or outside of the designated premises.

Article 2 Party A's knowledge or acquisition of the Administration's official secrets and business secrets shall be limited to what is necessary for the execution of this contract and only during the validity period of this contract. The Supplier hereby agrees that official secrets and business secrets shall be provided and disclosed only to members of the contract performing Contractor's team who need to know the secrets for the performance of the contract.

Article 3 Party A's shall be relieved from its confidentiality obligations under the following circumstances:

Information that was originally subject to confidentiality obligations was legally held or known without the need for confidentiality before being provided by the Administration.

Information that was originally subject to confidentiality obligations has been declassified in accordance with the law, the Administration is no longer responsible for confidentiality obligations under the contract, or the information has become public knowledge.

The information that was originally subject to a confidentiality obligation was obtained or acquired from a third party, and the third party has confidentiality obligations regarding such information.

Article 4 If Party A violates the provisions of this Affidavit, resulting in damage or compensation to the Administration or a third party, the Supplier hereby agrees to unconditionally bear all responsibilities, including all expenses and compensation required for litigation involving the Administration or a third party. In the event that a third party makes a claim or initiates litigation against the Administration, upon written notice from the Administration requesting relevant information, the Supplier shall cooperate and provide the necessary assistance.

Article 5 Party A hereby guarantees to fulfill confidentiality obligations and responsibilities regarding any confidential or sensitive business files, personal data, and information system operations known or held during the course of work. Party A shall adhere to relevant regulations such as the “Trade Secrets Act” , “Copyright Act”, “Trademark Act”, “Patent Act”, “Personal Data Protection Act”, and the “Enforcement Rules of the Personal Data Protection Act”. Without the written approval of authorized personnel from the Administration, Party A shall not extract, hold, transmit, or provide such information to any third party not related to the business. In case of violation, Party A hereby agrees to compensate for all resulting damages and bear relevant civil and criminal liabilities. Additionally, upon termination or completion of the contract, Party A shall delete or destroy any personal data obtained during the contractual relationship, return the media containing personal data, and provide records of the time, method, and location of such deletion, destruction, or return. The Administration reserves the right to audit these actions.

1. Without approval, Party A shall not remove the Administration’s information equipment, media files, and official documents.
2. Information equipment brought in shall not be connected to the Administration’s network without verification and approval from relevant personnel. If

connection to the Administration's network is approved, it is strictly prohibited to use modems or wireless transmission devices to connect to external networks.

3. Approved information equipment intended to be brought in for connection to the Administration's network or other information equipment shall be tested for viruses, vulnerabilities, or backdoor programs by designated personnel in the computer mainframe room. If it passes the inspection, an inspection certificate and label will be issued which shall be affixed to a conspicuous location on the equipment for inspection.
4. In principle, Party A's on-site service and dedicated maintenance personnel should use the personal computers and peripheral equipment provided by the Administration and are only allowed to use the Administration's internal network. If business needs require the use of the Administration's email or directory services, it shall be confirmed and approved by relevant personnel. Additionally, internet connection hall also be confirmed and approved by relevant personnel.
5. The Administration shall have the right to periodically or randomly send personnel to check or audit compliance with the above work regulations by the signatory of this Affidavit.
6. This Affidavit remains effective regardless of the signatory's resignation.
7. For any damages arising from the breach of confidentiality obligations and responsibilities outlined in this Affidavit, the company of the signatory or the Supplier shall bear joint liability for compensation.

Article 6: If Party A violates the provisions of this Affidavit, the Administration may request Party A to compensate for any damages suffered by the Administration and pursue criminal liability for the Party A's breach of confidentiality. If a third party suffers damages as a result, the Party A shall also bear the responsibility for compensation.

To: Tourism Administration of the Ministry of Transportation and Communications

Signatory:

Name: ———————————

Address: ———————————————————————————

The Administration collects the personal data listed on this form to identify you as the signatory of this Affidavit and to trace any violations of the related provisions of this Affidavit. This data will not be used beyond these purposes and will be handled in accordance with the Personal Data Protection Act and the Administration's data protection requirements.

Dated MM____DD____2024

Authorship Agreement

This is to certify that employee/contractor _____, during the period of employment/contract with ○○○ Company, hereby agrees that all works completed by the employee/contractor while performing the contract for the ○○○○○○○○ project entrusted by the Tourism Administration of the Ministry of Transportation and Communications shall be attributed to the employer/recruiter as the author.

Signatory of the Agreement Employer (Recruiter) / Supplier:
Representative:
Address:

Signatory of the Agreement Employee/Contractor:
ID Number:
Address:

Dated MM____DD____2024

Supplier Service Team Member Register

Name and Address of Supplier and Subcontractor	Country of Origin of Supplier and Subcontractor	Name	Title	Nationality	Education/ Experience	Job Responsibility

Agreement To Accept Competency Audit By Supplier's Personnel

I, during the period from MM___DD___YY__ to MM___DD___YY__ while employed by (supplier's name) under the commission of the Tourism Administration of the Ministry of Transportation, engaged in ____(business), involving important affairs of the Administration and classified national security information. In accordance with Article 9 of the Cyber Security Management Law and Article 4 of the Implementation Regulations of the Cyber Security Management Law, I hereby agree that the Tourism Administration of the Ministry of Transportation may conduct competency audit to check whether I have any of the following circumstances:

1. One who had committed the offense of disclosing secret, or had committed the offense of civil disturbance or treason after the termination of the Period of National Mobilization in Suppression of Communist Rebellion, and was finally convicted, or was put on a wanted list which has not been closed.
2. One who was a former public official, was subject to administrative penalty or demerit record due to a violation of relevant regulatory for security confidentiality.
3. One who was induced or coerced by foreign government, mainland China, Hong Kong or Macau government to engage in activity unfavorable to national security or significant interest of the nation.
4. Other concrete item relating to the protection of classified national security information.

Name and Signature of Signatory:
ID Number:
Mailing Address:
Contact Number:
Name and Seal of Supplier:
Name and Signature of Person-In-Charge of Supplier:
Address of Supplier:

Dated MM____DD____2024