Mobile Application Basic Security Autonomous Inspection Promotion System

V4.2

Industrial Development Bureau, Ministry of Economic Affairs

August 2020

Mobile Application Basic Security Autonomous Inspection Promotion System Revision History

Date	Mobile Application Basic Security Autonomous Inspection Promotion System Revision History
August 2015	Mobile Application Basic Security Autonomous Inspection Promotion System V1.0
February 2016	Mobile Application Basic Security Autonomous Inspection Promotion System V2.0
March 2017	Mobile Application Basic Security Autonomous Inspection Promotion System V3.0
August 2018	Mobile Application Basic Security Autonomous Inspection Promotion System V4.0
September 2019	Mobile Application Basic Security Autonomous Inspection Promotion System V4.1
August 2020	Mobile Application Basic Security Autonomous Inspection Promotion System V4.2

Table of Contents

Part 1: Regulations for Mobile Application Basic Security Autonomous Inspection Promotion System........ 1
1. System Purpose........ 1
2. Applicable Scope........ 2
3. Definition........ 2
4. Autonomous Inspection System........ 3
5. Mobile Application Security Alliance........ 4
6. Mobile Application Security System Promotion Committee........ 4
7. Certification Institution........ 4
8. Inspection Laboratory........ 4
9. Mobile Application Basic Security Mark (MAS Mark)........ 5
10. Information Control........ 6
11. Tracking Management........ 6
12. Fees........ 6
Part 2: Mobile Application Basic Security Inspection Laboratory Qualification Certification and Management Regulations........ 8
1. Basic Principle........ 9
2. Inspection Laboratory Approval Procedure Review........ 9
3. Correction Period........ 11
4. Inspection Laboratory Certification Certificate........ 11
5. Non-disclosure Principle for Inspection Laboratory Personnel........ 11
6. Inspection Laboratory Fee Collection Principle........ 11
7. Rights and Obligations of Inspection Laboratory........ 12
Part 3: Mobile Application Basic Security Mark Use and Management Regulations........ 15
1. Basic Principle........ 16
2. Definition of Terms........ 16
3. Issuance and Use of Mark........ 16
4. Update of Mark and Information Notice........ 17
5. Tracking Management of Mark........ 18
6. Fees........ 18
Appendix 1. Inspection Laboratory Qualification Certification Application Process........ 1
Appendix 2. “Mobile Application Basic Security Inspection Laboratory” Registration Application Form........ 1
Appendix 3. “Mobile Application Basic Security Inspection Laboratory” Regulations of Rights and Obligations........ 1
Appendix 4. Mobile Application Developer Applying for Inspection and MAS Mark Process........ 1
Appendix 5. “Mobile Application Basic Security Mark” Use Application Form1

Appendix 6. “Mobile Application Basic Security Mark” Use Right and Obligation Regulations 1
Appendix 7. “Mobile Application Basic Security Mark” Additional Use Request Application Form 1

Part 1:

Regulations for Mobile Application Basic Security Autonomous Inspection Promotion System

Background

With the increasing popularity of mobile devices, various types of mobile applications have become essential to the living of the public. However, some developers lack awareness of security, leading to the disclosure of users' data or property damages. In view of the above, in accordance with the resolution reached in the "The 26th Committee Meeting of National Information Security and Communication Security Taskforce, Executive Yuan," the Industrial Development Bureau (IDB), Ministry of Economic Affairs (MOEA), plans and establishes the cybersecurity inspection standard and encourages business operators to perform the service of autonomous verification. Presently, in August 2020, the version of "Regulations for Mobile Application Basic Security" has been updated to V1.3 in order to be used as the basis for promoting the mobile application security inspection mechanism. In September 2019, to implement the basic security regulations, IDB of MOEA entrusted the Institute for Information Industry and the Chinese Cryptology and Information Security Association to jointly revise these "Regulations for Mobile Application Basic Security Autonomous Inspection Promotion System" to V4.1, and further updated and revised to V4.2 in August 2020, to be used as the basis for promoting the mobile application autonomous inspection system development in our nation.

1. System Purpose

    1.1. To implement the "Regulations for Mobile Application Basic Security," to establish mobile application basic security inspection system, and to encourage developer, platform operators to comply with such regulations.

    1.2. To establish the "Mobile Application Basic Security Mark" (referred to as the "MAS Mark"), in order to allow consumers to easily identify mobile applications qualifying this promotional system inspection.

    1.3. To promote the Mobile Application Basic Information Autonomous Inspection Promotion System, and to establish mobile application security.

2. Applicable Scope

2.1. This promotion system adopts the method of voluntary participation. According to the “Regulations for Mobile Application Basic Security,” it is applicable to non-specific fields and all types of mobile applications described in the “Regulations for Mobile Application Basic Security.”

2.2. Under these regulations, a System Promotion Committee is established to manage and maintain the operation of the overall system. Certification institution is responsible for certifying the qualification of inspection laboratories. Inspection laboratories are responsible for accepting the mobile application basic security inspection and issuing inspection qualification report. The inspection laboratories can also apply for the inspection qualification certificate or the use of the MAS Mark with the System Promotion Committee or its authorized institution.

3. Definition

3.1. Mobile Application Basic Security Mark: Certificate representing that the mobile application inspection complies with the “Mobile Application Basic Security inspection Standard.”

3.2. Qualification Registration Management Website: Referred to as the “Management Website,” a public website established by the System Promotion Committee to register and announce the list of the certification institutions, qualified inspection laboratories, and a list of mobile applications qualifying the inspection and granted with the inspection qualification mark.

3.3. Certification: a procedure for a certification Institution to grant official approval to a specific individual or specific agency (institution), in order to prove its capability to perform a specific work.

3.4. Verification: A procedure for a qualified inspection laboratory to issue a written certificate proving that a specific product or service can satisfy the requirements specified.

3.5. Mobile Application: An application designed for smartphones, tablet computers, or other mobile devices for use, and also referred to as "Mobile App" in this document.

3.6. Application Store: A mobile application store built-in in the mobile devices of users or an online store where mobile device users can perform browsing, downloading or purchase of corresponding applications, music, magazines, books, movies or television shows.

4. Autonomous Inspection System

4.1. Mobile Application Security Alliance: To improve the security autonomous inspection mechanism, and to improve the mobile application information security in our nation.

4.2. Mobile Application Security System Promotion Committee: A unit responsible for the management, maintenance and execution of this autonomous inspection promotion system. It is also responsible for the authorization and audit of the MAS Mark, and the management of the website operation.

4.3. Certification institution: In compliance with the regulation specified in Article 6, responsible for certifying whether an inspection laboratory is equipped with the adequate mobile application basic security inspection capability.

4.4. Inspection laboratory: In compliance with the regulation specified in Article 7, a unit for accepting applications from mobile application developers, and providing mobile application developer cybersecurity inspection service according to the "Mobile Application Basic Security Inspection Standard."

4.5. Mobile application developer: The party performing the development, design and maintenance of mobile applications. For entrusted development, the principal may be treated as the developer.

5. Mobile Application Security Alliance

   It is responsible for promoting the development of mobile application related industries in our nation, to improve the security autonomous inspection mechanism, to cultivate mobile application security industry talents, to enhance the domestic mobile application security and to expand domestic and international business opportunities.

6. Mobile Application Security System Promotion Committee

   6.1. Mobile Application Security System Promotion Committee refers to as the "System Promotion Committee."

   6.2. The System Promotion Committee is established under the Mobile Application Security Alliance, and its members are elected from the Mobile Application Security Alliance.

   6.3. The missions of the System Promotion Committee are as follows:

      a. To promote mobile applications' basic security regulations and verification system.

      b. To assist the government in the promotion of the mobile application industry policy, and to handle system operation and regulations addition/revision, management of qualified inspection laboratories and review of inspection reports, authorization and management of qualification certificates and MAS Mark, educational training, international cooperation, promotional events, etc.

7. Certification Institution

   The certification institution of this system is the Taiwan Accreditation Foundation (TAF).

8. Inspection Laboratory

   8.1. Qualification certification: Inspection laboratories shall be certified with qualification by the certification institution in accordance with the

"Mobile Application Basic Security Inspection Laboratory Qualification Certification and Management Regulations," and the valid period of such certification is three years.

8.2. Rights and Obligations of Inspection Laboratory:

8.2.1. Inspection laboratories shall apply for registration with the System Promotion Committee, and after the review and approval by the System Promotion Committee, registration and announcement are then made. For the application procedure, please refer to Appendix 1. For the relevant registration application form and the rights and obligations, please refer to Appendix 2 and Appendix 3.

8.2.2. Other management matters are handled according to the "Mobile Application Basic Security Inspection Laboratory Qualification Certification and Management Regulations."

9. Mobile Application Basic Security Mark (MAS Mark)

9.1. For mobile applications qualifying the inspection performed by the inspection laboratories according to the "Mobile Application Basic Security Inspection Standard," the developers can apply for the issuance of the MAS Mark with the System Promotion Committee or the inspection laboratories authorized by the System Promotion Committee. For the application procedure, please refer to Appendix 4. For relevant mark use application form and regulations on the rights and obligations for the mark use, please refer to Appendix 5 and Appendix 6. Prior to the approval of the certification mark application for the MAS Mark, applicants may, instead, use the qualification certificate issued.

9.2. The MAS Mark, according to the "Mobile Application Basic Security Inspection Standard," classifies mobile applications into three categories:

a. "L1" mobile application: An application not requiring the identification of the user's identity.

b. “L2” mobile application: An application requiring the identification of a user's identity.

c. “L3” mobile application: An application involving transaction actions.

9.3. Registration announcement: A mobile application qualifying the inspection and obtaining the mark shall be registered and announced on the Management Website.

9.4. Validity period: The validity period of MAS Mark is one year. In addition, in case of any one of the following conditions, the System Promotion Committee may stop or terminate its effect:

a. Where there is any matter violating the “Mobile Application Basic Security Mark Use and Management Regulations.”

b. Where there is a violation of the provisions of the regulations for mark use rights and obligations.

9.5. Other mark management matters: Such matters shall be handled according to the “Mobile Application Basic Security Mark Use and Management Regulations.”

10. Information Control

When there is a change to the name or ownership etc. of a mobile application, the mobile application developer shall inform the System Promotion Committee immediately.

11. Tracking Management

The System Promotion Committee may regularly or irregularly use the general survey or random inspection method to verify whether the mobile application qualified version is consistent with the version on the Application Store etc.

12. Fees

12.1. The fees of the autonomous inspection promotion system include various administrative management fees of the certification fee, inspection fee, qualification certificate application fee, etc.

12.2. The certification fees of inspection laboratories are announced and collected by the certification institution.

12.3. The inspection fees are collected by each inspection laboratory individually.

12.4. The qualification certificate application fee and other various fees are announced and collected by the System Promotion Committee.

Part 2:

Mobile Application Basic Security Inspection Laboratory Qualification Certification and Management Regulations

1. Basic Principle

1.1. According to Article 7 of the “Regulations for Mobile Application Basic Security Autonomous Inspection Promotion System,” the requirements related to the qualification and management of inspection laboratories are specified according to these regulations. However, where the certification institution specifies further rules, such rules shall prevail.

1.2. For a domestic inspection laboratory of a legal entity or an academic research institution registered legally, equipped with a certain professional criteria and performing works related to mobile application testing and inspection according to its management system and also issuing reports, the representative of the legal entity or the responsible person of the institution may submit an application to the certification institution for the certification Institution to perform the approval procedure.

2. Inspection Laboratory Approval Procedure Review

For the inspection laboratory approval procedure, the following matters shall be reviewed:

2.1. Inspection laboratory certification application form of the certification institution.

2.2. Photocopies of theproof documents for the registration of the domestic legal entity or institution according to the laws.

2.3. Documents capable of proving the capability of the inspection laboratory.

2.3.1. Inspection laboratory qualification: It is required to be equipped with the laboratory certification certificate of CNS 17025 or ISO/IEC 17025 issued domestically or by an international certification organization.

2.3.2. Personnel qualification: The basic members of the inspection laboratory shall adopt the responsibility delegation principle, and it shall include at least three official employees of the laboratory supervisor, quality supervisor and report signing person etc. Their qualification shall satisfy the following requirements:

2.3.2.1. Laboratory supervisor: Graduated from college and above, and equipped with more than two years of experience in information security-related management jobs, and equipped with the training qualification certificate for laboratory certification standard of ISO/IEC 17025 or CNS 17025.

2.3.2.2. Quality supervisor: Graduated from college and above, and equipped with more than two years of relevant working experience in quality management or auditing, and also equipped with relevant training qualification certificates for quality management or auditing.

2.3.2.3. Report signing person: Graduated from college and above, and equipped with more than three years of working experience in information security-related works, and equipped with the information security-related professional certificates:

a. Equipped with the Certified Ethical Hacker (CEH) or GIAC Security Essentials (GSEC).

b. Equipped with one of the following certificates: Certified Information Systems Security Professional (CISSP), or Certified Secure Software Lifecycle Professional (CSSLP), or EC-Council Certified Security Analyst (ECSA), or EC-Council Computer Hacking Forensic Investigator (CHFI), or GIAC Penetration Tester (GPEN), or GIAC Mobile Device Security Analyst (GMOB), or Certificate of Application Vetting Professional (CAVP).

2.3.3. Performance achievement: Equipped with the actual experience of more than two cases (inclusive) of inspection of mobile application security in three years, shall be equipped with proof documents for review (such as contract or order with the customer end, inspection report etc.).

3. Correction Period

When any document described in all subparagraphs of Article 2 is incomplete or content thereof is insufficient, the certification institution shall inform for correction within a time-limit. In case no correction is made or correction is incomplete within the time-limit, the application shall be rejected. The correction period shall be based on the period informed by the certification institution.

4. Inspection Laboratory Certification Certificate

For an inspection laboratory qualifying the review by the certification institution, the certification institution then issues the "Inspection Laboratory Certification Certificate" (referred to as the "certification certificate").

5. Non-disclosure Principle for Inspection Laboratory Personnel

The inspection laboratory or its service personnel shall bear the non-disclosure obligation on data related to the applicant and inspection, and the same requirements shall be applied to its retired personnel.

6. Inspection Laboratory Fee Collection Principle

The inspection fee announced by the inspection laboratories shall comply with the principle of transparency and fairness.

6.1. The inspection fee shall be classified into three categories according to the type of mobile application applied by the App developer.

6.2. When an inspection laboratory informs that a mobile application developer fails to comply with the regulations, it is necessary to describe the nonconformity and inform the developer for improvement. The notice for the improvement method and fee collection mechanism is to be self-established by the inspection laboratory.

6.3. Inspection laboratories shall follow the requirements for various administrative management fees of qualification certificate fee etc. announced by the System Promotion Committee and shall collect fees on behalf of the System Promotion Committee.

7. Rights and Obligations of Inspection Laboratory

After an inspection laboratory qualifies the certification, it shall comply with the following obligations:

7.1. An inspection laboratory shall maintain its inspection quality and technical capability in order to satisfy the requirements specified in the provision of Article 2.

7.2. A security inspection report issued by an inspection laboratory shall not contain any fraud or deceptive content, or verified and determined by the System Promotion Committee to be disqualified.

7.3. An inspection laboratory accepting inspection application cases shall maintain its fair, just and independent position, and shall not refuse to accept applications without proper reasons, engage in any conduct or differential treatment or violation of impartiality and fairness.

7.4. An inspection laboratory and a mobile application developer with its application accepted thereby shall not have any relationship hindering the impartiality of the inspection system.

7.5. In case of any violation of the conditions described in Sections 7.1~7.4, the System Promotion Committee may announce such violation on the Management Website and inform the certification institution to revoke the certification certificate.

7.6. Inspection laboratories shall accept and cooperate with the regular or irregular supervision evaluation, visit, interview, re-assessment operations etc. arranged by the certification institution, and shall assist necessary for completing the operation successfully. The System Promotion Committee may regularly or irregularly inspect and review the aforementioned operations.

7.7. For changes of relevant information described in the following, inspection institutions shall inform the certification Institution and shall also inform the System Promotion Committee within fifteen days from the date of occurrence of such changes.

a. Change of ownership, name, or address.
b. Change of responsible person of the institution.
c. Change of content described in the certification certificate.
d. Termination or cessation of business.

7.8. For the changes described in the preceding paragraph, in case an inspection laboratory fails to inform the System Promotion Committee within the time-limit, the System Promotion Committee may inform the certification institution to revoke the certification certificate when it is considered necessary.

7.9. Inspection laboratories shall preserve the mobile application files submitted for inspection and shall preserve for at least one year in order to ensure the correctness of the mobile application version submitted for inspection and to protect the files from alternation or damage. When there is a need for inspection, the System Promotion Committee may request inspection laboratories to provide the App original file data preserved by the inspection laboratories.

7.10.Where there is any personnel change in the laboratory supervisor, quality supervisor or report signing person, the inspection laboratory shall actively inform the Secretary Team of the

Mobile Application Security Alliance.

8. Inspection Laboratory Visit Principle

8.1. When a new inspection laboratory receives more than 20 cases (inclusive) and obtains the Mark, a visit is to be performed within three months.

8.2. In the event that an inspection laboratory is not receiving any applications for a period of six months, the Mobile Application Security Alliance shall perform a field visit within one month following such a period to understand the condition of the laboratory.

8.3. The rest of the relevant conditions are handled by the Secretary Team of Mobile Application Security Alliance according to TAF regulations.

Part 3:

Mobile Application Basic Security Mark Use and Management Regulations

1. Basic Principle

1.1. According to the “Regulations for Mobile Application Autonomous Inspection Promotion System: 9. Mobile Application Basic Security Mark,” matters related to the management of the Mark shall follow the provisions of these regulations.

1.2. These regulations are established to clearly define the application issuance and management of the “Mobile Application Basic Security Mark.”

2. Definition of Terms

2.1. Unless specifically described in these regulations, all matters shall be handled in accordance with the provisions of the “Regulations for Mobile Application Autonomous Inspection Promotion System” and “Mobile Application Basic Security Regulations” in principle.

2.2. “Mobile Application Basic Security Mark” (referred to as the “MAS Mark”) is proof representing that a mobile application inspection complies with the “Mobile Application Basic Security Inspection standard.”

3. Issuance and Use of Mark

3.1. Issuance of Mark

3.1.1. Inspection laboratories qualifying the certification are responsible for the mobile application basic security verification and shall issue a qualification inspection report and certificate to mobile applications qualifying the verification, and shall also report to the System Promotion Committee. After a mobile application developer qualifies the verification, it may fill out the MAS Mark use the application form and the regulations for rights and obligations in order to apply for the use of the MAS Mark with the System Promotion Committee.

3.1.2. The System Promotion Committee shall review the application according to Section 3.1.1. In case of any disqualification of review or necessary correction, the applicant shall be informed.

3.2. Use of Mark

3.2.1. Developers shall use the MAS Mark according to the pattern specified by the System Promotion Committee on the website pages of Application Store without changes to its shape, color or additional texts. In cases where there are other methods of use, developers shall submit additional use request application forms to apply for such use with the System Promotion Committee.

3.2.2. It is prohibited to use the MAS Mark for purposes other than for the certification mark.

3.2.3. The System Promotion Committee shall announce the mobile applications certified for the MAS Mark on the Management Website for inquiries.

4. Update of Mark and Information Notice

4.1. Validity period: The validity period of MAS Mark is one year. In addition, in case of any one of the following conditions, the System Promotion Committee may stop or terminate its effect:

a. Where there is any violation of the provisions of these regulations related to the use, update, and tracking management of the Mark.

b. Where there is a violation of the provisions of the regulations for mark use rights and obligations.

4.2. For any change of the name or program version of a mobile application, if the mobile application with the name change or version change plans to use the Mark, it is necessary to re-submit the application according to these regulations again.

4.3. When there is any change in the information of name or ownership etc. of a mobile application, it is necessary to inform the System Promotion Committee immediately.

5. Tracking Management of Mark

5.1. The System Promotion Committee may self-perform or entrust an inspection laboratory to implement a regular or irregular general survey or inspection method to determine whether the version of a mobile application qualifying the inspection is consistent with the version with the use of the Mark. If it is not consistent, then the right to use the Mark shall be stopped.

5.2. Where a mobile application developer is aware that its mobile application qualifying the MAS Mark may cause mobile devices to have the risks of improper access or disclosure, alteration, damage, or loss of personal data, then it shall inform the System Promotion Committee.

5.3. Where the System Promotion Committee is aware of the condition described in Section 5.2, it shall perform re-inspection on such mobile applications. If such mobile application is confirmed to have the likelihood of causing mobile devices to have the risks of improper access or disclosure, alteration, damage, or loss of personal data, then it shall stop the right to use the Mark, and shall also order the mobile application developer to improve within a time-limit. In case no improvement is made within the time-limit, the right to use the Mark shall be terminated.

6. Fees

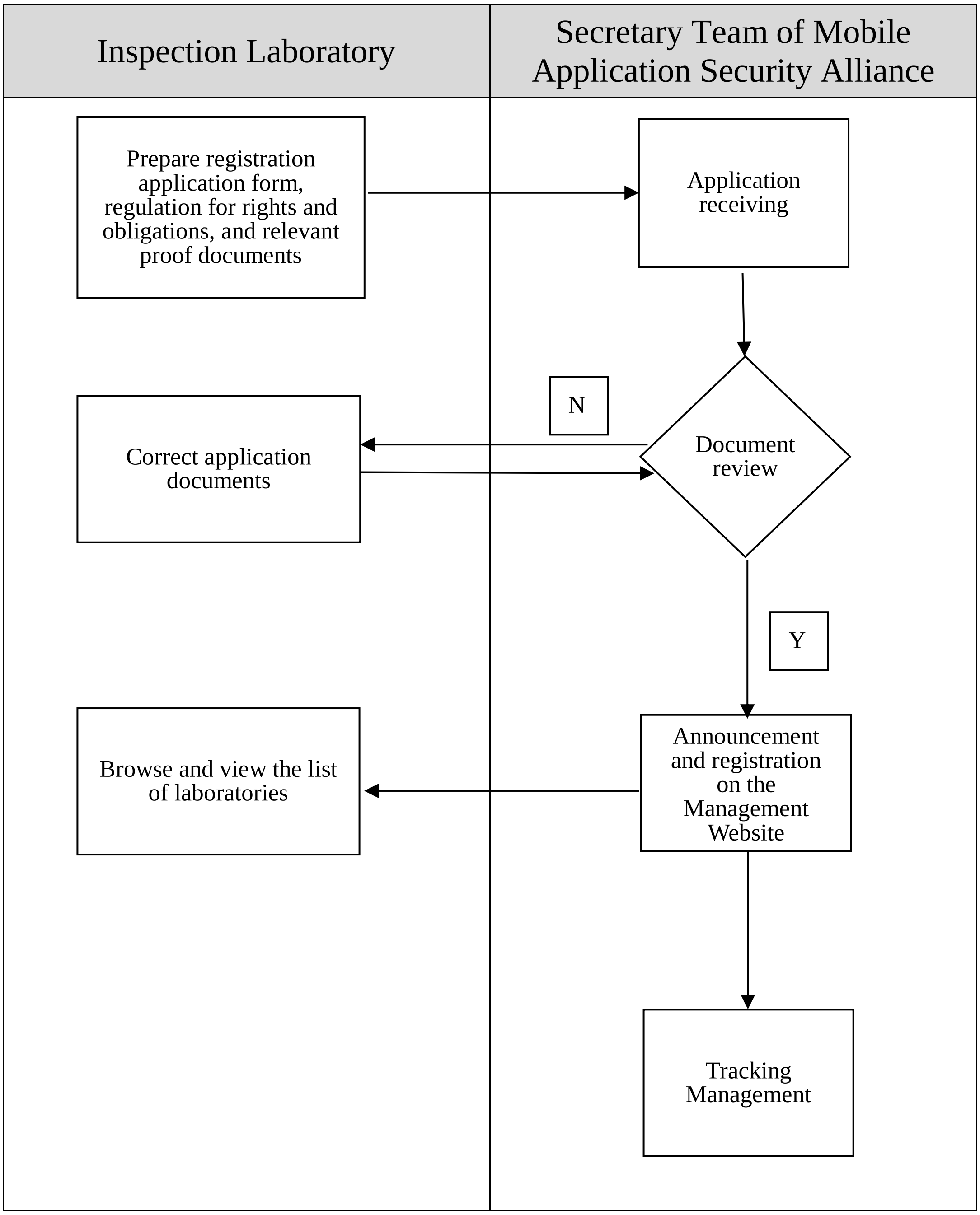
6.1. The inspection fee is announced and collected by each inspection laboratory, and it shall be collected according to the "Mobile Application Inspection Laboratory Qualification

Certification and Management Regulations," "6. Inspection Laboratory Fee Collection Principle."

6.2. The administrative management fees are announced and collected by the System Promotion Committee.

Appendix

Appendix 1. Inspection Laboratory Qualification Certification Application Process


Inspection Laboratory
Secretary Team of Mobile Application Security Alliance
Prepare registration application form, regulation for rights and obligations, and relevant proof documents
Application receiving
Document review
N
Correct application documents
Y
Announcement and registration on the Management Website
Browse and view the list of laboratories
Tracking Management

Appendix 2. “Mobile Application Basic Security Inspection Laboratory” Registration Application Form

We, (hereinafter referred to as the “Applying Institution”) hereby applies for the registration of the “Mobile Application Basic Security Inspection Laboratory” with the “Secretary Team of Mobile Application Security Alliance” and agree to abide by the terms and conditions set forth in the following:

I. Basic Information on Applying Institution:

Full Name of Institution	
Responsible Person of Institution	
Address of Institution	
Name of Laboratory	
Laboratory Supervisor	
Laboratory Address	
TAF Certificate No.	
Contact Window for External	Name: Telephone: Ext. Fax: E-mail:

II. The Applying Institution agrees and understands the “Mobile Application Basic Security Inspection Laboratory Right and Obligation Regulations” (as shown in the Attachment) constitute the regulation for the rights and obligations of both parties.

III. The Applying Institution authorizes the inspection laboratory supervisor described in Article 1 of this application form to represent the Applying Institution and the inspection laboratory and to bear the responsibility for supervising the inspection laboratory to comply with the regulations established by the Committee.

IV. The Applying Institution agrees that the information described in Article 1 of this application form may be provided to the Committee for use in purposes related to external announcements, notification service, and sending of relevant messages. The Applying Institution confirms that the aforementioned laboratory supervisor and contact person are aware of and understand the matters described above, and also agrees with the reasonable collection, processing, and use of the aforementioned data within the scope of collection purpose described above. In case of any change of the information described in Article 1 of this application form, the Committee will be informed within fifteen days from the date of occurrence of such change.

Submitted to

Secretary Team, Mobile Application Security Alliance

Seal of Applying Institution	Signature or Seal of Responsible Person of Applying Institution

Application Date: Month Date, Year

"Mobile Application Basic Security Inspection Laboratory" Regulations of Rights and Obligations form an integral part of this application form. Please submit and affix seals together with this application.

Appendix 3. “Mobile Application Basic Security Inspection Laboratory” Regulations of Rights and Obligations

The Applying Institution (hereinafter referred to as the “Inspection Laboratory) applies for the registration of a “Mobile Application Basic Security Inspection Laboratory” (hereinafter referred to as the “Inspection Laboratory”) of the “Mobile Application Basic Security Autonomous Inspection Promotion System” (hereinafter referred to as “this “Promotion System”), and agrees to abide by the terms and conditions set forth in the following:

1. Definition of Inspection Laboratory

The Inspection Laboratory described in these regulations refer to a “Mobile Application Basic Security Inspection Laboratory” applying for the “Mobile Application Basic Security Inspection Laboratory Certification Service Plan” with the “Taiwan Accreditation Foundation” (hereinafter referred to as “TAF”) and obtaining approval from TAF.

2. Rights and Obligations of System Promotion Committee

2.1. The System Promotion Committee may revise these regulations at any time due to provisions or requirements announced by the competent authority or the System Promotion Committee, and accordingly, for any part involving the Applying Institution due to such change directly, the Applying Institution shall be informed within a reasonable time-limit. After the Applying Institution receives such notice of a change, if it fails to express any dissenting opinions, it shall be treated to agree with such change.

2.2. The System Promotion Committee shall announce the information described in the content of the qualification certificate on the website of the System Promotion Committee or make a public announcement via other methods.

3. Rights and Obligations of Applying Institution

3.1. The Applying Institution shall submit relevant certifications or documents necessary to other similar operations according to the actual facts, and shall also cooperate with the regular or irregular supervision, visit, interview and inspection operations requested by the System Promotion Committee to provide relevant information. In case any information provided by the Applying Institution is found to be deceptive or inadequate, the System Promotion Committee may inform the certification Institution to revoke its qualification certificate. For any damages caused due to deceptive statements or negligence, the Applying Institution shall bear the indemnification liability.

3.2. Where the System Promotion Committee is subject to damage claims from any third party due to the registration of the Applying Institution, the Applying Institution shall be liable for such damage claims.

3.3. For changes of relevant information described in the following, the

Applying Institution shall inform the System Promotion Committee within fifteen days from the date of occurrence of such changes.

a. Change of institution name or address

b. Change of responsible person of institution

c. Change of laboratory name or address

d. Change of laboratory supervisor

e. Change of content described in the certification certificate

f. Business termination or cessation

3.4. For the changes described in the preceding paragraph, in case the Applying Institution fails to inform the System Promotion Committee within the time-limit, the System Promotion Committee may inform the certification institution to revoke the qualification certificate when it is considered necessary.

4. Rights and Obligations of Inspection Laboratory

4.1. The Inspection Laboratory shall maintain the quality system and technical capability in order to comply with the regulations and requirements specified by the System Promotion Committee.

4.2. The Inspection Laboratory shall accept the regular or irregular supervision, visit, interview, inspection operations etc. arranged by the System Promotion Committee, and shall cooperate with the System Promotion Committee to provide necessary relevant information, place, personnel and necessary assistance for completing the operation.

4.3. A security inspection report issued by an inspection laboratory shall not contain any fraud or deceptive content, or verified and determined by the System Promotion Committee to be disqualified.

4.4. An inspection laboratory accepting inspection application cases shall maintain its fair, just and independent position, and shall not refuse to accept applications without proper reasons, engage in any conduct or differential treatment or violation of impartiality and fairness.

4.5. An inspection laboratory and a mobile application developer with its application accepted thereby shall not have any relationship hindering the impartiality of the inspection system.

4.6. The inspection laboratory or its service personnel shall bear the non-disclosure obligation on data related to the applicant and inspection, and the same requirements shall be applied to its retired personnel.

4.7. In case of any violation of any conditions described in Sections 4.1~4.6, the System Promotion Committee may announce such violation on the Management Website and inform the certification institution to revoke the qualification certificate.

4.8. Inspection laboratories shall preserve the mobile application files submitted for inspection and shall preserve for at least one year in order to ensure the correctness of the mobile application version submitted for inspection and to protect the files from alternation or damage. When there is a need for inspection, the System Promotion Committee may request inspection laboratories to provide the App original file data preserved by the inspection laboratories.

5. Inspection Laboratory Fee Collection Principle

5.1. The inspection fee announced by the inspection laboratories shall comply with the principle of transparency and fairness.

5.2. The inspection fee shall be announced and collected by each Inspection Laboratory according to three mobile application categories and their corresponding inspection items described in the latest version of "Mobile Application Basic Security Inspection Standard" announced.

5.3. When an inspection laboratory informs that a mobile application developer fails to comply with the regulations, it is necessary to describe the nonconformity and inform the developer for improvement. The notice for the improvement method and fee collection mechanism is to be self-established by the inspection laboratory.

5.4. The Inspection Laboratory shall follow the requirements for various administrative management fees announced by the System Promotion Committee and shall collect fees on behalf of the System Promotion Committee upon the authorization of the System Promotion Committee.

6. Inspection Qualification Certificate and Mark

6.1. The Inspection Laboratory shall perform works according to this Promotion System or the "Mobile Application Basic Security Inspection Qualification Standard" and Mark management regulations announced by the System Promotion Committee.

6.2. The Inspection Laboratory shall issue the "Mobile Application Basic Security Inspection Qualification Certificate" according to the inspection report on all inspection items required for the mobile application category defined in the "Mobile Application Basic Security Inspection Standard."

6.3. The inspection qualification certificate shall include the content of the following, and the certificate format is designed and printed by the System Promotion Committee:

a. Certificate number (according to the coding principle specified by the System Promotion Committee, such as: TAF certificate number, year, and serial number of the laboratory)

b. Name of applying unit

c. App name, App version

d. Mobile Application Basic Security Inspection Standard version, mobile application category

e. Certificate valid period (one year from the issuance date)

f. Name of inspection laboratory

g. Inspection date (inspection report date issued by the inspection laboratory)

6.4. Inspection qualification certificate (one original copy) issued by the System Promotion Committee, collection of relevant review fee.

7. Intellectual Property Ownership

7.1. The Applying Institution authorizes the System Promotion Committee to use the documents or objects submitted by the Applying Institution without compensation for the needs of certification, inspection, or other similar operations.

7.2. Unless both parties agree in writing that any intellectual property already possessed by the Applying Institution prior to the application shall not be affected by this document.

8. Default Handling

8.1. Unless these regulations specify otherwise, in case the Applying Institution is subject to any breach, for a minor violation, the System Promotion Committee may inform the Applying Institution to complete improvement within one month, and if there is a special reason, an extension of one month may be applied.

8.2. However, where the violation is not improved within the time-limit, and such violation is considered major, the System Promotion Committee may inform the certification institution to revoke the qualification certificate.

8.3. In case the Applying Institution is subject to any one of the following conditions, the System Promotion Committee may inform the certification institution to revoke its qualification certificate:

a. Where its application information is deceptive and untrue.

b. Where its operation violates relevant regulatory requirements.

c. Where it issues a deceptive certificate or document of the same purpose.

d. Where it makes inappropriate statements or causes the System Promotion Committee to get involved in a dispute.

e. Where it exceeds the content of the qualification certificate or it is subject to violation of the regulations of the System Promotion Committee, and such violation is considered major.

9. Non-disclosure Obligation

9.1. The Applying Institution shall provide reasonable confidentiality measures for the data and relevant information provided by the App developer. Except where the service executing personnel need to know confidential information for providing or handling App security inspection service, the Applying Institution shall not use, disclose or reproduce confidential information, and it is prohibited to use the confidential information for other purposes.

9.2. The confidential information described in the preceding article does not include any information on the following conditions:

a. Information that has been disclosed before the App developer provides such information or information that is subsequently disclosed but not due to the fault of the Applying Institution.

b. Information legally obtained by the Applying Institution from a third party that is not required to bear non-disclosure obligation for the App developer.

c. Information that has been possessed by the Applying Institution before such information is provided by the App developer, and there are written records to prove such matters.

d. Information independently developed by employees of the Applying Institution without the use of any means referring to the confidential information, and there are written records to prove such matters.

e. Information that is provided in accordance with regulatory requirements or demands of government agencies.

9.3. Either party of this document shall have the freedom to determine whether to inform the other party about the following information:

a. Confidential information of the other party learned from a third party.

b. Laws, technical regulations, or technical standards applicable to the certification.

c. Information required to be disclosed by the certification institution according to the laws.

10. Responsibility

10.1. Where the Applying Institution is subject to any abuse of the certification issued by the certification institution such that the System Promotion Committee suffers damages, the Applying Institution shall bear the indemnification liability for the System Promotion Committee.

10.2. Both parties shall bear all liabilities individually for damages of any third party caused by matters attributable to each of the parties respectively.

10.3. Where any one party of this document is aware of any events that may cause the aforementioned indemnification claim, it is necessary to inform the other party, and shall also adopt any possible methods to prevent the occurrence and expansion of damages.

11. Others

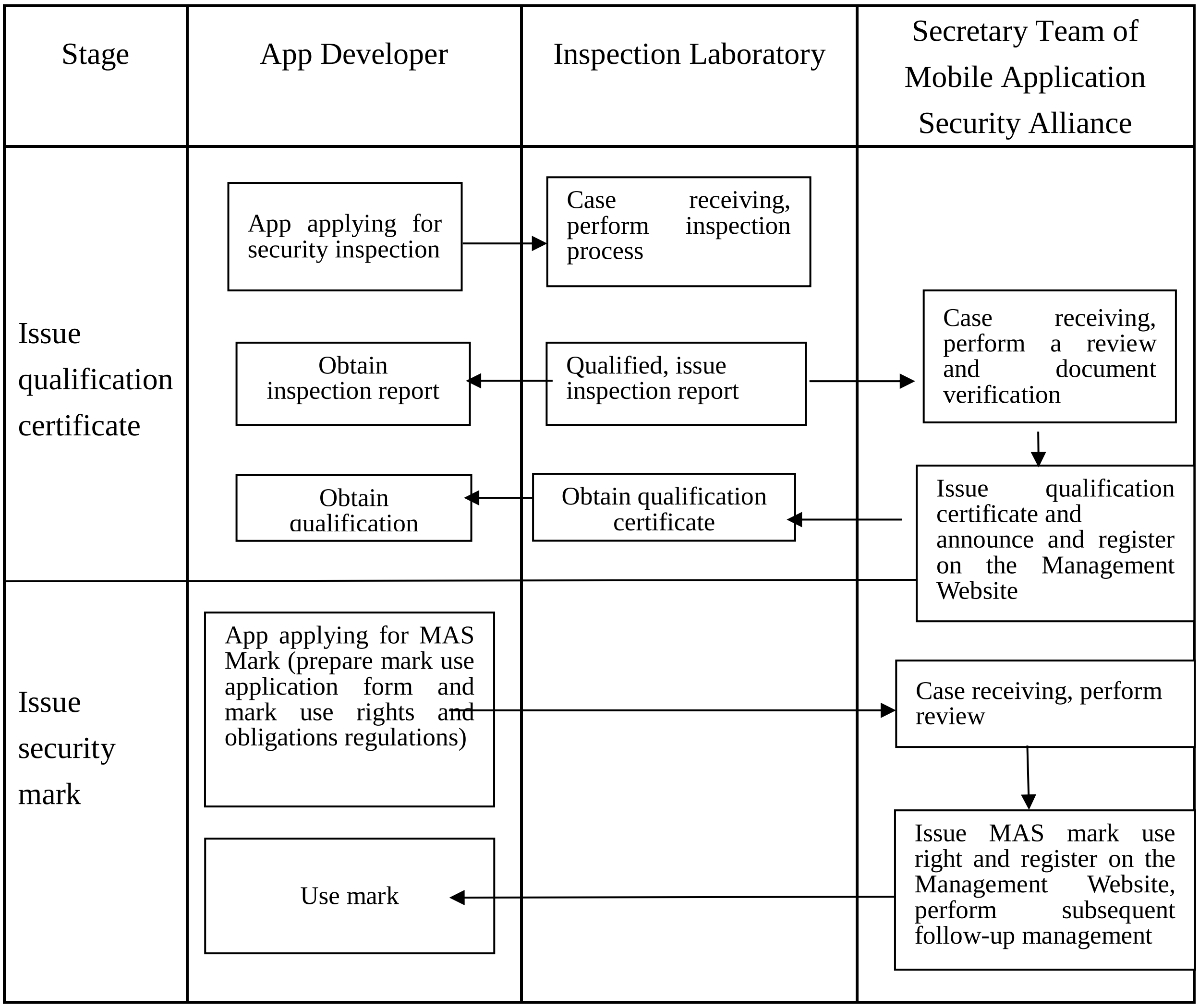
11.1. In case of any dispute, conflict, disagreement, or violation arising from these regulations, the arbitration shall be filed according to the Arbitration Law of R.O.C., and Taipei City shall be the place of arbitration.

11.2. In case of any matters not specified in these regulations, such matters may be further supplemented and specified by both parties through negotiation.

(Blank below)

Appendix 4. Mobile Application Developer Applying for Inspection and MAS Mark Process

For a mobile application qualifying the inspection performed by an inspection laboratory, the Inspection laboratory shall issue the “Mobile Application Basic Security Inspection Qualification Certificate” and the security mark according to the inspection report on all inspection items required for the mobile application category defined in the “Mobile Application Basic Security Inspection Standard.”


Stage
App Developer
Inspection Laboratory
Secretary Team of Mobile Application Security Alliance
Issue qualification certificate
App applying for security inspection
Case receiving, perform inspection process
Obtain inspection report
Qualified, issue inspection report
Case receiving, perform a review and document verification
Obtain qualification
Obtain qualification certificate
Issue qualification certificate and announce and register on the Management Website
Issue security mark
App applying for MAS Mark (prepare mark use application form and mark use rights and obligations regulations)
Case receiving, perform review
Use mark
Issue MAS mark use right and register on the Management Website, perform subsequent follow-up management

Appendix 5. “Mobile Application Basic Security Mark” Use Application Form

We, (hereinafter referred to as the “Applying Institution”) applies for the use of Mobile Application Basic Security Mark (hereinafter referred to as the “MAS Mark”) with the “Mobile Application Security Alliance” (hereinafter referred to as “the Alliance”) and agree to abide by the terms and conditions set forth in the following:

I. Basic Information on Applying Institution:

Mobile Application Basic Information	Application Date	Month Date, Year		
	App Name for Application			
	App Security Type	□L1 □L2 □L3		
	Operating System	□Android □iOS		
	App Version		Standard Version	
	App Category (Single selection on main function)	□Financial (bank, insurance) □Shopping (online shop) □Government □Medical □Communication (call, message, social) □Tool/application □Education □Others		
	App Submission for Inspection Intention	□Voluntary submission □Cooperate with policy (demanded by competent authority)		
Inspection Institution	Name of Inspection Institution			
	Name of inspection laboratory			
	Inspection Application Date	Month Date, Year		
	Inspection Completion Date	Month Date, Year		
	Inspection Report No.			
Mobile	Name of Unit	□Inspected unit (App owner)		

Application Supplier Information	Applying for Certificate	□Developing unit (App developer)
	Name of Inspected Unit	(required)
	Unified Business No.	(required)
	Address of Inspected Unit	(required)
	Name of Contact Person	(required)
	Telephone of Contact Person	(required)
	E-mail of Contact Person	(required)
	Name of Developing Unit	(required)
	Unified Business No.	(required)
	Address of Developing Unit	(required)
	Name of Contact Person	(required)
	Telephone of Contact Person	(required)
	E-mail of Contact Person	(required)
Announcement	Announced on MAS Website	□Announced □Not announced
	Release Status	□Released □Expected to be released □For internal use only
	Application Store Website Address	
English Certificate Application	Whether to Apply for English Certificate	□Yes (please fill out the following table) □No

	App Name (English)	
	Unit Name (English)	(※Please provide information according to the unit name applying for the certificate)
	Name of Inspection Institution (English)	
	Inspection	

II. The Applying Institution agrees and understands that the "Mobile Application Basic Security Inspection Use Right and Obligation Regulations" constitute the regulations for the rights and obligations of both parties.

III. In case the damage is caused due to deceptive information provided by the Applicant, the Applicant agrees to bear relevant legal liabilities, and the Applicant shall also guarantee to have the right to upload the mobile application onto the Application Store.

Submitted to

Mobile Application Security Alliance

Signature or Seal of Inspection Laboratory Supervisor
Signature or Seal of Case Handler of Inspected Unit
Signature or Seal of Case Handler of Developing Unit
(Required for inspection submitted by Development Unit)

"Mobile Application Basic Security Mark" Use Right and Obligation Regulations form an integral part of this application form. Please submit and affix seals together with this application.

Appendix 6. “Mobile Application Basic Security Mark” Use Right and Obligation Regulations

The Applying Institution (hereinafter also referred to as the “Mobile Application Developer”) applies for the use of Mobile Application Basic Security Mark (hereinafter referred to as the “MAS Mark”) with the “Mobile Application Security System Promotion Committee” (hereinafter referred to as “the System Promotion Committee”) and agrees to abide by the terms and conditions set forth in the following:

1. Use Period of Mark:

   The validity period of the MAS Mark is one year, and the System Promotion Committee agrees that the Applying Institution may use the MAS Mark for the App name indicated on the application form.

2. Method of Use of Mark

   2.1 The Applying Institution shall use the MAS Mark according to the pattern specified by the System Promotion Committee on the website pages of the Application Store without changes to its shape, color, or additional texts. In case there are other methods of use, the Applying Institution shall submit the MAS Mark additional use method application form to apply for such use with the System Promotion Committee.

   2.2 The Applying Institution shall not use the MAS Mark for purposes other than for the certification mark.

3. Use Basis of MarkThe Applying Institution using the MAS Mark shall comply with relevant provisions of the “Regulations for Mobile Application Autonomous Inspection Promotion System” and “Mobile Application Basic Security Mark Use and Management Regulations.”

4. Rights and Obligations of System Promotion Committee

   4.1 The System Promotion Committee may revise these regulations at any time due to provisions or requirements announced by the competent authority or the System Promotion Committee, and accordingly, for any part involving the Applying Institution due to such change directly, the Applying Institution shall be informed within a reasonable time-limit. After the Applying Institution receives such notice of a change, if it fails to express any dissenting opinions, it shall be treated to agree with such change.

   4.2 The System Promotion Committee shall announce the certificate numbers of MAS Mark on the website of the System Promotion Committee or make a public announcement via other methods.

5. Rights and Obligations of the Mobile Application Developer

   5.1 The Applying Institution agrees to accept irregular inspection by the System Promotion Committee at any time without refusal based on any excuses. In case the System Promotion Committee discovers that the Applying Institution fails to comply with the provisions of these regulations or requirements specified in the Mobile Application Basic Security Inspection Standard, the System Promotion Committee may inform the Applying Institution to stop its use of the MAS Mark and may announce such matter.

5.2 After the System Promotion Committee issues a notice or makes an announcement, the Applying Institution shall stop its use of the MAS Mark immediately, and relevant advertisement propaganda shall be recalled. When the System Promotion Committee issues a written notice requesting for improvement within a time-limit, and when re-inspection is implemented after the expiration of such time-limit, if the Applying Institution is still found to be non-complying with the regulations during the re-inspection, the System Promotion Committee may terminate its use of the Mark.

5.3 During the validity period of the MAS Mark, in case the System Promotion Committee discovers that the Applying Institution obtains the grant on the use of the MAS Mark through illegal means of fraud, threat, forgery or alteration etc., the System Promotion Committee may terminate its use of the Mark. The Applying Institution shall be responsible for the recall of advertisement propaganda and shall also indemnify the damages suffered by the System Promotion Committee due to such matter.

5.4 The Applying Institution agrees that when there is any change in the information of name or ownership etc. of a mobile application, it is necessary to submit relevant proof documents to report to the System Promotion Committee.

5.5 Within the valid period of the MAS Mark, where the Applying Institution is subject to any one of the following conditions, the System Promotion Committee shall terminate the Applying Institution's use right of the MAS Mark, and the Applying Institution shall not raise any objection:

a. Where the Applying Institution applies for termination of use.

b. Where the Applying Institution is subject to dissolution or cessation of business.

c. Where the profit-seeking enterprise registration certificate of the Applying Institution is revoked by the competent authority according to the law.

d. Where the Applying Institution violates the provision of Section 2 of these regulations.

e. Where the Applying Institution violates the provision of Section 6 of these regulations.

f. Where the Applying Institution violates the provisions Section 7.1 and Section 7.2 of these regulations and fails to provide a notice or fails to improve within the time-limit.

g. Where the Applying Institution avoids, hinders, or refuses any irregular inspection performed by the System Promotion Committee.

h. Where the Applying Institution obtaining the App certificate is under inspection or re-inspection, and it is found to fail to comply with the requirements of Mobile Application Basic Security Inspection Standard.

i. Where the MAS Mark of App certificate obtained by the Applying Institution according to the provision of Section 8.4 of the “Regulations for Mobile Application Basic Security Autonomous Inspection Promotion System” has become invalid. Where the MAS Mark uses the right of the Applying Institution is terminated by the System Promotion Committee, the System Promotion Committee shall inform the Applying Institution in writing about the stop of use of the MAS Mark and shall self-remove relevant marks from the Application Store within the time-limit. In the event that the Applying Institution fails to remove relevant marks within the time-limit, the Applying Institution shall indemnify all damages suffered by the Industrial Development Bureau, Ministry of Economic Affairs, or the System Promotion Committee.

6. Default Handling

6.1 The Applying Institution guarantees that this Mark shall be used for the mobile application described in Section 1 of these regulations only, and this Mark shall not be used for other mobile applications.

6.2 The MAS Mark use right obtained by the Applying Institution according to these regulations shall not be assigned, traded, or transferred to any third party. Where the Applying Institution violates this provision, the Applying Institution shall indemnify all damages suffered by the Industrial Development Bureau, Ministry of Economic Affairs, or the System Promotion Committee.

7. Responsibility

7.1 Where the Applying Institution is aware that its mobile application qualifying the MAS Mark may cause mobile devices to have the risks of improper access or disclosure, alteration, damage, or loss of personal data, then it shall inform the System Promotion Committee.

7.2 Where the System Promotion Committee is aware of the condition described in the preceding paragraph, it shall perform re-inspection on such a mobile application. If such mobile application is confirmed to have the likelihood of causing mobile devices to have the risks of improper access, or disclosure, alteration, damage, or loss of personal data, then the effect of the Mark shall be suspended, and the Applying Institution shall be ordered to improve within a time-limit.

7.3 The Applying Institution agrees that in case of violation of this document such that the rights and interests of the two parties of the Industrial Development Bureau, Ministry of Economic Affairs, or the System Promotion Committee are damaged, the Applying Institution agrees to bear the indemnification liability in full.

7.4 After the Applying Institution qualifies the review on the use of the MAS Mark and signs these regulations, it shall actively cooperate with various technical seminars, training lectures and promotional activities organized by the two parties of the Industrial Development Bureau, Ministry of

Economic Affairs and the System Promotion Committee to promote the MAS Mark.

8. Others

   8.1 For any disputes arising from the application, inspection, use, stop or termination of the MAS Mark, the Applying Institution shall clearly describe the reason and claim in writing to file an appeal with the System Promotion Committee within one month after the date of receiving relevant notice. The System Promotion Committee shall reply to the appeal result to the appellant within one month from the date of receiving the appeal letter.

   8.2 For any disputes arising from the application, inspection, use, stop, or termination of the MAS Mark, the Applying Institution may apply for mediation or may resolve such disputes according to the civil litigation procedure, and the Taipei District Court shall be the competent court of the first instance.

   8.3 All amended content of this document subsequently supplemented or amended shall be treated as an integral part of this document and shall have the same effect as this document.

(Blank below)

Appendix 7. “Mobile Application Basic Security Mark” Additional Use Request Application Form

Application Date: Month Date, Year

Name of Applicant	
App Name for Application	(Chinese) (English)
Explanation of Additional Request	(Please explain the request for additional labeling or the method for posting the security mark and its layout location in a list form)