**Notification of the Office of Insurance Commission**
**Re: Criteria, Procedure, and Conditions for Registration of Electronic Activities, Application for Approval for Third Party Service Providers, and Certification of Information Systems for Non-life Insurance Business**
**B.E. 2566 (2023)**

---

By virtue of Clause 22 and Clause 23 of the Notification of the Insurance Commission Re: Criteria and Procedure for the Issuing and Offering of Insurance Policies for Sale, and Making Payments or Indemnity Payments under Non-Insurance Contracts by Electronic Means B.E. 2566 (2023), the Office of Insurance Commission hereby prescribes this Notification as follows:

Clause 1 This Notification shall be called the Notification of the Office of Insurance Commission Re: Criteria, Procedure, and Conditions for Registration of Electronic Activities, Application for Approval for Third Party Service Providers, and Certification of Information Systems for Non-life Insurance Business B.E. 2566 (2023)".

Clause 2 The Notification of the Office of the Insurance Commission Re: Criteria, Procedure, and Conditions for Registration of Electronic Activities, Application for Approval for Third Party Service Providers, and Certification of Information Systems B.E. 2560 (2017) shall be repealed.

Clause 3 This Notification shall be in full force and effect from the date of its publication onwards.

Clause 4 In this Notification:

"Company" means a company that has obtained a license to engage in the non-life insurance business under the law on life insurance, and shall include branch offices of foreign non-life insurance Companies that have obtained licenses to engage in the non-life insurance business in the Kingdom of Thailand under the law on non-life insurance;

"Non-Life Insurance Broker" means a non-life insurance broker under the law on non-life insurance, but excluding Banks;

“Bank” means a bank that has obtained a Non-Life Insurance Broker license under the law on non-life insurance;

“Third Party Service Provider” means a person who has an information system for providing the offering insurance policies for sale by electronic means (Online), the offering of insurance policies for sale using electronic devices, the issuing of insurance policies by electronic, and making indemnity payments under insurance contracts by electronic means under the Notification of the Insurance Commission on Criteria and Procedure for Issuing and Offering of Insurance Policies for Sale, and Indemnity Payments under Non-Life Insurance Contracts by Electronic Means;

“Independent Auditor” means an external auditor who has been granted the certificate of the Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), ISO 27001 Lead Auditor;

“Internal Auditor” means an information technology auditor of the Company, who is independent from the information technology unit and has been granted the licenses of Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), ISO 27001 Lead Auditor;

"Certified Body” means an agency that has the duty to certify the information system according to the data security standards, namely, British Standards Institution (BSI) or Bureau Veritas or other agencies that have been registered by the Accreditation Body, namely, United Kingdom Accreditation Service (UKAS), ANSI-ASQ National Accreditation Board (ANAB), and the Thai Industrial Standards Institute (TISI) or other system certified bodies recognized by the Office;

“Office” means the Office of the Insurance Commission.

Clause 5 In certifying of the information system by the Independent Auditor or the Internal Auditor the Companies, the Non-Life Insurance Brokers, or the Banks or the Third-Party Service Providers, as the case may be, may use the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System).

Clause 6 The Company wishing to register shall file an application to the Office in form OrWor. 1 attached to this Notification, and submit along with the following documents and evidence, at a minimum:

(1) Documentation describing electronic activities and details;

(2) Flow chart and steps of electronic activities; ;

(3) Documentation describing the information system and the electronic means to accommodate the activities by electronic means;

(4) Strict security audit certification for information system of the activities under (1) by the Independent Auditor under the letter of confirmation in form OrWor. 3 attached to this Notification or certificate issued by the Certified Body, provided that the Company must present information to the satisfaction of the Office that the information system that has been certified under that certificate has the information system security at the strict level for the activities under (1);

(5) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3).

Clause 7 The Non-Life Insurance Broker or the Bank wishing to register shall file an application to the Office in form OrWor. 2 attached to this Notification, and submit along with the following documents and evidence, at a minimum:

(1) Documentation describing electronic activities and details;

(2) Flow chart and steps of electronic activities;;

(3) Documentation describing the information system and the electronic means to accommodate the activities by electronic means;

(4) Strict security audit certification for information system of the Company and the Non-Life Insurance Broker or the Bank for the activities under (1) by the Independent Auditor under the Certificate in form OrWor. 3 attached to this Notification or certificate issued by the Certified Body, provided that the Non-Life Insurance Broker or the Bank must present information to the satisfaction of the Office that the information system that has been certified under that certificate has the information system security at the strict level for the activities under (1);

(5) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(6) Company's letter of consent for offering of insurance policies for sale by electronic means (Online) .

Clause 8 In filing an application for registration and approval for a Third-Party Service Provider, the Company, or the Non-Life Insurance Broker, or the Bank shall file an application to the Office in form OrWor. 4 attached to this Notification, and submit along with the following documents and evidence, at a minimum:

(1) Documentation describing electronic activities and details;

(2) Flow chart and steps of electronic activities; ;

(3) Documentation describing the information system and the electronic means to accommodate the activities by electronic means ;

(4) Strict security audit certification for information system of the Third Party Service Provider and the Company, the Non-Life Insurance Broker, or the Bank for the activities under (1) by the Independent Auditor under the letter of confirmation in form OrWor. 3 attached to this Notification or certificate issued by the Certified Body, provided that the Company, the Non-Life Insurance Broker or the Bank must present information to the satisfaction of the Office that the information system that has been certified under that certificate has the information system security at the strict level for the activities under (1);

(5) Certification statement on clear policies and operating procedures, for example, the risk assessment system, the risk management system, the service process, the internal control, the security measures, and the contingency plan in the case that the Third Party Service Provider is unable to provide service;

(6) A copy of the information system service agreement between the Third Party Service Provider and the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, which covers the following conditions:

(a) Personal data security measures in compliance with the laws on personal data protection;

(b) Protection from unauthorized use or disclosure;

(c) Report of irregularities and breach of persona data;

(d) Responsibility of the Third Party Service Provider in the case of subcontracting whereby the Third Party Service Provider shall be responsible as if it has provided the service itself;

(e) Right to audit by the Company and the Office;

(f) Return, erasure, or deletion of personal data;

(g) Consequences of breach of conditions;

(7) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(8) Juristic person affidavit from the Department of Business Development in the case of the Third Party Service Provider juristic person.

Clause 9 In the case that the Company, the Non-Life Insurance Broker, or the Bank file an application for registration of electronic activities or approval for using a Third Party Service Provider but the supporting documents and evidence are not proper and complete, the Office will inform the Company, the Non-Life Insurance Broker, or the Bank to rectify documents and evidence or submit additional documents and evidence within the period specified by the Office.

If the Company, the Non-Life Insurance Broker, or the Bank fails to rectify documents and evidence or submit additional documents and evidence within the specified period without justifiable reason, the Office shall have the right to reject the application.

Clause 10 In consideration of the application for registration of electronic activities or the application for approval for using a Third Party Service Provider, the Office will consider the application within 30 days from the date on which the Office receives the application and a complete set of supporting documents or within 30 days from the date on which the Company has submitted the revised application and the supporting documents as the Office has given its opinion or observation for revision. With the exception in the case of any necessity or justifiable reason, the Office may extend the period, but it shall be no more than two extensions, each of which shall not exceed a period of 15 days. After approval has been granted, the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, must carry out the activities in accordance with the application for registration or approval at all times.

In the case of any revision, or change of information which has been approved, the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, shall take the following acts:

(1) In the case that the information system, that has been used with the activities, is materially beyond the scope of the certification if the existing information system, for example, the infrastructure, or the system, or the platform has been changed; or the Third Party Service Provider has caused the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, to perform a certification of the new information system by the Independent Auditor or the Certified Body and to file an application for approval for revision, or change of information under form PorWor. 1, PorWor. 6, or PorWor. 4 attached to this Notification and submit along with the revised supporting documents and evidence. If the Office does not inform the Company, the Non-Life Insurance Broker, or the Bank of the results of consideration or does not request the Company, the Non-Life Insurance Broker, or the Bank to give clarification or submit additional documents within 30 days from the date on which the Office receives the application or within 30 days from the date on which the Company has submitted the revised application and the supporting documents as the Office has given its opinion or observation for revision, the Company, the Non-Life Insurance Broker, or the Bank can carry out the activities in accordance with the application for approval.

(2) In the case that the Company, the Non-Life Insurance Broker, or the Bank has been registered for the offering insurance policies for sale by electronic means (Online) and is desirous to apply for additional group insurance products and commercial insurance products for the online offering for sale, the Company, the Non-Life Insurance Broker, or the Bank shall file an application for registration or approval in form PorWor. 1, PorWor. 6, or PorWor. 4 attached to this Notification and submit along with the revised supporting documents and evidence to the Office. In this regard, the Company, the Non-Life Insurance Broker, or the Bank will be able to carry out the activities in accordance with the application for approval only after the Registrar has granted approval.

Clause 11 In the offering insurance policies for sale by electronic means (Online), the offering of insurance policies for sale by using electronic devices, the issuing of insurance policies by electronic means, or the making indemnity payments under insurance contracts by electronic means, the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, shall cause the information system certification in accordance with the following criteria:

(1) To perform the information system certification every year, within a period of no longer than one year and to cause the information system certification by the Independent Auditor or the Internal Auditor or the Certified Body;

(2) To perform the information system certification every three years, within a period of no longer than three years and to cause to the information system certification by the Independent Auditor or the Certified Body

(3) in the case of the first application for registration for electronic activities or in the case of any material change to the registered system or in case of any material necessity, whereby additional certification is required for the information system, to cause to the information system certification by the Independent Auditor or the Certified Body.

In this regard, the Company, the Non-Life Insurance Broker, or the Bank, as the case may be, shall submit the results of certification within 30 days from the date of certification of the information system and submit the strict security audit certification for information system prepared by the auditor who performs the certification according to the certification type under paragraph one under the letter of confirmation in form OrWor. 3 attached to this Notification or submit the certificate issued by the Certified Body to the Office.

Notified on this 20th day of June B.E. 2566 (2023)

Secretary-General

Office of the Insurance Commission

Form OrWor. 1

Application for Registration of Electronic Activities and Certification of Information System

(Non-life Insurance Company)

Made at.....

Date:

.....

1. We,..... Public Limited Company, are desirous to apply for registration of electronic activities in order to use electronic means in the following matters:

(...)Offering insurance policies for sale by electronics means (Online)

(...)Offering insurance policies for sale using electronic devices

(...)Issuing insurance policies by electronic means

(...)Making of payments or indemnity payments under insurance contracts by electronic means

2. We have assigned Mr./Mrs./Miss.....to be the person responsible for the relevant information function that has been applied for registration or approval this occasion, at telephone number....., email.....

3. We hereby certify that our information system security standards are at the strict level for the activities under Clause 1 and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System).

4. We have enclosed the following documents:

(...)Documentation describing electronic activities and details (examples of screenshots);;

(...) Flow chart and steps of electronic activities;

(....) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(....) Certificate of information system security certification by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001) ;

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this

Notification (in the case of certification by the Independent Auditor under the Letter of Confirmation in form OrWor. 3).

We,..... Public Limited Company, hereby certify that the statements and information in this form OrWor. 1 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/Authorized Person of the Company

Form OrWor. 2 Page 1

Application for Registration of Electronic Activities and Certification of Information System

(Non-Life Insurance Broker or Bank)

Made at.....

Date:

.....

1. We,....., holding the Non-Life Insurance Broker License No. ....., expiring....., are desirous to apply for

(...) Offering insurance policies for sale by electronic means (Online) which has been consented by .....Public Company Limited in carrying out the activity;

(....) Offering insurance policies for sale using electronic devices.

2. We have assigned Mr./Mrs./Miss.....to be the person responsible for the relevant information function that has been applied for registration or approval this occasion, at telephone number....., email.....

3. We hereby certify that our information system security standards are at the strict level for the activities under Clause 1 and the information system has been certified by the Independent Auditor under the Letter of Confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System).

4. We have enclosed the following documents:

(...) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(....) Certificate of information system security certification by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the Letter of Confirmation in form OrWor. 3);

(...) Company's letter of consent for offering of insurance policies for sale by electronic means (Online).

We,....., hereby certify that the statements and information in this form OrWor. 2 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/

Authorized Person of the Non-Life Insurance Broker of the Bank

Form OrWor. 3 Page1

Letter of Confirmation

Information System Security Certification by Independent Auditor

Made at.....

Date:

.....

1. (.....) I,..... have been granted the ..... (CISA, CISM, CISSP, as the case may be) certificate....., which expires..... as detailed in the enclosed copy of the certificate (in the case of an individual).

(.....) Certified Body (name).....is a Certified Body of which the registration is not suspended or revoked and has been registered at..... as detailed in the enclosed copy of the registration.

2. I hereby certify that I have audit the information system of:

(...) ..... Public Limited Company

(...) .....Non-Life Insurance Broker or Bank

(...) .....Third Party Service Provider

for the use of electronic means in the following matters:

(...)Offering insurance policies for sale by electronic means (Online)

(...)Offering insurance policies for sale using electronic devices

(...)Issuing insurance policies by electronic means

(...)Making of payments or indemnity payments under insurance contracts by electronic means

and certify that the information system security standards are in accordance with the information system security standard evaluation guideline according to the strict-level security procedure specified in the attachments to this Notification

3. I have audited the information system in accordance with the professional principles and standards in the Notification of the Office of Insurance Commission Re: Criteria, Procedure, and Conditions for Registration of Electronic Activities, Application for Approval for Third Party Service Providers, and Certification of Information Systems B.E. 2565 (2022) and agree for the Office to verify the information of the Certificate with the issuing agency or the documents for registration of the Certified Body with the agency in Clause 1.

Affix stamp (if any)

Signed.....

.....

(.....)

Independent Auditor/ Certified Body

4. I, the person under Clause 2, hereby certify that the information given to the Independent Auditor for the certification of the information system security is factually accurate in all respects and affix my signature as evidence.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/ Authorized Person*

*Authorized Director/Authorized Person of the Company/the Non-Life Insurance Broker or the Third Party Service Provider, as the case may be.

Form OrWor. 4 Page 1

Application for Approval for Use of Third Party Service Provider and Certification of Information System

**Part 1: In the case that the Company uses the Third-Party Service Provider**

1. We,..... Public Limited Company, are desirous to apply for registration of electronic activities and apply for approval for the use of.....(specify the name of the Third Party Service Provider)..... in order to use electronic means in the following matters:

(...)Offering insurance policies for sale by electronic means (Online)

(...)Offering insurance policies for sale using electronic devices

(...)Issuing insurance policies by electronic means

(...)Making of payments or indemnity payments under insurance contracts by electronic means

2. We hereby certify that:

2.1 The Third Party Service Provider has the information system security standards are at the strict level for the activities under Clause 1 in accordance with the criteria specified in the attachments to this Notification and the information system has been certified by the Independent Auditor under the Letter of Confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System); and

We have the information system security standards which are at the strict level for the activities under Clause 1 and the information system has been certified by the Independent Auditor under the Letter of Confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System).

2.2 We have clear policies, processes, and operating procedures, for example, the risk assessment system, the risk management system, the service process, the internal control, the security measures, and the contingency plan in the case that the Third Party Service Provider is unable to provide service;

2.3 The information system service agreement between the Company and the Third Party Service Provider covers the following conditions:

(a) Personal data security measures in compliance with the laws on personal data protection;

(b) Protection from unauthorized use or disclosure;

(c) Report of irregularities and breach of persona data;

(d) Responsibility of the Third Party Service Provider in the case of subcontracting whereby the Third Party Service Provider shall be responsible as if it has provided the service itself;

(e) Right to audit by the Company and the Office;

(f) Return, erasure, or deletion of personal data;

(g) Consequences of breach of conditions.



3. We have enclosed the following documents:

(...) Juristic person affidavit from the Department of Business Development in the case of the Third-Party Service Provider juristic person

(...) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification of the Third-Party Service Provider by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Certificate of information system security certification of the by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(...) A copy of the information system service agreement between the Company and the Third-Party Service Provider.

**Part 2 In the case that the Non-Life Insurance Broker or the Bank uses the Third-Party Service Provider**

4. We, ....., holding the Non-Life Insurance Broker License No....., expiring ....., are desirous to apply for registration of electronic activities and apply for approval for the use of the information system of.....(specify the name of the Third Party Service Provider)..... in order to use electronic means in the following matters:

(...) Offering insurance policies for sale by electronic means (Online) which has been consented by .....Public Company Limited in carrying out the activity;

(....) Offering insurance policies for sale using electronic devices and has been consent by .....Public Company Limited in carrying out the activity above;

5. We hereby certify that:

5.1 The Third Party Service Provider has the information system security standards are at the strict level for the activities under Clause 4 in accordance with the criteria specified in the attachments to this Notification and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System); and

We have the information system security standards are at the strict level for the activities under Clause 4 and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certification of the information security management system with ISO/IEC 27001 (ISMS: Information Security Management System).

5.2 We have clear policies, processes, and operating procedures, for example, the risk assessment system, the risk management system, the service process, the internal control, the security measures, and the contingency plan in the case that the Third Party Service Provider is unable to provide service;

5.3 The information system service agreement between us and the Third Party Service Provider covers the following conditions:

(a) Personal data security measures in compliance with the laws on personal data protection ;

(b) Protection from unauthorized use or disclosure;

(c) Report of irregularities and breach of persona data;

(d) Responsibility of the Third Party Service Provider in the case of subcontracting whereby the Third Party Service Provider shall be responsible as if it has provided the service itself;

(e) Right to audit by the Company and the Office;

(f) Return, erasure, or deletion of personal data;

(g) Consequences of breach of conditions;

6. We have enclosed the following documents:

(...) Juristic person affidavit from the Department of Business Development in the case of the Third-Party Service Provider juristic person

(...) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification of the Third-Party Service Provider by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Certificate of information system security certification by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(...) A copy of the information system service agreement with the Third-Party Service Provider;

(...) Company's letter of consent for offering of insurance policies for sale by electronic means (Online).

☐ Company ☐ Non-Life Insurance Broker or Bank .....hereby certifies that the statements and information in this form OrWor. 4 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/ Authorized Person*

*Authorized Director/Authorized Person of the Company/Non-Life Insurance Broker/Bank, as the case may be,

Form PorWor. 1 Page1

Notice of Change and Certification of Information System Form

(Non-life Insurance Company)

Made at.....

Date:

.....

1. We,..... Public Limited Company, are desirous to notify the change(s) to the registration of electronic activities in the following matters:

(...)Offering insurance policies for sale by electronic means (Online)

(...)Offering insurance policies for sale using electronic devices

(...)Issuing insurance policies by electronic means

(...)Making of payments or indemnity payments under insurance contracts by electronic means

Details of the change.....

.....

.....

2. We have assigned Mr./Mrs./Miss.....to be the person responsible for the relevant information function has been applied for registration or approval this occasion, at telephone number....., email.....

3. We hereby certify that our information system security standards are at the strict level for the activities under Clause 1 and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001).

4. We have enclosed the following documents: (only the documents concerning changes)

(....) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3).

We,.....Public Limited Company, hereby certify that the statements and information in this form OrWor. 1 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/ Authorized Person of the Company

Form PorWor. 2 Page1

Notice of Change and Certification of Information System Form

(Non-Life Insurance Broker or Bank)

Made at.....

Date:

.....

1. We,....., holding the Non-Life Insurance Broker License No. ....., expiring....., are desirous to notify the change(s) to the registration of electronic activities in the following matters:

(...) Offering insurance policies for sale by electronic means (Online) which has been consented by .....Public Company Limited in carrying out the activity;

(....) Offering insurance policies for sale using electronic devices.

Details of the change.....

.....

2. We have assigned Mr./Mrs./Miss.....to be the person responsible for the relevant information function that has been applied for registration or approval this occasion, at telephone number....., email.....

3. We hereby certify that our information system security standards are at the strict level for the activities under Clause 1 in accordance with the criteria specified in the attachments to this Notification and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001).

4. We have enclosed the following documents: (only the documents concerning changes)

(....) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification by the Independent Auditor in form OrWor. or the certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(...) Company's letter of consent for offering of insurance policies for sale by electronic means (Online)

We,....., hereby certify that the statements and information in this form OrWor. 2 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/ Authorized Person of the Non-Life Insurance Broker or Bank

Form PorWor. 4 Page 1

Notice of Change and Certification of Information System Form

**Part 1: In the case that the Company uses the Third-Party Service Provider**

1. We ..... Public Limited Company, are desirous to notify the following change(s) to the registration of electronic activities and the use of the information system of .....(specify the name of the Third Party Service Provider).....in the following matters:

(...) Offering insurance policies for sale by electronic means (Online)

(...) Offering insurance policies for sale using electronic devices

(...) Issuing insurance policies by electronic means

(...) Making of payments or indemnity payments under insurance contracts by electronic means

Details of the change.....

.....

.....

2. We hereby certify that:

2.1The Third Party Service Provider has the information system security standards are at the strict level for the activities under Clause 1 in accordance with the criteria specified in the attachments to this Notification and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001); and

We have the information system security standards are at the strict level for the activities under Clause 1 and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001).

2.2We have clear policies, processes, and operating procedures, for example, the risk assessment system, the risk management system, the service process, the internal control, the security measures, and the contingency plan in the case that the Third Party Service Provider is unable to provide service;

2.3 The information system service agreement between the Company and the Third Party Service Provider covers the following conditions:

(a) Personal data security measures in compliance with the laws on personal data protection ;

(b) Protection from unauthorized use or disclosure;

(c) Report of irregularities and breach of persona data;

(d) Responsibility of the Third Party Service Provider in the case of subcontracting whereby the Third Party Service Provider shall be responsible as if it has provided the service itself;

(e) Right to audit by the Company and the Office;

(f) Return, erasure, or deletion of personal data;

(g) Consequences of breach of conditions.

3. We have enclosed the following documents:

(...) Juristic person affidavit from the Department of Business Development in the case of the Third-Party Service Provider juristic person;

(...) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification of the Third-Party Service Provider by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Certificate of information system security certification of the Company by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001)

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(...) A copy of the information system service agreement between the Company and the Third-Party Service Provider.

**Part 2 In the case that the Non-Life Insurance Broker or the Bank uses the Third-Party Service Provider**

4.We,....., holding the Non-Life Insurance Broker License No. ....., expiring....., are desirous to apply for registration of electronic activities and apply for approval for the use of the information system service of .....(specify the name of the Third Party Service Provider)..... in the following matters:

(...) Offering insurance policies for sale by electronic means (Online) which has been consented by .....Public Company Limited in carrying out the activity;

(....) Offering insurance policies for sale using electronic devices.

Details of the change.....

.....whi
ch has been consented by .....Public Company Limited in carrying out the activity above;

5. We hereby certify that:

5.1 The Third Party Service Provider has the information system security standards are at the strict level for the activities under Clause 4 in accordance with the criteria specified in the attachments to this Notification and the information system has been certified by the Independent Auditor under the letter of confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001); and

We have the information system security standards are at the strict level for the activities under Clause 4 and the information system has been certified by the Independent Auditor under the Letter of Confirmation in form OrWor. 3 or the certificate issued by the Certified Body (ISO27001).



5.2 We have clear policies, processes, and operating procedures, for example, the risk assessment system, the risk management system, the service process, the internal control, the security measures, and the contingency plan in the case that the Third Party Service Provider is unable to provide service;

5.3 The information system service agreement between us and the Third-Party Service Provider covers the following conditions:

(a) Personal data security measures in compliance with the laws on personal data protection;

(b) Protection from unauthorized use or disclosure;

(c) Report of irregularities and breach of persona data;

(d) Responsibility of the Third Party Service Provider in the case of subcontracting whereby the Third Party Service Provider shall be responsible as if it has provided the service itself;

(e) Right to audit by the Company and the Office;

(f) Return, erasure, or deletion of personal data;

(g) Consequences of breach of conditions.

6. We have enclosed the following documents:

(...) Juristic person affidavit from the Department of Business Development in the case of the Third-Party Service Provider juristic person

(...) Documentation describing electronic activities and details (examples of screenshots);

(...) Flow chart and steps of electronic activities;

(...) Documentation describing the information system and the electronic means in accommodating the activities using electronic means (system architecture);

(...) Certificate of information system security certification of the Third-Party Service Provider by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Certificate of information system security certification by the Independent Auditor in form OrWor. 3 or certificate issued by the Certified Body (ISO27001);

(...) Information system security standard evaluation guideline according to the strict-level security procedure in accordance with the criteria specified in the attachments to this Notification (in the case of certification by the Independent Auditor under the letter of confirmation in form OrWor. 3);

(...) A copy of the information system service agreement with the Third-Party Service Provider;

(...) Company's letter of consent for offering of insurance policies for sale by electronic means (Online).

☐ Company ☐ Non-Life Insurance Broker or Bank.....hereby certify that the statements and information in this form OrWor. 4 are factually accurate in all respects.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/ Authorized Person*

*Authorized Director/Authorized Person of the Company/Non-Life Insurance Broker/Bank, as the case may be.

Attachment

Information System Security Standard Evaluation Guideline

according to the Strict-Level Security Procedure

| Subject | Details |
|---|---|
| **1. Cooperation for management security** | |
| 1.1 To determine the information system security policy with an approval and encouragement from high-level executives, and make the policy for all employees and relevant third parties broadly known.<br>1.2 To formulate following-up and evaluation plan for the use of the information system security, and the information system security policy on a regular basis for the purpose of adjustment in in case of any changes within the agency, in order for the plan to be suitable for any situations and efficient at all times. | |
| **2. Structuring of the information system with regard to information system security management within and outside the agency or organization** | |
| 2.1 High-level executive of the agency responsible for information-related works to provide support and clearly direct the operations relating to the information security, as well as clearly to delegate relevant tasks to workers, to be responsible for any cases of risk, damage or hazard to the information system.<br>2.2 In case of a new information system, to ensure that there is reviewing process as to approve the formulation, installation, or use in various aspects, for example, management of system users, or interoperability between the existing and new systems.<br>2.3 To define a confidentiality agreement or non-disclosure agreement appropriate to the situation and requirements of the agency to protect the data and information.<br>2.4 To have in place the information security rules regarding the permission of a third-party service users to access the information system or use the data and information of the agency.<br>2.5 The agreement granting Third Party Service Providers a permission to access the information system or use the information the agency for the purposes of reading, processing, management, or development of the information system shall include the rules on information security therein. | |

| Subject | Details |
|---|---|
| 2.6 Contents of the works or details of responsibilities regarding the information security are clearly defined.<br>2.7 Steps and channels to engage a third-party agency with a particular area of expertise, or an agency expert on information security under various circumstances are clearly defined.<br>2.8 To ensure that the information system security standard evaluation guideline is reviewed on a regular basis or upon any changes in the operation by a person independent therefrom.<br>2.9 To form cooperation amongst the persons having roles relating to information security of the agency in any work or activity relevant to information security.<br>2.10 Steps and channels to engage a third-party agency with a duty to regulate or an agency relating to enforcement of law, including an agency monitoring emergency circumstances under various circumstances are clearly defined.<br>2.11 Before granting permission for an agency or a third party to access the information system or use the data and information of the agency, the potential risks that may arise therefrom must be identified and the guidelines to prevent such risks must be formulated. | |
| **3. Management of Information Assets** | |
| 3.1 Information asset data are stored and recorded. The data stored shall comprise data that is necessary for searching for future use.<br>3.2 A person with the duties to monitor the use of and be responsible for the information assets are clearly designated.<br>3.3 Rules and regulations on use of the information assets must be clearly defined in a form of documentation and announced and enforced within the agency.<br>3.4 Data and information are categorized based on their value, legal requirements, level of confidentiality and importance to the agency.<br>3.5 Appropriate procedures for data and information categorization are defined and put in place, and the information are handled in accordance | |

| Subject | Details |
|---|---|
| with the guidelines for data and information categorization applied by the agency. | |
| **4. Cooperation for personnel security** | |
| 4.1 Duties and responsibilities on information security of the employees, or the agency, or a third party that has been engaged are defined to be in line with the information security and the policy to maintain the information security put in place by the agency.<br>4.2 High-level executives of the agency must ensure that the employees, or the agency, or a third party that has been engaged operate their works in compliance with the policy or the security practice guidelines put in place by the agency.<br>4.3 Internal punishment procedures for an employee who violates the policy, or the security practice guidelines is formulated.<br>4.4 To clearly define the duties and responsibilities on termination of employment or change of employment status, and to clearly designate a responsible person.<br>4.5 The employees of the agency or a third party that has been engaged must return the information assets of the agency upon their employee status ceasing, or expiration of employment contract, or the engagement agreement to the agency,<br>4.6 To revoke authorization of the employees of the agency of a third party to access the information system upon their employee status ceasing, or expiration of employment contract, or agreement to operate works, and appropriately adjust the authorization level for accessing of the information system upon any change in duties and responsibilities.<br>4.7 The employees or third parties must receive training to create awareness regarding the information security in the part relating to their duties and responsibilities and be informed of the policy or the practice guidelines for information security enforced by the agency on a regular basis, or upon any changes. | |

| Subject | Details |
|---|---|
| 4.8 In considering hiring an employee, or engaging an agency or a third party, their profiles or qualifications must be verified in order to be in compliance with the relevant laws, rules and regulations, and ethics by taking into account the confidentiality level of the data and information for which the access is granted, and the assessed risk level.<br>4.9 The employment contract or the engagement agreement of the employees, or the agreement to engage an agency or a third party must include the duties and responsibilities regarding the information security. | |
| **5. Cooperation for physical and surrounding security** | |
| 5.1 To ensure the security perimeter for the location of where the agency that the information system and the data and information are installed, stored, or used.<br>5.2 Physical security must be designed and installed to prevent any external perils, disasters whether man-made or act of god, for example, fire, flood, earthquake, explosion, riot.<br>5.3 To place and protect the information equipment to mitigate risks from natural disasters or hazard, and to prevent any unauthorized access.<br>5.4 To prevent the information equipment from power failure, or interruption due to malfunction of supporting utilities' infrastructure.<br>5.5 The information equipment is properly maintained for the purposes of accuracy, completeness, and ready-to-use at all times.<br>5.6 Physical security must be designed and installed to ensure prevention for the premise, or place of operation, or the information equipment.<br>5.7 Without authorization, the information equipment, data and information, or software should not be relocated from the place of operation of the agency.<br>5.8 The access to and exit from the secure area must be controlled, i.e., only authorized persons are allowed to access to and exit from the secure area.<br>5.9 Preventive guidelines for working in the secure area must be designed and implemented. | |

| Subject | Details |
|---|---|
| 5.10 The areas to which an unauthorized person may have access, for example, pick-up point, must be controlled, or if applicable, such areas should be separated from the area where the information system and the data and information are installed, stored, or used in order to prevent any unauthorized access.<br>5.11 Communications cable or electrical wires are protected from any interception or damage.<br>5.12 The information equipment used outside the agency's place of operation are maintained and secured based on risk levels which are varied with the uses in each location.<br>5.13 Before cancelling the use or selling the information equipment used in storing of the information, such information equipment must be verified whether or not the material information or software purchased and installed are erased, moved, or destroyed by mean causing the information or software unrecoverable. | |
| **6. Communications Management, and Operations of Computer Network Systems, Computer Systems, Computer Work Systems, and the Information System** | |

| Subject | Details |
|---|---|
| 6.1 Operation manual is updated and maintained so that it is in a ready-to-use condition for the employees to put into practice.<br>6.2 To ensure that a third-party or an external agency engaged to provide service to the agency perform the contract or service agreement which must cover the security work, nature of service provision, and level of service.<br>6.3 The reports or records of service provision of a third party or an external agency engaged to provide service to the agency are regularly monitored and verified.<br>6.4 To ensure the criteria for inspection and acceptance of the information system which is updated or of a new version. The information system should be tested during development and before the inspection and acceptance.<br>6.5 To ensure that there are procedures to control the verification, protection, and recovery in case of a malware, and create awareness on malware to the users of the information system or the data and information.<br>6.6 To ensure the back-up of the information, and the restoration in accordance with the information back-up policy put in place by the agency.<br>6.7 To ensure the management of the control of the computer network to prevent any threats and ensure the security of the information system and applications operating on the computer network, as well as the data and information exchanged on the network.<br>6.8 The maintenance of the security, level of service, management requirements are defined in the computer network service agreement, whether the service is provided by the agency itself or subcontracted to a third-party service provider.<br>6.9 To ensure that there are a policy and operating procedures, as well as a control of the information exchange via communication channel in an electronic form. | |

| Subject | Details |
|---|---|
| 6.10 To ensure that there is an agreement on an exchange of the data and information or software between the agency and a third-party or an external agency.<br>6.11 To ensure that there are a policy and operating procedures to protect the data and information communicated or exchanged via the information system connected to other information systems.<br>6.12 To protect the data and information exchanged in an electronic commerce transaction via a public computer network to prevent any fraud, breach of contract, or data leakage, or the information is modified without authorization.<br>6.13 To protect the data and information communicated or exchanged in online transaction to prevent any incomplete transmission, or displacement, or leakage of data, or the information is modified, replicated, or sent without authorization.<br>6.14 For the data and information which are publicized to the public, the information shall be protected from any modification without authorization in order to maintain the completion and accuracy of the data and information.<br>6.15 To ensure the recording of the audit log which records the activities of users of the information system, and events relating to security matters, for the purposes of future investigation, and monitoring of access control.<br>6.16 To ensure that there are procedures in monitoring the use of the information system, and evaluation of such monitoring on a regular basis.<br>6.17 To protect the information system on which the logs and log data are stored from any unauthorized access or modification.<br>6.18 To ensure that the logs relevant to the maintenance of the information system is recorded by the system administrator or system operator.<br>6.19 The changes to the information system must be controlled and restricted. | |

| Subject | Details |
|---|---|
| 6.20 The use of the information resources must be monitored, and the plan on the information resources must be formulated to be able to appropriately accommodate future operation.<br>6.21 Operating procedures for the data and information management and storage must be set to prevent any leakage or misuse of information.<br>6.22 To ensure that the logs relevant to any errors of the information system are recorded, such logs are analyzed on a regular basis, and any detected errors must be rectified appropriately.<br>6.23 The time systems of each information system used in the agency or in the security domain must demonstrate synchronization with the settings based on the time from the reliable source.<br>6.24 The duties and scope of responsibilities are clearly defined to mitigate any mistake in changing to or misuse of the information system or the data and information.<br>6.25 The information systems for development, test, and practical use are separated to mitigate risks from any unauthorized access or change in the information system.<br>6.26 Any changes relating to the preparation of service provision and the improvement of the information system security policy, operating procedures, or the control on the information security are managed by taking into consideration, on a continual basis, the significance level of the operation of the relevant businesses, and the risk assessment.<br>6.27 In the case where the agency allows for the use of mobile code (such as a certain Script of a web application that automatically executes upon launching a webpage), the configuration should be set to ensure that the mobile code works in compliance the information security and the information system security policy, and the mobile code must not automatically be able to execute in the information system if the information system security policy forbids the mobile code of such category from execution. | |

| Subject | Details |
|---|---|
| 6.28 The operating procedures for the management of equipment used in electronic data recording which can be removed or connected to a computer (removable media) must be set.<br>6.29 The operating procedures for safely and securely destroying equipment used in electronic data recording which can be removed or connected to a computer (removable media) must be set.<br>6.30 The information or documents relating to the information system (system documentation) are protected from any unauthorized access.<br>6.31 In the case where the equipment used in storing the data and information is relocated, it must be protected to protect the equipment from any unauthorized access or misuse, or to protect the equipment or the data and information from damage.<br>6.32 The data and information electronically communicated (electronic messaging) must be protected, for example, e-mail, electronic data interchange (EDI), or instant messaging. | |
| **7. Access Control for Computer Network Systems, Computer Systems, Computer Work Systems, Information Systems, Information, Data and information, Electronic Data, and Computer Data** | |
| 7.1 Access control policy must be formulated in a form of documentation and ensure that the subject matter of the policy is in line with the requirements or demands with respect to the operation or service provision and maintenance of security of the information system.<br>7.2 Users of the information system must be registered, and user accounts must be officially cancelled to control the granting and cancellation of access authorization for any information system of the agency.<br>7.3 High-level authorization of access must be granted limitedly and under supervision.<br>7.4 Users must maintain and protect any of the information equipment under their responsibility when the equipment is not in used. | |

| Subject | Details |
|---|---|
| 7.5 Access to the agency's computer network accessible from outside the agency must be restricted in accordance with the access control policy and the terms of use of the application for operation.<br>7.6 All users must have their own user accounts, and the information system must comprise adequate identification technique to be able to identify the users of the information system.<br>7.7 The information system screen must be terminated or closed automatically if there is no activity for a maximum time of the period specified.<br>7.8 The access of the users and the information system administrator or system operator to the data and information and functions in applications must be restricted in line with the access control policy so formulated.<br>7.9 The security management policy and guideline must be formulated to mitigate the risks in the use of the information equipment or mobile communication devices, for example, laptops or smart phones.<br>7.10 Rules to which require the users to be complied must be established in order for the users to securely set the password as required by the agency.<br>7.11 The users must be able to access the computer network services for which they have authorization for only.<br>7.12 An adequate identification method must be set in order to control any remote access to the information system of the agency.<br>7.13 The access channels whether physical and via computer-connection for maintenance of the information systems which can be access remotely, for example, remote diagnostic or configuration facility of the computer network equipment, must be controlled.<br>7.14 In a computer network, the data and information must be categorized properly based on their service types provided to the group of users of the data and information. | |

| Subject | Details |
|---|---|
| 7.15 The flow data and information in a computer network must be controlled to ensure the compliance with the access control policy of the application.<br>7.16 Logging-in procedures must be set to control the access to the computer operating system.<br>7.17 An interactive password management system must be prepared or arranged, and that system must be able to support a use of secured passwords.<br>7.18 A password setting management procedure must officially be set.<br>7.19 A designated executive must officially monitor and review authorization level of the users on a regular basis.<br>7.20 A clear desk policy for the data and information in a documentation form and in an electronic form recorded in a removable media, as well as a clear screen policy for the information system, must be formulated.<br>7.21 An automatic equipment identification must be arranged in order to verify whether or not a connection of equipment is actually made from that equipment or from a designated location only. It is necessary for the information system to allow only connections made by or from an authorized equipment or location.<br>7.22 An access to utility programs must be strictly restricted for such programs may be able to control and change an operation of the information system.<br>7.23 A period of a connection to the information system that demonstrates high risk level must be limited as to improve the security level.<br>7.24 For the information system of high importance, the information system must operate in a separated environment and not confound with other information system.<br>7.25 A policy, work plan, and procedure in operation relating to any activity operated from outside the agency (teleworking) must be formulated. | |

| Subject | Details |
|---|---|
| **8. Procurement or Arrangement, and Maintenance of Computer Network Systems, Computer Systems, Computer Work Systems, and Information Systems** | |
| 8.1 Requirements for the information security control must be set in the preparation of minimum requirements of a new information system or an update to the existing information system.<br>8.2 Subcontracted software development works must be monitored, controlled, and inspected.<br>8.3 Any data to be accepted into an application must always be validated to ensure that the data is accurate and in a compatible format.<br>8.4 Any data derived from a data processing of an application must be validated to ensure that the data is accurate and in a compatible format.<br>8.5 A key management guideline must be set to support a technique relevant to an encryption of the agency.<br>8.6 A set of the data and information to use in a test of the information system must carefully be selected, as well as a data leakage control and prevention policy must be formulated.<br>8.7 An access to source codes of a program must be restricted.<br>8.8 In the case of any change in a computer operating system, significant programs' execution must be verified, reviewed, and tested to ensure that such change does not affect the security of the information system and the service provision of the agency.<br>8.9 An execution of application must be validated for any error of data which may arise from an erroneous execution or processing.<br>8.10 Minimum requirements must be set for the maintenance of authenticity and integrity of the data in an application, as well as an appropriate preventive procedure must be formulated and complied with.<br>8.11 A policy on the use of encryption-related techniques must be formulated.<br>8.12 Operating procedures to control an installation of software on the information system in service must be set. | |

| Subject | Details |
|---|---|
| 8.13 Any changes in the development of the information system must be controlled with an official controlling procedure.<br>8.14 Any changes to a software package must be restricted, provided changes must be made in the case of necessity, and every change must be strictly controlled.<br>8.15 A preventive measure must be arranged to mitigate a leakage of the data and information. | |
| **9. Management of Undesirable or Unforeseeable Security Situations** | |
| 9.1 An undesirable or unforeseeable security situation must be reported via an appropriate management channel as soon as practicable.<br>9.2 An employee or a third-party user must record and report any weak point which may have found while using the information system.<br>9.3 The scope of responsibilities of the executives and the operating procedures must be defined in order to be able to effectively deal with any undesirable or unforeseeable security situations in a timely manner.<br>9.4 In the process of following up with a person or agency, if there is an undesirable or unforeseeable security situation which is relating to a legal action (whether civil or criminal), evidence must be collected, kept, and presented in compliance with the provision of the application laws. | |
| **10. Management of Service or Operation of Agency or Organization for the Purpose of Continuity** | |
| 10.1 A plan for maintenance or recovery of information service after any event causing operation interruption must be formulated in order for the data and information to be in a ready-to-use condition in a specified level and within the specified time.<br>10.2 Necessary requirements on information security must be defined as a part of the management procedures to achieve continuity in operation during any emergency incident.<br>10.3 Main framework for the development of management plan must be set to achieve continuity in operation during any emergency incident. | |

| Subject | Details |
|---|---|
| 10.4 The management plan must be regularly tested and improved to achieve continuity in operation during any emergency incident as to ensure that the plan is always up-to-date and effective.<br>10.5 Any events which may cause operation interruption, and possibility of the event causing impact, as well as continual result from such interruption in the information security aspect must be identified. | |
| **11. Examination and evaluation of Compliance to Any Policies, Measures, Criteria, or Procedures, as well as Security Requirements of the Information System** | |
| 11.1 A guideline for the operation of the information system which is in compliance with the law and in line with the and provisions under agreements of the agency must be clearly specified in a form of document which is updated regularly.<br>11.2 Misuse of the information system must not be allowed.<br>11.3 The employees of the agency must ensure that the information security works under their responsibilities are in compliance with the law and in line with the and provisions under agreements of the agency.<br>11.4 Personal data must be protected in compliance with the law and in line with the provisions under agreements of the agency.<br>11.5 An encryption technique that is in compliance with the law and in line with the and provisions under agreements of the agency must be put in place.<br>11.6 Technical review and validation of the information system must be arranged on a regular basis to satisfy the information security development standard.<br>11.7 Validation requirements and activities relevant to the validation of the information system must be planned and arranged as to mitigate any service provision interruption risks.<br>11.8 An access to use any validation tools must be allowed to protect the tools from being misused or compromised.<br>11.9 Operating procedures must be set to ensure that the use of information which may deemed an intellectual property, or the use of a | |

| Subject | Details |
|---|---|
| software is in compliance with the law and in line with the and provisions under agreements.<br>11.10 The material data and information must be protected from any damage, loss, or falsification, provided the protection must be carried out in compliance with the law and in line with the and provisions under agreements of the agency and the terms of service. | |

(...) .....Public Company Limited

(...) .....Non-Life Insurance Broker or Bank

(...) .....Third Party Service Provider

hereby certify that the statements and information in this document are factually accurate in all respects and are willing to submit the information relating to the audit of the information system security standards.

Affix stamp (if any)

Signed.....

.....

(.....)

Authorized Director/Authorized Person*

* Authorized Director/Authorized Person of the Company/Non-Life Insurance Broker/Bank, as the case may be.