GOVERNMENT **--------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independent - Freedom – Happiness** **----------**
No. 85/2016/ND-CP	*Hanoi, July 01, 2016*

DECREE

ON THE SECURITY OF INFORMATION SYSTEMS BY CLASSIFICATION

Pursuant to the Law on Government Organization dated June 19, 2015;

Pursuant to the Law on security of information over network dated November 19, 2015;

At the request of the Minister of Information and Communication;

The government promulgates the Decree on the security of information systems by classification.

Chapter I

GENERAL

Article 1. Scope

This Decree defines criteria, authority, procedures and formalities to classify the safety of information systems and responsibilities for securing information systems by classification.

Article 2. Regulated entities

This Decree applies to organizations and individuals participating or being involved in the construction, configuration, administration, operation, upgrade and expansion of Vietnam-based information systems that service the application of information technology in the activities of government bodies and agencies and in the provision of online services to the people and enterprises.

Relevant entities are encouraged to adopt this Decree for protecting their information systems.

Article 3. Terminology

In this Decree, the following words and phrases are construed as follows:

1. Administrators of an information system refer to authorities, organizations and individuals given authority to manage the information system directly. In government bodies and agencies, administrators of information systems refer to ministers, ministerial-level bodies, government

agencies, provincial People's Committees or entities given discretion in investment projects for the construction, configuration, upgrade and expansion of such information systems.

2. Processing of information refers to the action(s) of generating, providing, collecting, editing, using, storing, transmitting, sharing and exchanging information online.

3. Operators of an information system refer to agencies and organizations that the administrators of the information system designate to operate such system. If the administrators of an information system outsource information technology services, the operators of the information system shall be providers of such services.

4. Specialized information technology units have a functional role in information technology in ministries, ministerial-level bodies, government agencies, provincial Departments of Information and Communications and in the administrators of information systems, which are designated by such administrators.

5. Specialized information security units bear functions and missions to secure the data for administrators of information systems.

6. Information security divisions are formed or designated by administrators of information systems to carry out missions of securing data and responding to network-related information issues.

7. Online services are provided by enterprises or government agencies over a network to organizations and individuals.

Article 4. Principles of security of information systems by classification

1. Information systems concerning operations of agencies and organizations shall be secured by classification into a routine and on the basis of continuity in design, construction, operation and termination in accordance with standards and technical regulations.

2. Information systems concerning operations of agencies and organizations shall be secured comprehensively, synchronously and centrally with regard to investing in protective solutions and sharing resources to optimize performance and preclude redundant and overlapping investments.

3. Resources to secure information systems shall be allocated in descending order of priority.

Article 5. Principles of classification

1. The identification of an information system for later classification is subject to these principles:

a) The information system is solely subjected to an administrator;

b) The information system can operate independently and takes shape to service or facilitate professional operations and specific business activities of organizations and agencies, as defined in Section 2, Article 6 of this Decree.

2. If an information system is comprised of various constituent systems classified differently, the entire system shall adopt the highest among classifications of constituent systems.

Chapter II

CRITERIA OF CLASSIFICATION

Article 6. Classification of information and information systems

1. The confidentiality level of the information processed by an information system is classified as follows:

a) Public information is the online data that an organization or individual owns and discloses to every entity without identifying and locating such entities;

b) Private information is the online data that an organization or individual owns and does not disclose or only provides to one or some entities identified and located;

c) Personal information is the online data related to the identification of a particular person;

d) Classified state information are the data classified as confidential, secret and top secret in conformity to the laws on protection of classified state information.

2. An information system shall be classified by professional function as follows:

a) An information system that services internal activities solely contributes to the internal management and operation of an agency or organization;

b) An information system that is of use to the people and enterprises provide directly or support the provision of online services, e.g. online public services and other online services regarding telecommunications, information technology, commerce, finance, banking, health, education and other specialties;

c) A system of information infrastructure is comprised of equipment and transmission lines that serve organizations and agencies en masse, e.g. wide area networks, database, data centers, cloud computing, electronic authentication, digital verification, digital signature, interconnection of information systems;

d) An industrial maneuver information system has the functional role in supervising and collecting data, managing and controlling vital sections for maneuvering and operating the ordinary activities of buildings;

dd) Other information systems.

Article 7. Criteria of first class

A 1st-class information system serves internal operations of an organization or agency and only processes public information.

Article 8. Criteria of second class

A 2nd-class information system shall meet one of these criteria:

1. An information system that serves internal operations of an organization or agency, processes private information and personal information of users but does not handle classified state information.

2. An information system that serves the people and enterprises in one of these manners:

a) Provide information and online public services at level 2 or lower as per the law;

b) Provide online services that are not stated in the list of conditional business services;

c) Provide other online services of processing private and personal information of less than 10,000 users.

3. A system of information infrastructure that is of use to an organization or agency.

Article 9. Criteria of third class

A 3rd-class information system shall meet one of these criteria:

1. An information system that processes classified state information or services the national defense and security and whose sabotage compromises the defense and security of the country.

2. An information system that serves the people and enterprises in one of these manners:

a) Provide information and online public services at level 3 or higher as per the law;

b) Provide online public services that are defined in the list of conditional business services;

c) Provide other online services of processing private and personal information of 10,000 or more users.

3. A system of shared information infrastructure that is of use to agencies and organizations in an industry, a province or some provinces.

4. An industrial maneuver information system that directly services the maneuver and operation of ordinary activities of buildings of grade II, III or IV as per the regulated gradation of construction.

Article 10. Criteria of fourth class

A 4th-class information system shall meet one of these criteria:

1. An information system that processes classified state information or services the national defense and security and whose sabotage gravely compromises the defense and security of the country.

2. A national information system that services the development of the electronic government, functions on round-the-clock basis and does not halt without prior schedule.

3. A system of shared information infrastructure that services agencies and organizations on nation-wide scale and round-the-clock basis and does not halt without prior schedule.

4. An industrial maneuver information system that directly services the maneuver and operation of ordinary activities of buildings of grade I as per the regulated gradation of construction.

Article 11. Criteria of fifth class

A 5th-class information system shall meet one of these criteria:

1. An information system that processes classified state information or services the national defense and security and whose sabotage causes excessively grave detriment to the defense and security of the country.

2. An information system that services the centralized storage of particularly vital information and data of the country.

3. A system of national information infrastructure that connects Vietnam with the world.

4. An industrial maneuver information system that directly services the maneuver and operation of ordinary activities of special-graded buildings as per the regulated gradation of construction or vital buildings concerning national security according to legal regulations on national security.

5. Other information systems at the discretion of the Prime Minister.

Chapter III

AUTHORITY, PROCEDURE AND FORMALITIES OF CLASSIFICATION

Article 12. Authority to verify and validate classifications

1. For an information system to be given class 1 or class 2:

The specialized information security unit of the administrator of the information system shall verify and validate the proposal for the classification of the information system at class 1 or class 2.

2. For an information system to be given class 3:

a) The specialized information security unit of the administrator of the information system shall verify the classification proposal;

b) The administrator of the information system shall validate the classification proposal.

3. For an information system to be given class 4 or class 5:

a) Ministry of Information and Communications shall lead and cooperate with the Ministry of National Defense and Ministry of Public Security in verifying the classification proposal, unless otherwise governed by Point b and Point c, Section 3 of this Article;

b) Ministry of National Defense shall lead and cooperate with the Ministry of Information and Communications, relevant ministries and bodies in verifying the proposal for classification of information systems under the management of the Ministry of National Defense;

c) Ministry of Public Security shall lead and cooperate with the Ministry of Information and Communications, relevant ministries and bodies in verifying the proposal for classification of information systems under the management of the Ministry of Public Security;

d) The administrator of such information systems shall validate the proposal for classification of the information systems at class 4 and validate the information security proposal of the information systems classified at class 5;

dd) Prime Minister shall validate the list of information systems classified at class 5 (List of national vital information systems).

Article 13. Procedure and formalities for classification upon new investment projects or expansion and upgrade of information systems

1. The investor shall provide and include explanations of the classification proposal in the feasibility study report, the scheme of the information technology application feasibility project or the investment report of the project. Such report shall be sent to functional agencies for verification and to the authorities competent to validate the feasibility study report, the scheme of the information technology application feasibility project or the investment report in accordance with the laws on investment and this Decree.

2. If outsourcing information technology services, the leading outsourcer shall formulate and include explanations of the classification in the plan and/or the scheme of the outsourcing

project, which shall be delivered to functional agencies for verification and to competent authorities for validation as per the laws on outsourcing of information technology services and in accordance with this Decree.

3. Documents that explain the classification are defined in Article 15 of this Decree.

Article 14. Procedure and formalities for classification of information systems in operation

1. Proposal of classification:

a) The operator of the information system shall prepare the classification proposal as defined in Article 15 of this Decree;

b) For an information system to be given class 1 or class 2:

The operator of the information system shall submit the classification proposal to the verification body according to Section 1, Article 12 of this Decree;

c) For an information system to be given class 3:

The operator of the information system shall submit the classification proposal to the verification body according to Point a, Section 2, Article 12 of this Decree;

d) For an information system to be given class 4 or class 5:

- The operator of the information system shall submit the classification proposal to the specialized information security unit of the administrator of such system for professional advice on the pertinence of the proposal and on the solutions for securing the information system as classified;

- The operator of the information system shall provide the administrator of the information system with the classification proposal that is sent to the verification body as stated in Point a, Point b or Point c, Section 3, Article 12 of this Decree.

2. Verification of classification proposals:

The authorities competent to verify classification proposals are defined in Article 16 of this Decree.

3. Validation of classification proposals:

a) For an information system to be given class 1 or class 2:

The specialized information security unit of the administrator of the information system shall validate the classification proposal and report to the administrator;

b) For an information system to be given class 3 or class 4:

The operator of the information system shall present the classification proposal to the administrator of such system for validation;

c) For an information system to be given class 5:

- Ministry of Information and Communications shall base on the result of verification of the classification proposal to lead and cooperate with the Ministry of National Defense, Ministry of Public Security, relevant ministries and bodies in presenting the list of information systems classified at class 5 to the Prime Minister for validation;

- The operator of the information system shall present the information security scheme to the administrator of such system for validation;

Article 15. Documents in the classification proposal

A classification proposal includes:

1. Documents that describe and explain the information system in general.

2. Design documents comprised of:

a) For new investment projects or expansion and upgrade of information systems: The preliminary design or equivalent documents;

b) For information systems in operation: The construction design validated by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

5. Professional opinion(s) of the specialized information security unit of the administrator of the information system to be classified at class 4 or class 5.

Article 16. Verification of classification proposals

1. The following details in the classification proposal shall be verified:

a) The compatibility of the classification;

b) The compatibility of the scheme for securing the information system by classification as indicated in the preliminary design, construction design or equivalent documents;

c) The pertinence of the scheme for securing the information system to the operation of the system by classification.

2. Time limit for verification of classification proposals:

a) A valid proposal for classification of an information system at class 3, when received in full, shall be verified in at most 15 days.

b) A valid proposal for classification of an information system at class 4 or class 5, when received in full, shall be verified in at most 30 days.

Article 17. Validation of classification proposals

1. The validation of a classification proposal shall include:

a) The classification proposal;

b) Opinion(s) of verification of the verification body for information systems classified at class 3 or higher.

2. Time limit for validation of classification proposals:

Valid documents, when received in full, shall be processed in at most 07 working days.

Article 18. Procedure and formalities for re-classification of information systems with a validated class

The re-classification of information systems with a validated class, if required according to actual circumstances, shall adhere to the procedure and formalities for initial classification.

Chapter IV

RESPONSIBILITIES FOR SECURING INFORMATION SYSTEMS

Article 19. Scheme for security of information systems by classification

1. Schemes for security of information systems must meet basic requirements as defined in technical standards and regulations on security of information systems by classification.

2. A scheme for security of an information system shall consist of:

a) Security of the information system during the phase of design and construction;

b) Securing of the information system during the process of operation;

c) Inspection and assessment of the information safety;

d) Management of information safety risks;

dd) Supervision of information safety;

e) Provisions, emergency response and disaster recovery;

g) Termination of operation, liquidation, disposal.

Article 20. Responsibilities of administrators of information systems

1. The head of an agency or organization administering an information system shall be responsible for:

a) Directing and undertaking the security of information in the activities of his agency or organization;

b) If there is no independent unit specialized in securing information:

- Designate the specialized information technology unit to specialize in information security;

- Establish or designate a specialized information security unit directly under the specialized information technology unit.

2. The administrator of an information system is responsible for:

a) Directing the operator of the information system to make classification proposal(s); verifying and validating classification proposal(s) as per this Decree;

b) Directing and organizing the implementation of scheme(s) for securing the information system under its management by classification as per Article 25, 26 and 27 of the Law on security of information over network, this Decree and relevant legal regulations;

c) Directing and organizing the inspection and assessment of information safety and the management of risks in information safety intra vires, as follows:

- Carry out the inspection and assessment of information safety and general information safety risk management in relation to the activities of the agency or organization on 2-year basis;

- Carry out the inspection and assessment of information safety and information safety risk management over information systems of class 3 and class 4 on annual basis;

- Carry out the inspection and assessment of information safety and information safety risk management over information systems of class 5 on 6-month basis (or when deemed necessary, requested or warned by a functional authority);

- The inspection and assessment of information safety and information safety risks over information systems of class 3 or higher shall be conducted by a professional organization licensed by competent authorities, a government agency given suitable functions and assignments or a specialist organization designated by competent authorities.

d) Directing and organizing the provision of short-term training and propagandas to propagate and heighten awareness and information security drills, as follows:

- Provide short-term training courses that enhance knowledge and skills of public officials and employees in securing information in their agency or organization;

- Propagandize and raise the awareness of public officials and employees in securing information in their agency or organization;

- Carry out information security drills during the activities of the agency or organization; participate in national and international drills that the Ministry of Information and Communications holds.

dd) Direct the operator of the information system(s) to cooperate with relevant functional agencies of the Ministry of Information and Communications in deploying the equipment, connecting technical processor systems, reducing network attacks, supporting the supervision of the information safety of the information system(s) providing online public services, and developing the electronic government.

Article 21. Responsibilities of specialized information security units under administrators of information systems

1. Provide counsels, organize, expedite, inspect and supervise the security of information.

2. Verify, validate or professionally remark on classification proposals within authority as per Section 1 and Section 2, Article 12 and Section 5, Article 15 of this Decree.

Article 22. Responsibilities of operators of information systems

The operator of an information system shall be responsible for:

1. Classifying the security class of the information system as per Article 14 of this Decree.

2. Securing information as per the law, guidelines, standards and regulations on information safety;

3. Assessing the efficiency of information security measures periodically and reporting to the administrator of the information system when necessary;

4. Reporting the security of the information system on periodic or ad hoc basis upon request(s) of the administrator of the information system or competent state management authorities;

5. Cooperating with other entities and actualize requests of functional agencies related to the Ministry of Information and Communications for the security of information.

Article 23. Responsibilities of state management authorities

1. Ministry of Information and Communications shall be responsible for:

a) Verifying the classification proposals intra vires as per Point a, Section 3, Article 12 of this Decree;

b) Drafting national standards and promulgating national technical regulations on security of information by classification;

c) Providing detailed guidelines on the classification of information systems as per Section 2, Article 6 of this Decree;

d) Promulgating regulations and guiding documents on the security of information systems by classification, on the evaluation and certification of compliance and conformity in relation to the security of information systems by classification;

dd) Guiding agencies and organizations providing short-term training and propagandas to propagate and heighten awareness and information security drills;

e) Regulating the inspection and assessment of information safety and information safety risk management within the operations of state agencies and governmental organizations, unless otherwise governed by Point d, Section 2 and Point d, Section 3 of this Article;

g) Deploying nation-wide centralized technical facilities to handle and reduce network attacks, support the supervision of the security of information systems providing online public services and to develop the electronic government.

2. Ministry of National Defense shall be responsible for:

a) Verifying information security schemes in the classification proposals intra vires as per Point b, Section 3, Article 12 of this Decree;

b) Drafting standards and promulgating technical regulations and guidelines for the security of information systems under its management;

c) Providing guidelines for criteria defined in Section 1 of Article 9, Section 1 of Article 10 and Section 1 of Article 11 in this Decree according to its functions and assignments;

d) Regulating the inspection and assessment of information safety and information safety risk management within the operations of the Ministry of National Defense.

3. Ministry of Public Security shall be responsible for:

a) Verifying information security schemes in the classification proposals intra vires as per Point c, Section 3, Article 12 of this Decree;

b) Drafting standards and promulgating technical regulations and guidelines for the security of information systems under its management;

c) Providing guidelines for criteria defined in Section 1 of Article 9, Section 1 of Article 10 and Section 1 of Article 11 in this Decree according to its functions and assignments;

d) Regulating the inspection and assessment of information safety and information safety risk management within the operations of the Ministry of Public Security.

Article 24. Expenditure for information security

1. State funds shall be allocated for the security of information by classification during activities of state agencies and government organizations.

2. Public fund(s) shall be invested in the security of information as per the Law on public investment. Public investment projects for construction or expansion and upgrade of information systems shall employ their investment capital to finance investments in the security of information by classification.

3. The annual budget estimate of state agencies and government organizations shall allot fund(s) for their supervision, assessment and management of information safety risks; provision of short-term training, propagandas, information safety drills and emergency response as per the Law on state budget.

4. Ministry of Finance shall provide guidelines for spending on the security of information from the budget estimate, for management and use of administrative expenditure for the security of information during the operations of state agencies and government organizations.

5. State agencies and government organizations shall base on their assignments to estimate the budget, manage, use and finalize the expenditure for the security of information as per the law on state budget.

Chapter V

IMPLEMENTATION

Article 25. Effect

This Decree comes into force as of July 01, 2016.

Article 26. Implementation

1. Ministry of Information and Communications shall be responsible for guiding and inspecting the implementation of this Decree.

2. Ministers, Heads of ministerial-level agencies, Heads of governmental agencies, Chairpersons of provincial People's Committees and relevant entities are responsible for implementing this Decree./.

FOR THE GOVERNMENT
PRIME MINISTER

Nguyen Xuan Phuc

APPENDIX

THE FORMS FOR CLASIFICATION OF INFORMATION SYSTEMS
(Enclosed to the Government's Decree No. 85/2016/ND-CP dated July 01, 2016)

Form No. 01	Request for verification and validation of the classification proposal
Form No. 02	Request for verification of the classification proposal
Form No. 03	Request for professional remarks on the classification proposal
Form No. 04	Verification of the classification proposal
Form No. 05	Request for validation of the classification proposal
Form No. 06	Decision to validate the security class of the information system
Form No. 07	Decision to validate the scheme for information security

Form No. 01

(NAME OF THE AGENCY / ORGANIZATION)

No. ……..Request for verification / validation of the classification proposal

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom – Happiness

……. [place],… … … [date]

To: (The unit specialized in information security).

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

(Name of the agency / organization) requests the verification / validation of the classification proposal as follows:

Part 1. General information

1. Name of the information system:

2. The operator of the information system:

3. Address:

4. Security class of the information system recommended:

Part 2. Documents

1. Documents that describe and explain the information system in general.

2. The construction design approved by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

(Name of the agency / organization) requests (The specialized information security unit) to verify and validate the proposal for classification of (name of the information system)./.

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Recipient:
- As above:
- ……..

Form No. 02

(NAME OF THE AGENCY / **SOCIALIST REPUBLIC OF VIETNAM**

ORGANIZATION) **--------**	**Independent - Freedom – Happiness** **----------**
No. ……..Request for verification of the classification proposal	..... *[place],... ... ... [date]*

To: (The unit specialized in information security).

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

(Name of the agency / organization) requests (name of the verification body) to verify the classification proposal as follows:

Part 1. General information

1. Name of the information system:

2. The operator of the information system:

3. Address:

4. Security class of the information system recommended:

Part 2. Documents

1. Documents that describe and explain the information system in general.

2. The construction design approved by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

5. Professional opinion(s) of the specialized information security unit of the administrator of the information system (classified at class 4 or class 5).

(Name of the agency / organization) requests (the verification body) to verify the proposal for classification of the security class of (name of the information system)./.

Recipient:
- As above:
- ……...

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Form No. 03

(NAME OF THE AGENCY / ORGANIZATION)

No. ……..Request for professional remarks on the classification proposal

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom – Happiness

..... *[place],… … … [date]*

To: (The unit specialized in information security).

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

(Name of the agency / organization) requests (the specialized information security unit) to given professional remarks on the classification proposal as follows:

Part 1. General information

1. Name of the information system:

2. The operator of the information system:

3. Address:

4. Security class of the information system recommended:

Part 2. Documents

1. Documents that describe and explain the information system in general.

2. The construction design approved by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

(Name of the agency / organization) requests (the specialized information security unit) to remark on the suitability of the classification and the scheme for class-based security of (name of the information system)./.

Recipient:
- As above:
- ……...

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Form No. 04

(NAME OF THE AGENCY / ORGANIZATION)

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom - Happiness

No. ……..Verification of the classification proposal

……. *[place],… … … [date]*

To: (The administrator/ operator of the information system).

(Name of the verification body) has received the official dispatch n^{o} … dated … by (name of the requesting agency) on the verification of the proposal for classification of (name of the information system). After considering the proposal and soliciting remarks and findings of relevant agencies and organizations, (name of the verification body) provides the following opinions:

Part 1. Documents verified

1. Documents that describe and explain the information system in general.

2. The construction design approved by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

5. Professional opinion(s) of the specialized information security unit of the administrator of the information system to be classified at class 4 or class 5.

Part 2. Legal grounds of verification

1. Pursuant to the Law on security of information over network dated November 19, 2015;

2. (Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

2. Other relevant legal grounds.

Part 3. The verification body

1. The leading agency:

2. The supportive agency:

3. Form of verification: Through a meeting or written inquiries or via both methods (if necessary).

Part 4. Remarks

1. Remarks of the supportive agency as per Section 3, Article 12 of this Decree.

2. Remarks on the suitability of the classification as per Article 16 of this Decree.

3. Other remarks (if any).

Part 5. Conclusion

The proposal for classification of the information system suits / does not suit (specify unfit details) the classification.

Such remark of verification is given by (name of the verification body) over the proposal for classification of (name of the information system). (Name of the requesting agency) is advised to report to the competent persons for amendment (if required) or to the competent authorities for validation (if the proposal is passed)./.

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Recipient:
- As above:
- ……..

Form No. 05

(NAME OF THE AGENCY / ORGANIZATION)

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom – Happiness

No. …….. ..... *[place],… … … [date]*

OFFICIAL DISPATCH

On the validation of the classification proposal

To: (Relevant competent authorities)

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

Pursuant to remarks of the specialized information technology unit/ verification body;

(Name of the agency / organization) requests the validation of the classification proposal as follows:

Part 1. General information

1. Name of the information system:

2. The operator of the information system:

3. Address:

4. Security class of the information system recommended:

Part 2. Documents

1. Documents that describe and explain the information system in general.

2. The construction design approved by a competent authority or equivalent documents.

3. Documents that explain the criteria-based classification in conformity to the law.

4. Documents that explain the scheme of information security by classification.

5. Professional opinion(s) of the specialized information security unit of the administrator of the information system to be classified at class 4 or class 5.

6. Remark(s) of verification of the verification body for information systems classified at class 3 or higher.

(Name of the agency) requests (the administrator of the information system) to consider and validate the proposal for classification of (name of the information system)./.

Recipient:
- As above:
- ……..

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Form No. 06

(ADMINISTRATOR OF INFORMATION SYSTEM)

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom – Happiness

No. ……..

……. [place],… … … [date]

DECISION

On validation of the security class of the information system

(HEAD OF THE AGENCY / ORGANIZATION)

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

At the request of (the requesting unit),

HEREBY DECIDES:

Article 1: The security class of (name of the information system) is validated as follows:

1. General information

a) Name of the information system:

b) The operator of the information system:

c) Address:

2. Security class of the information system: (class)

3. Scheme for security of information:

a) The scheme for security of information, as included in the design of the information system classified at (class) adheres to (name of national standards) and (name of national technical regulations) on security of information systems by classification.

b) The scheme for security of information during the operation of the information system classified at (class) adheres to (name of national standards) and (name of national technical regulations) on security of information systems by classification.

Article 2. Implementation

1. (Name of the requesting agency) is responsible for:

a) Performing the duties of securing the information system under its management as per Article 22 of this Decree.

b) Others (if any).

2. Responsibilities of other relevant agencies (if any).

Article 3. Implementation

1. (Name of the proposing agency) and relevant agencies shall be responsible for implementing this Decision.

2. The specialized information security unit shall be responsible for inspecting and supervising the implementation of this Decision and reporting to (the administrator of the information system) as per the law./.

Recipient:
-……..;
- ……...

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Form No. 07

(ADMINISTRATOR OF INFORMATION SYSTEM)

No. ……..

SOCIALIST REPUBLIC OF VIETNAM
Independent - Freedom – Happiness

……. [place],… … … [date]

DECISION

On the validation of the scheme for security of information

(HEAD OF THE AGENCY / ORGANIZATION)

Pursuant to the Law on security of information over network dated November 19, 2015;

(Pursuant to documents guiding the implementation of the Law on security of information over network and relevant documents);

At the request of (the requesting unit),

HEREBY DECIDES:

Article 1: The scheme for security of information for (name of the information system) is validated as follows:

1. General information

a) Name of the information system:

b) The operator of the information system:

c) Address:

2. Scheme for security of information:

a) The scheme for security of information, as included in the design of the information system classified at (class) adheres to (name of national standards) and (name of national technical regulations) on security of information systems by classification.

b) The scheme for security of information during the operation of the information system classified at (class) adheres to (name of national standards) and (name of national technical regulations) on security of information systems by classification.

Article 2. Implementation

1. (Name of the requesting agency) is responsible for:

a) Performing the duties of securing the information system under its management as per Article 22 of this Decree.

b) Others (if any).

2. Responsibilities of other relevant agencies (if any).

Article 3. Implementation

1. (Name of the proposing agency) and relevant agencies shall be responsible for implementing this Decision.

2. The specialized information security unit shall be responsible for inspecting and supervising the implementation of this Decision and reporting to (the administrator of the information system) as per the law./.

REPRESENTATIVE OF THE AGENCY / ORGANIZATION
(sign, seal, write full name and title)

Recipient:
-……..;
- ……..