MINISTRY OF INFORMATION AND COMMUNICATIONS -------	SOCIALIST REPUBLIC OF VIETNAM Independent - Freedom – Happiness ---------------
No. 03/2017/TT-BTTTT	*Hanoi, April 24, 2017*

CIRCULAR

ON GUIDELINES FOR THE GOVERNMENT'S DECREE NO. 85/2016/ND-CP DATED JULY 01, 2016 ON THE SECURITY OF INFORMATION SYSTEM BY CLASSIFICATION

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

Pursuant to the Government's Decree No. 85/2016/ND-CP dated July 01, 2016 on the security of information system by classification;

Pursuant to the Government's Decree No. 17/2017/ND-CP dated February 17, 2017 on defining the functions, tasks, powers and organizational structure of Ministry of Information and Communications;

At the request of the Minister of Information and Communication,

The Minister of Information and Communications promulgates the Circular on guidelines for the Government's Decree No. 85/2016/ND-CP dated July 01, 2016 on the security of information system by classification.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

1. This Circular regulates the security of information system by classification, including: guide the classification of information system by class; request the security of information system by classification; inspect and evaluate the security of information; keep and verify the proposal for the classification; report and share information.

2. Information system serving defense and security activities that are managed by the Ministry of National Defense and the Ministry of Public Security shall not be regulated by this Circular.

Article 2. Regulated entities

The entities regulated by this Circular are specified in Article 2 of the Government’s Decree No. 85/2016/ND-CP dated July 01, 2016 on the security of information system by classification (hereinafter referred to as Decree No. 85/2016/ND-CP).

Article 3. Definitions

In this Circular, these terms are construed as follows:

1. *“Multi-factor authentication”* is a method of authentication using at least two components in connection with the user, including: something that the user knows (password, access code, etc.), something the user possesses (ID, smart card, etc.) or some physical characteristic of the user (fingerprint, eye iris, etc.).

2. *"Hot backup"* refers to the ability to replace the system when there is an error without interrupting the operation of the system.

3. *“Complexity requirements of the password”* means password must be at least 8 characters in length which must contain upper case letters, lower case letters, special characters and numeric characters.

4. *“Main or important network device”* refers to devices that once stopped a part or all of them without planning will cause disruption in the information system.

Chapter II

GUIDELINE FOR THE DETERMINATION AND CLASSIFICATION OF INFORMATION SYSTEM

Article 4. Determination of specific information system

1. The determination of information system for classification is subject to the principles specified in Clause 1 Article 5 of Decree No. 85/2016/ND-CP.

2. The information system is established through one or several of the following forms: New construction investment; upgrading, expansion and integration with existing systems; rental or transfer of systems.

3. An information system that services internal activities solely contributes to the internal management and operation of an agency or organization, including:

a) Email system;

b) Document management and administration system;

c) Live conference and meeting system;

d) Specific information management system (personnel, finance, asset or other specific professional areas) or general information management system (integrated management of many different functions and operations);

dd) Internal information processing system.

4. 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, including:

a) Email system;

b) Document management and administration system;

c) Electronic single window system;

d) Website system;

dd) Directly or indirectly providing online service system;

e) Customer service system.

5. A system of information infrastructure is comprised of equipment and transmission lines that serve the operations of organizations and agencies, including:

a) Intranet, Wide area network, special data transmission network;

b) Database, data center and cloud computing network;

c) Electronic verification, electronic authentication and digital signature system;

c) Interconnection system, enterprise service bus.

6. An industrial maneuver information system has the functional role in supervising and collecting data, managing and controlling vital sections for maneuvering and operating ordinary activities of buildings, including:

a) Programmable logic controller (PLCs);

b) Distributed control system (DCS);

c) Supervisory control and data acquisition (SCADA).

7. Other information systems that do not belong to the abovementioned forms are used to directly serve or support professional operations, production and business of specific agencies or organizations in specialized operations.

Article 5. Administrators of information systems

1. Regarding state authorities and organizations, the administrator of the information system is one of the following cases:

a) Ministries, ministerial agencies, Governmental agencies;

b) Provincial People’s Committees;

c) Competent authorities given discretion in investment projects for the construction, configuration, upgrade and expansion of information systems

2. Regarding other businesses and organizations, administrators of information systems are competent authorities given discretion in investment projects for the construction, configuration, upgrade and expansion of information systems.

3. The information system administrator may authorize an organization to exercise direct management over the information system and be responsible for ensuring the security of the information system on its behalf as specified in Clause 2 Article 20 of Decree No. 85/2016/ND-CP.

The authorization must be made in writing, clearly identifying the authorization scope and time limit. The authorized organization must directly exercise the rights and obligations of the information system administrator without re-authorizing a third party.

Article 6. Operators of information systems

1. Operators of an information system refer to agencies and organizations that the administrators of the information system designate to operate such system.

2. If the information system consists of multiple components or distributed systems, or there is more than one operator, the information system administrator shall assign a unit to be the focal point in order to exercise the rights and obligations of operators of the information system in accordance with the provisions of law.

3. If the administrators of an information system outsource information technology services, the operators of the information system shall be providers of such services.

Article 7. Guideline for the determination and explanation of information system

The determination and explanation of information system consist of:

1. Determine and classify the information system; determine the information system administrator and operators in accordance with Article 5, 6 of Decree No. 85/2016/ND-CP and Article 4, 5 and 6 hereof.

2. Determine the information processed by an information system in accordance with Clause 1 Article 6 of Decree No. 85/2016/ND-CP.

3. The classification of information system level is subject to the principles specified in Article 7 to 11 of Decree No. 85/2016/ND-CP. If the information system is given class 4 or 5, the explanation of classification proposal shall specify the following contents:

a) The classification of other information systems that are related or have a connection to or have significant impact on the normal operation of the proposed information system; clearly determine the extent to which the proposing information systems are affected when these systems lose information security.

d) The list of proposal of important network components, equipment and important information processed in the system (if any);

c) The explanation on the importance of network components, equipment and the information, data processed or saved in the system (if any);

d) Explanation on the risks of network attacks, the loss of information security in the system, system components and network devices; the impact of such risks of network attacks and loss of information security on the criteria of classification according to Article 10 and 11 of Decree No. 85/2016/ND-CP;

dd) The assessment of the scope and scale of influence to public interest, social order or national defense and security when a network attack causes loss of information security or interruption in the operation of each classified system.

For information systems to be given class 4, the explanation must require them to function on round-the-clock basis and does not halt without prior schedule;

e) Other explanations (if any) based on practical operation of the information system.

Chapter III

REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEMS BY CLASSIFICATION

Article 8. General requirements

1. The security of information system by classification must comply with basic requirements as specified hereof; technical regulations and standards on information security and other related professional technical regulations and standards.

2. Basic requirements by classification as specified hereof are minimum requirements for information security excluding physical security requirements.

3. Basic requirements shall consist of:

a) Technical requirements: network infrastructure security; server security; application security and data security;

b) Management requirements: General Policy; organization, personnel; design and construction management; operational management; inspection, assessment and risk management.

4. The preparation of information security proposal according to basic requirements for each class shall comply with Clause 2 Article 4 of Decree No. 85/2016/ND-CP, specifically as follows:

a) For information system class 1, 2, 3: The information security proposal shall consider the ability to share resources and secure information between information systems to optimize performance and preclude redundant and overlapping investments. In cases of newly invested system, there must be an explanation that the existing solution does not meet the basic requirements;

b) For information system class 4, 5: Information security proposal shall be designed to ensure availability, segregation, and impact mitigation of the entire system when a component of the system or system-related information is insecure.

Article 9. Basic requirements for each class

1. Information system class 1 security proposal shall comply with the specific requirements specified in Annex 1 enclosed herewith.

2. Information system class 2 security proposals shall comply with the specific requirements for class 1 and supplemented requirements specified in Annex 2 enclosed herewith.

3. Information system class 3 security proposals shall comply with the specific requirements for class 2 and supplemented requirements specified in Annex 3 enclosed herewith.

4. Information system class 4 security proposals shall comply with the specific requirements for class 3 and supplemented requirements specified in Annex 4 enclosed herewith.

5. Information system class 5 security proposals shall comply with the specific requirements for class 4 and supplemented requirements specified in Annex 5 enclosed herewith.

Chapter IV

INSPECTION AND ASSESSMENT OF INFORMATION SECURITY

Article 10. Contents and forms of inspection and assessment

1. Contents of inspection and assessment:

a) Inspect the compliance with the laws on security of information systems by classification;

b) Assess the efficiency of information system security measures;

c) Assess the detection of malicious code, security holes and vulnerabilities, test the intrusion detection system;

d) Other inspection and assessment as regulated by the information system administrator.

2. Forms of inspection and assessment:

a) Inspect and assess periodically according to the plan of the information system administrator;

b) Inspect and assess irregularly at the request of competent authorities.

3. Competent authorities requesting the assessment and inspection:

a) Minister of Information and Communications;

b) Administrator of information system under the management;

c) Specialized information security units under administrators of information systems which classification proposals approved by such units.

4. Units in charge of inspection and assessment shall be assigned or selected by competent authorities.

5. The subject of inspection and assessment is the administrator of the information system or the operators of the information system and related information systems.

Article 11. Inspection of the compliance with the laws on security of information systems by classification

1. Inspection of the compliance with the laws on security of information systems by classification shall include:

a) Inspect the compliance with the laws on classification of security of information systems;

b) Inspect the compliance with the laws on the implementation of the proposal on security of information systems by classification;

2. The unit in charge of inspection is one of the following units:

a) The Authority of Information Security;

b) Specialized information security units.

3. Periodic inspection plans include the following contents:

a) A list of units, information systems (if any) being inspected;

b) Scope and contents of inspection;

c) Inspection duration;

d) Cooperating units (if any).

4. Decision on inspection shall be made after the plan on periodic inspection is approved by the competent authority or upon irregular inspection of the competent authority.

5. Regarding periodic inspection:

a) The unit in charge of inspection shall prepare the periodical inspection plan for the subsequent year and submit it to the competent authority for approval to serve as a basis for implementation;

b) In case of change compared to the approved periodic inspection plan, the unit in charge of inspection shall prepare the periodical inspection plan amendments and submit it to the competent authority for approval;

c) The periodic inspection plan shall be sent to the inspected subjects and superior agencies of the inspected subjects within 10 days from the approved date but at least 10 days before the inspection day.

6. Regarding irregular inspection:

Depend on the request for irregular inspection and decision on inspection, the head of the inspection unit shall prescribe the contents of the inspection where appropriate.

7. After the direct inspection at the establishment, the inspection unit shall notify the inspected subjects and hand over documents and equipment (if any) used in the inspection process.

The inspection team shall draft an inspection report and send it to the inspected subjects for comments. Within 5 working days after receiving the draft inspection report, the inspected subjects shall comment on the draft contents.

8. Based on the draft inspection report, opinions and explanations of inspected subjects, within 30 days from the inspection date at the establishment, the inspection unit shall complete the inspection report, draft inspection conclusion and send them to the competent authority for considering approval.

Inspection conclusion must be sent to the inspected subjects and superior agencies of such subjects (if any) and relevant units (if necessary).

Article 12. Assessment of the efficiency of information security measures

1. The assessment of the efficiency of information security measures refers to the overall review and verification of the efficiency of information security measures in accordance with each criterion and basic requirement.

The assessment of the efficiency of applied information security measures is the basis for adjusting the plan to ensure information security in accordance with practical requirements.

2. The unit in charge of assessment is one of the following units:

a) The Authority of Information Security;

b) Specialized information security units;

c) Government agencies given suitable functions and assignments;

d) Enterprises possessing licenses for provision of inspection and assessment of network information security;

3. The operators of the information system shall prepare the periodical assessment plan for the subsequent year and submit it to the competent authority for approval to serve as a basis for implementation. The assessment plan includes:

a) A list of units, information systems (if any) being assessed;

b) Assessment duration;

c) Operating unit: Self-operate or operated by a specialized information security unit or outsourced in accordance with the law.

4. b) In case of change compared to the approved assessment plan, the operators of the information system shall prepare the amendment of the assessment plan and submit it to the competent authority for approval;

5. After the direct inspection at the establishment, the assessment unit shall notify the operators of the information system and hand over documents and equipment (if any) used in the inspection process.

The assessment team shall draft an assessment report and send it to the operators of the information system for comments. Within 5 working days after receiving the draft assessment report, the operators of the information system shall comment on the draft contents.

6. Based on the draft assessment report, opinions and explanations of operators of the information system, the assessment unit shall complete the assessment report and send it to the operators and administrator of the information system.

Article 13. Assessment of the detection of malicious code, security holes and vulnerabilities, testing of the intrusion detection system

1. Assessment of the detection of malicious code, security holes and vulnerabilities, testing of the intrusion detection system refers to the detection of vulnerabilities and holes in the system and testing of intrusion detection systems, and assessment of risks and damages of information systems which may exists when the system is attacked by intruders.

2. The unit in charge of assessment is one of the following units:

a) The Authority of Information Security;

b) Specialized information security units;

c) Government agencies given suitable functions and assignments;

d) Enterprises possessing licenses for provision of inspection and assessment of network information security or other organizations allowed by the information system administrator to assess the detection of malicious code, security holes and vulnerabilities, testing of the intrusion detection system .

3. The unit in charge of assessing the detection of malicious code, security holes and vulnerabilities, test the intrusion detection system shall:

a) Inform the system administrator of discovered information security vulnerabilities to overcome and prevent information security incidents.

b) Ensure the data security related to the assessed system, do not release relevant data without the consent of the information system administrator;

c) Ensure that the assessment of the detection of malicious code, security holes and vulnerabilities, testing of the intrusion detection system do not affect normal operation of the system.

Chapter V

RECEIPT AND VERIFICATION OF THE CLASSIFICATION PROPOSAL

Article 14. Submission and receipt of the classification proposal

1. For an information system to be given class 1, 2 or 3:

Operators of the information system shall send 01 original copy and 02 authenticated copies of the classification proposal to the specialized information security units for verification.

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

a) The administrator of the information system shall send 01 original copy and 04 authenticated copies of the classification proposal to the Ministry of Information and Communications (the Authority of Information Security) for verification;

b) For an information system to be given class 4 or 5, the recipient and receiving address shall be:

Ministry of Information and Communications (the Authority of Information Security), Floor 8, 115 Tran Duy Hung Building, Cau Giay District, Hanoi.

In case of changing the receiving address, the Authority of Information Security shall announce the change of address in accordance with laws.

3. Within 05 working days from the day on which the proposal is received, the recipient shall verify whether it is satisfactory. If the proposal is unsatisfactory, the recipient shall send a written notification to the applicant for supplements.

Article 15. Verification of the classification proposal

1. For an information system to be given class 1, 2 or 3:

The specialized information security unit shall verify the classification proposal as prescribed in Article 16 of Decree No. 85/2016/ND-CP.

During the verification process, the specialized information security unit shall collect written opinions of related units if necessary.

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

The Ministry of Information and Communications shall verify the classification proposal as prescribed in Article 16 of Decree No. 85/2016/ND-CP. The verification of the classification proposal shall follow the process below:

a) The Authority of Information Security shall request for written comments of the Department of Legal Affairs and other related unit affiliated with the Ministry of Information and Communications if necessary within their assigned functions and duties;

b) The Ministry of Information and Communications shall request for written comments of the Ministry of National Defense and the Ministry of Public Security in accordance with the laws.

c) Based on written comments of the Ministry of National Defense, the Ministry of Public Security and other related units, the Ministry of Information and Communications shall establish a verification council to discuss and give specific opinions. The chairperson of the verification council is assigned by the Minister of Information and Communications, the members are representatives of the leaders of the Authority of Information Security, Department of Legal Affairs, VNCERT - Ministry of Information and Communications, representatives of leaders of functional units of the Ministry of Public Security, Ministry of Defense and some independent experts (if necessary).

Article 16. Mechanism for verification cooperation

1. Operators of the information system shall cooperate with the unit verifying the classification proposal in determining the suitability of the classification proposal and operational requirements of corresponding information system.

2. In case of necessity, the unit verifying the classification proposal shall inspect and assess the information system security proposal according to the proposed class. The security inspection and assessment shall not affect the normal operation of the information system and the information system administrator or operators shall be notified if there are weaknesses in the information security.

…………………………..

Protect confidentiality of origin and content of information as agreed between parties sharing information.

4. The Information sharing is done at least every quarter and in accordance with the actual operation of the respective information system.

5. Shared information includes:

a) Information has yet been analyzed or analyzed on the risk of information insecurity; Information about occurred network attacks

- Types of network attacks recorded at the system;

- Quantity of network attacks recorded at the system;

- Samples of the recorded information of network attacks;

- Other data as agreed between parties sharing information.

b) Information security activities such as propagation, training, experiment and other data.

Chapter VII

ORGANIZATION OF IMPLEMENTATION

Article 19. Effect

1. This Circular shall come into force as of July 01, 2017.

2. Any issue arising during the implementation of this Circular should be promptly reported to the Ministry of Information and Communications (the Authority of Information Security) for consideration and settlement./.

MINISTER

Truong Minh Tuan

ANNEX 1

BASIC REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEM CLASS 1
(*issued together with Circular No. 03/2017/TT-BTTTT dated April 24, 2017 of the Minister of Information and Communications)*

1. Technical requirements:

a) Server security:

- Authenticate by password and system log for server access and administration;

- Do not use unencrypted connections in remote server administration;

b) Application security;

Authenticate by password and system log for application access and administration login;

c) Data security:

Periodic backup data of the system depending on the requirements and purposes

2. Managerial requirements:

a) General policy: Have an information security policy for administrators and operators of the system;

b) Organization and personnel: Have a principle contact agent for notifying, exchanging and handling arising issues or information insecurity of the information system.

ANNEX 2

BASIC REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEM CLASS 2
(issued together with Circular No. 03/2017/TT-BTTTT dated April 24, 2017 of the Minister of Information and Communications)

1. Technical requirements:

a) Network infrastructure security:

- Split the network infrastructure into different network areas according to the requirements and purposes;

- Have the option to use the device that has a firewall function to prevent unauthorized access between the network area and the Internet;

- Have the authentication and encryption mechanisms when using wireless networks (if any);

- Have the option to authenticate administrator account on important network equipment;

- Have the option to use remote administration (if any) through encryption protocols;

b) Server security:

- Use anti-malware software that has a mechanism to automatically update the new version or new malicious code detection for this software.

- Have a password authentication mechanism to ensure necessary complexity, require a periodic password change according to the regulations of the organization and mechanisms to prevent password scans; Store credentials on the system in encrypted form;

- Have the option to disable the default or inactive accounts on the system; disable services, unused software on the server;

- Have system log for server access and administration;

- Establish a mechanism for updating patches of information security vulnerabilities for operating systems and system services on the server;

c) Application security:

- Establish a password requirement mechanism on applications that are sufficiently complex to prevent password scans; store credentials on the system in encrypted form;

- Establish access log and error log requirements;

- Do not use unencrypted internet connections in remote application administration.

d) Data security: Use a system or portable storage device to back up important data on the server. The backups are done periodically according to regulations of the organization.

2. Managerial requirements:

a) General policy:

- Have an information security policy for users including: policy of access and use of network and resources on the Internet; policy of access and use of application;

- Have an information security policy for administrators and operators of the system that not being restricted by the management policy of network security, server security, application security and data security;

b) Organization and personnel:

Have procedures for the allocation, removal of accounts and access of new staff, changed staff or ex-staff of the system.

c) Design and construction management:

- Have design documents and description of the options of the information system security;

- Check and verify whether the system is implemented in accordance with the design documents and information security requirements before acceptance and handover;

- Have a classification proposal verified and by specialized information security units under administrators of the information system.

d) Operational management:

- Have the management and operation process of the system in conformity with the basic technical requirements; manage the system change and migration; end of operation, exploitation, liquidation, cancellation of the system;

- Have the procedure for response to an information security incident;

dd) Inspection, assessment and management of risks:

- Carry out the inspection and assessment of information security and management of information security risks every 02 years or when necessary according to the provisions of law.

- The inspection and assessment of information security and risk assessment must be conducted by the specialized information security unit of the information system administrator or outsourced according to the provisions of law.

ANNEX 3

BASIC REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEM CLASS 3
(issued together with Circular No. 03/2017/TT-BTTTT dated April 24, 2017 of the Minister of Information and Communications)

1. Technical requirements:

a) Network infrastructure security:

- Design specific networks includes local area networks for local servers, specific area networks for servers that provide essential system services (such as DNS, DHCP, NTP and other services), specific networks for database servers and other specifics networks as required by the organization;

- Design local area networks into functional networks according to operational requirements; separate wireless networks from functional area networks; separate specific area networks for servers that provide services from the Internet;

- Have the option of load balancing and mitigation of denial of service attacks;

- Design centralized storage management system and information security administration

- Use the device that has a firewall function between important network areas;

- Detect, prevent intrusion and block malicious software between the Internet and internal networks;

- Store logs of network equipment and perform centralized network management within function area of network equipment that have this feature or important network equipment.

- Store logs of network equipment at least 03 months and ensure synchronization of logs with real time of the server in Vietnam time zone;

- Have redundant design of main network devices in the system to ensure the normal operation of the system when a network device fails.

- Update software; handle information insecurity and weaknesses in optimal configuration of network devices before using in the network;

- Authenticate admin account on all network devices in which ensure necessary complexity of the password and prevent password scans;

- Restrict access and administration to network devices;

- Only allow administrators to manage network devices through the Internet using virtual private networks or other equivalent methods;

- Store logs for activities on intranet devices and ensure synchronization of log time with real time servers;

- Encrypt the credentials stored on the network devices;

b) Server security:

- Manage centralized authentication; prevent automatic login and automatic cancelation of login sessions after a timeout in accordance with the organization policy;

- Set up access, administration and use of resources of each account on the system in accordance with different tasks and operational requirements;

- Manage patches and upgrade centralized system software;

- Perform storage and centralized management of server logs. The logs are stored for at least 03 months;

- Synchronize the server logs with the information security monitoring system;

- Restrict sources of access and administration of server; the server administration through the Internet must use virtual private networks or other equivalent methods;

- Use a firewall on each server to only allow legitimate connections according to services provided by the server;

- Backup server operating system, server configuration in accordance with the requirements of the organization;

- Record logs for access, administration and incidents;

c) Application security:

- Set up a periodic password change request for the application administration account; limit the execution timeout when the application does not receive a request from the user;

- Separate the administrative application with the application that provides service to the user and ensure that the application operates with minimum permissions on the system.

- Restrict sources of access and administration of application; the application administration through the Internet must use virtual private networks or other equivalent methods;

- Inspect and sanitize input data from the user, ensure that those data do not affect the application information security.

d) Data security:

- Encrypt saved data (not public information or data) on storage system/storage media;

- Automatically backup information/data in accordance with the frequency of change of data;

2. Managerial requirements:

a) General policy: Biannually or when necessary, review and update the general policy on information security;

b) Organization and personnel:

- Prepare plans and periodically organize training, re-training, propagation and dissemination to raise knowledge and skills on information security for related managerial staffs and technicians.

- Establish policies that require related employees to commit to not reveal confidential information relating to system data, private information or the organization or other sensitive information in case of resignation.

c) System design and construction:

Have a classification proposal verified and by specialized information security units under administrators of the information system;

d) Operational management:

- Monitor the system information security during operation in accordance with the law;

- Prepare plans and periodically organize experiment to ensure system information security; send staffs to participate in national or international experiment convened by competent authorities;

- Prepare plans to restore the normal operation of the system in case of an incident or disaster;

dd) Inspection, assessment and management of risks:

- Carry out the inspection and assessment of information security and management of information security risks annually according to the provisions of law;

- The inspection and assessment of information security and risk assessment must be conducted by a professional organization licensed by competent authorities or a government agency given suitable functions and assignments designated by the administrator of the system.

ANNEX 4

BASIC REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEM CLASS 4
(issued together with Circular No. 03/2017/TT-BTTTT dated April 24, 2017 of the Minister of Information and Communications)

1. Technical requirements:

a) Network infrastructure security:

- Detect, prevent intrusion between important networks;

- Centrally manage wireless networks (if any);

- Establish a centralized malware management system in which, the system has basic functions including: update data, send alerts and receive control information from centralized management system to the software installed on the server/workstation of the network;

- Establish a hot backup for main network devices to ensure continuous availability of the system; the capacity of the backup device must meet the operational scale of the system;

- Use additional multi-factor authentication methods for important network devices;

- Store logs independently and match the operation of network devices. Log data must be stored for at least 06 months;

- Send real-time alerts directly to system administrators via a monitoring system when problems are detected on network devices;

- Maintain at least two Internet connections from ISPs using different domestic infrastructure networks (if the system requires an Internet connection);

- Establish a data loss prevention system;

b) Server security:

- Use multi-factor authentication mechanism when accessing servers in the system;

- Store logs independently and match the operation of servers. Log data must be stored for at least 06 months;

- Check the integrity of the system files and the integrity of the permissions granted on the system accounts;

c) Application security:

- Use multi-factor authentication mechanism when accessing the application's administrator accounts; mechanism that requires the users to periodically change their credentials;

- Store logs independently and match the operation of applications. Log data must be stored for at least 06 months;

- Encrypt credentials of users before sending them to the application through a network;

- Authenticate information and sources of information when exchanging information in the process of application management (not public information or data) through a network;

d) Data security:

- Check the integrity of the data, detect and warn when there are changes;

- Sort and manage stored data by type/group using different labels;

- Use a fault-tolerant backup system to ensure data recovery when a problem occurs;

2. Managerial requirements:

a) General policy: Annually or when necessary, review and update the general policy on information security;

b) Organization and personnel:

- Inspect and verify the identity of managers and technicians, be responsible for the system information security, ensure the conformity of professional knowledge, professional ethics and meet the requirements and specific nature of the work;

- Prepare plans and periodically or annually organize training, re-training, propagation and dissemination to raise knowledge and skills on information security for related managerial staffs and technicians.

- Establish a specialized information security unit and assign the leader of the unit directly in charge of information security;

c) System design and construction:

- Have a classification proposal verified by Ministry of Information and Communications;

- Check the compatibility and impact of patches, update information security of system operation;

- Have the optimal configuration; ensure information security for network devices and servers before using in the system;

- Conduct overall inspection and evaluation of the system information security before putting it into operation and exploitation;

d) Operational management:

- Have private plan on monitoring information security system in accordance with the law; supervise on-site 24/7;

- Prepare plans and annually organize experiment to ensure the system information security;

- Establish emergency response to ensure network information security in accordance with the law

dd) Inspection, assessment and management of risks:

- Carry out the inspection and assessment of information security and management of information security risks;

- The inspection and assessment of information security and risk management must be conducted by a professional organization licensed by competent authorities or a government agency given suitable functions and assignments designated by the administrator of the system.

ANNEX 5

BASIC REQUIREMENTS FOR SECURITY OF INFORMATION SYSTEM CLASS 5

(issued together with Circular No. 03/2017/TT-BTTTT dated April 24, 2017 of the Minister of Information and Communications)

1. Technical requirements:

a) Network infrastructure security:

- Use firewall, intrusion detection and prevention system between the network areas of the system;

- Store logs of network devices for at least 12 months;

- Prepare backup plans for all network devices to ensure the system operation is uninterrupted;

b) Server security:

- Use workstation-level intrusion prevention system for servers;

- Store logs independently and match the operation of servers. Logs of the servers must be stored for at least 12 months;

c) Application security:

- Apply two-way authentication when exchanging important data through a network;

- Use a specific storage device to store credentials;

- Store logs of applications for at least 12 months;

d) Data security:

- Use private channel when transmitting and exchanging data through a network;

- Backup system data in different geographic locations;

- Maintain at least 02 network connections from the primary backup system with the secondary backup system;

2. Managerial requirements:

a) General policy:

General policy: Biannually or when necessary, review and update the general policy on information security;

b) Organization and personnel:

- Assign different full-time staffs for different positions, do not use part-time staff;

- Assign at least 02 staffs for important operational positions;

c) System design and construction:

Products and equipment invested in the system must be inspected for information security before being put into operation and exploitation;

d) Operational management:

Prepare plans and biannually organize experiment to ensure the system information security;

dd) Inspection, assessment and management of risks:

- Carry out the inspection and assessment of information security and information security risk management on a biannual basis or when deemed necessary, requested or warned by a functional authority;

- The inspection and assessment of information security and risk assessment must be conducted by a professional organization licensed by competent authorities or a government agency given suitable functions and assignments designated by the administrator of the system.
