|  |  |
| --- | --- |
| **THE STATE BANK OF VIETNAM-------** | **SOCIALIST** **REPUBLIC OF VIETNAM Independence - Freedom - Happiness ---------------** |
| No: 01/2011/TT-NHNN | *Hanoi, February 21, 2011*  |

**CIRCULAR**

PROVIDING FOR ENSURING SAFETY, KEEPING SECRETS THE INFORMATION TECHNOLOGY SYSTEM IN BANKING OPERATION

*Pursuant to the Law on State Bank of Vietnam No.46/2010/QH12 dated 16/6/2010;
Pursuant to the Law on credit institutions No.47/2010/QH12 dated 16/6/2010;
Pursuant to the Law on Information Technology No.67/2006/QH11 dated 29/6/2006;
Pursuant to the Decree No.96/2008/ND-CP dated 26/8/2008 of the Government regulating functions, tasks, powers and organizational structure of the State Bank of Vietnam;
the State Bank of Vietnam provides for ensuring safety, keeping secrets the information technology system in banking operation as follows:*

**Chapter 1.**

**GENERAL PROVISIONS**

**Article 1. Scope of governing and subjects of application**

1. This Circular provides for requirements of ensuring safety, keeping secrets the information technology system (IT) in banking operation.

2. This Circular applies to the State Bank of Vietnam; credit institutions; branches of foreign banks (hereinafter collectively called as units).

**Article 2. Interpretation of terms**

In this Circular, the below terms are construed as follows:

1.  *Information technology system*: means a structured set of hardware equipment, software, databases and network systems for one or more technical operations, operations of the banks.

*2.*  *IT assets:* means equipments, information under IT system of the units, including:

a) *Physical assets:* mean IT equipment, mass media and equipment for the operation of IT systems.

b) *Information* *assets:* mean data and documents relating to IT systems. Information assets are represented by paper documents or electronic data.

c) *Software assets:* include the applicable programs, system software, databases and development tools.

3. *IT risk:* means ability of happening loss when making activities related to IT systems. IT risk related to management, use of hardware, software, communications, interface systems, operating and people.

4. *Risk management:* means the coordinating activities aiming at determining and controlling IT risk which may happen.

5. *Third parties*: mean organizations and individuals having professional skill hired by or coordinate with units to provide goods, technical services for the IT system.

6. *Network security systems:* a set of firewall devices and equipment to control and detect illegal access, management software, monitoring and logging of network security status and other equipment with function to ensure the safe operation of the network, all work together in a synchronized network security policies in order to strictly control all activities on the internet.

7. *Firewall*: means a collection of components or a system of equipment and software placed between two networks to control all connections from inside to outside of the network or vice versa.

8. *Virus*: means a computer program enabling to spread, causing abnormal operation to the digital device or copy, modify and delete the stored information in digital equipment.

9. *Malicious-logic software (mal-ware):* means software that its features cause harmful such as viruses, spy-ware (spy-ware), advertising software (ad-ware) or other similar forms.

10. *Technology weak points:* mean its position in the IT system vulnerable when being attacked or illegally invaded.

**Article 3. General principles**

1. Each unit must ensure safety; keep secrets IT system of its unit according to provisions in this Circular.

2. Promptly identify, classify, evaluate and effectively handle IT risk which may occur in the unit.

3. To build, deploy safety regulations, keep secrets IT system on the basis of harmony between benefits, costs and risk acceptable level of the unit.

4. To allocate adequate qualified resources appropriate to the scale aiming at ensuring safety, keeping secrets IT systems.

5. Clearly define powers and responsibilities of heads of units, levels, departments and each individual in the unit for the acts to ensure safety and keep secrets IT system.

**Article 4. Regulations on safety, keeping secrets information technology system**

1. The units must build safety regulations; keep secrets IT system suitable to the units’ IT system, organizational structure, managerial requirement and operation. The regulations of safety, keeping secrets IT system must be approved and organized to implement by heads of units and be deployed to all managers, staffs and relative parties.

2. The regulations on safety, keeping secrets IT system must include the basic provisions on:

a) Management of IT assets;

b) Management of human resource;

c) Physique and environment;

d) Communications and operation;

đ) Accessing management;

e) Receipt, development, maintaining information system;

g) Trouble-shooting;

h) Storage and disaster prevention.

3. Periodically, the units must review, edit, improve safety regulations and keep secrets IT system at least once a year, ensuring the suitableness, adequacy and efficiency of the regulations. In case of detecting the inadequacies and irrationalities causing unsafe to the IT systems or at the request of the competent agencies, units must conduct to amend, supplement immediately its regulations.

**Chapter 2.**

**PROVISIONS ON ENSURING SAFETY, KEEPING SECRETS THE INFORMATION TECHNOLOGY SYSTEM**

**ITEM 1. ORGANIZATION ENSURING SAFETY, KEEPING SECRETS THE INFORMATION TECHNOLOGY**

**Article 5. Safety management, keeping secrets information technology inside of units**

1. Heads of units must directly guide the acts of ensuring safety, keeping secrets IT and stipulate clearly responsibilities in the acts of ensuring safety, keeping secrets IT to individuals, divisions.

2. Individuals in the units relating to keeping secrets information must sign commitments to keep secrets information.

**Article 6. Safety management, keeping secrets information technology of the unit to third party**

1. Evaluating technical capability, personnel, financial ability of third parties before signing the contract to provide goods and services.

2. Clearly define responsibilities, powers and obligations of the parties on security, IT security when signing the contract. Contracts with third parties must include the clauses of the sanctions against third parties due to violate safety regulations, information security and the responsibility to pay damages of third parties in case of having damages caused by the violation of third parties.

3. Specially pay attention to issues of confidentiality, integrity, availability, reliability, maximum performance, ability to recover disaster, storage mean of information systems.

4. Fully determine the risks of units related to third parties which may arise and apply risk management measures.

5. To apply measures to closely monitor and restrict right to access of third parties when allowing them access to IT systems of units.

**ITEM 2. MANAGEMENT OF INFORMATION TECHNOLOGY ASSETS**

**Article 7. Responsibility for information technology assets**

1. To make statistics, inventory of IT assets in the unit at least once each year. Contents of the property statistics must include the following information: type of property, values, important levels, the installation location, backup information, copyright information.

2. To classify, arrange priority order at value, the importance of IT assets to take measures to protect the assets accordingly and build and implement regulations on management, use of assets.

3. To add the right to use property to individual or specific department. IT property user must comply with the regulations on management and use of the property, ensuring the property which is used for proper purposes.

**Article 8. Classification of information technology assets**

1. To classify IT property according to criteria of value, sensitivity and importance, frequency of use, storage time.

2. To implement the management measures suitable to each type of information asset classified.

**ITEM 3. MANAGEMENT OF HUMAN RESOURCE**

**Article 9. Management of internal human resource of unit**

**1. Before the recruitment or duty assignment**

a) To define responsibility for safety, IT security of the position need to be recruited or assigned.

b) To check background, review, valuate strictly ethics, professional qualifications when recruiting, assigning managers, staffs members to work in the key position of IT systems such as system administration, management of security systems, system operation, database management.

c) Decision or an employment contract (if any) must include the Articles, clauses of responsibility to ensure safety, IT security of persons who are employed during and after working in the unit.

**2. Within working time**

a) The units are responsible for dissemination and updating of regulations on safety, IT security to managers, staffs.

b) Requiring and examining the execution of regulations on safety and IT security of individuals, organizations to be of units at least once a year.

c) Applying discipline measures to managers, staffs of the unit who committed violations of safety and IT security.

d) The important works such as network security system configuration, operating system parameters change and firewall device installation, the device of detection and intrusion prevention (IPS) must be performed by at least two people or must have a supervisor.

đ) Not to grant administrative right (who can edit the configuration, data, logs) on the main IT system and backup system for the same individual.

**3. When terminating or changing jobs**

When managers, staffs terminate or change jobs, the unit must:

a) Clearly defining responsibility of managers, staffs and relative parties on IT system.

b) Making asset transfer minute to staffs, managers.

c) Withdrawing or changing right of accessing IT system of staffs, managers to suit the job changed.

**Article 10. Management of third parties’ human resource**

**1. Before deploying works**

a) Requiring third parties to supply list of personnel who join in.

b) Examining legal status, professional capability of personnel of third-parties suitable to job requirements.

c) Requiring third parties to sign commitment of not disclosing the unit’s information for the important information.

**2. Within the time of deploying works**

a) Providing and requiring third parties to comply in full with the regulations and provisions on safety and IT security of unit.

b) Monitoring the compliance with regulations on safety, IT security of third parties’ personnel.

c) In case of detecting signs of violation or committing violations of regulations on safety, information security of third parties, the unit needs:

- Suspending or terminating third parties’ operation depending on the seriousness of violation.

- Officially notify violations on safety and IT security of personnel to third parties.

- Checking to determine, making report on seriousness of the violation and notifying to third parties about the damages caused.

- Withdrawing IT system accessing right which was granted to third parties.

**3. When finishing works**

a) Requiring third-parties to transfer using assets of the unit during the job deployment.

b) Withdrawing IT system accessing right which was granted to third parties right after finishing the jobs.

c) Changing the locks, passwords receiving from third parties’ delivery.

**ITEM 4. ENSURING SAFETY ON PHYSICAL AND ENVIRONMENTAL ASPECT**

**Article 11. Physical safety and environment**

1. The areas of handling, storing information and information handling facilities must be protected safely by walls, controlled gateway.

2. The areas having high requirements on safety and security as server room must apply suitable entry and existing control measures, to ensure that only those who have duties can enter into that area.

3. Having measures to protect, prevent, combat risks from fire, explosion, flood, earthquake and other disasters caused by natural and human being. The server room must be ensured industrial hygiene: not to be leaked, waterproof; equipment installed on the technical floor is not shone directly by the sun shining; the humidity, the temperature reaching the standards as prescribed for devices and servers; equipping in full devices to prevent fire, explosion, flood, lightning;.

4. Having internal rules, guidance to work in the safe, secure area.

5. Areas of common use, distribution and shipping must be controlled and isolated from in the safe, secure area.

**Article 12. Safety, keeping secrets information technology assets**

1. IT assets must be located and installed at the safe location and be protected to minimize the risks due to intimidation, danger from environment and illegal intrusion.

2. IT assets must be secured on the power and support system when the main power is interrupted. Must take measures to resist overload or voltage drop, surge lightning; with adjacent systems; a system backup generators and UPS systems to ensure equipment operating continuously.

3. Cable providing power and communications cables used in transmitting data or information support services must be protected from intrusion or damage.

4. All data storage devices must be checked to ensure that critical data and copyrighted software stored in the device to be deleted or overwritten unable to recover before removing or re-used for other purposes.

5. IT assets shall be sent out only when the unit has permission of the competent levels.

6. The equipment used for installing operations outside of unit’s head office must take measures to monitor, secure safely against unauthorized access.

**ITEM 5. OPERATING MANAGEMENT AND COMMUNICATIONS**

**Article 13. Process of operation**

1. Promulgating and deploying the process of operating IT systems to users including: The process of turning on, off device, the backup, data recovery, device maintenance, operating application; troubleshooting.

2. Controlling change of IT systems including software version, hardware configuration, documentation, operating procedures; having backup plans for recovery if the change is not successful or meeting unanticipated problems; recording changes; making plan of implementation and examination, test of the changes before the formal application.

3. The official operating system must meet the requirements:

- Separating from development environments and test, examination environments.

- Only allowing to connect Internet for the IT system has been adopted fully safety, security solution and able to protect against threats and attacks from outside.

- Not to install tools, means of developing application on the official operating system.

4. For the professional information system:

a) Not to assign an individual to do the whole processes from initial process to an approval of a professional transaction.

b) Every action on the system is tracked, ready for inspection and control as needed.

**Article 14. Management of services supplied by third parties**

1. Must supervise and inspect the services provided by third parties to ensure service supplying levels, the system operating ability to meet in accordance with agreements signed.

2. Ensuring to implement, maintain security, safety measures of services provided by third parties in accordance with agreement.

3. Managing changes for services provided by third parties including: Upgrading the new version, using new techniques, tools and new development environment; valuating fully impact of the change to ensure safety when putting into use.

**Article 15. Management of setting up plan and accepting information technology system**

1. Monitoring and maximizing performance of IT systems, planning on performance and capacity of IT systems in the future to ensure the necessary standards.

2. Setting up requirements and standards such as performance, time to recover when meeting troubles, ensuring the continuity; training and technical transfer to the changing contents to users and implementing the examination, valuation the ability of new IT systems or upgraded systems before the official application.

**Article 16. Storing for backup**

1. Promulgating and implementing backup procedures and recovery for software, data needed.

2. Make a list of data, software need to be backed up with classification according to storage time, backup time, backup methods and system recovery inspection time from backup data.

3. Backup data must be stored securely and checked regularly to ensure readiness for use when needed. Inspecting and recovering system from backup data at least every six months.

**Article 17. Management on safety, keeping secrets internet**

1. Performing network management and control to prevent hazards and maintain safety to systems, applications using network:

a) Having logical outline and physique on network system;

b) Using a firewall device or equipment to detect and prevent intrusions and other equipment to ensure safety, network security.

2. Setting up, configuring fully all the features of network security devices. Use tools for detecting and timely finding out weak points, vulnerabilities and unauthorized access to the network. Regularly inspecting and detecting the connections, equipment and software installed illegally into the network.

3. Identifying and clearly writing safety features, the security level of service and management requirements in the agreements on network services provided by third party.

**Article 18. Information exchange**

1. Promulgating regulations of exchanging information and software through communication network in the unit and with other units. Determining responsibility and liability for the components involved.

2. Having agreement to the information exchange with the external.

3. Taking measures to protect means of keeping information when moving.

4. Setting up and implementing measures to protect the information exchanged between IT systems.

**Article 19. Electronic trading services**

1. Taking measures to protect information in electronic commerce to combat activities of fraud, illegal modification:

a) Transmission and communication protocols must be encrypted;

b) Using strong authentication methods such as multi-component authentication or digital signatures for members participating in the transaction.

2. Information in online transactions must be transmitted in full and correct address, avoiding being modified, disclosure or an unauthorized duplicate.

3. Public information on the IT systems must be protected to prevent unauthorized modification.

**Article 20. Supervision and writing up operation diary of information technology system**

1. Logging and prescribing storage time of information on the operation of IT systems and users, errors arising and incidents causing unsafe to the information to assist in later investigation, supervision.

2. Reviewing and making periodic reports on logs and activities dealing with errors and necessary incidents.

3. Protecting features logging and log information, anti-counterfeit and unauthorized access. System administrators and users may not delete or modify the system log which records their own activities.

4. There are mechanisms of time synchronization between IT systems.

**Article 21. Prevention and combat of virus and mal-ware**

Setting up and implementing regulations on anti-virus, malicious code to meet the following basic requirements:

1. Developing systems to prevent computer viruses for the entire IT system of units.

2. Inspecting, killing virus, malicious code for the entire IT system of units every day and means of keeping information from the outside before using.

3. No opening strange e-mails, the attachments or links in the strange email to avoid viruses, malicious code.

4. No accessing websites which have no clear origin, suspicious.

5. Promptly updating the model virus, mal-ware and antivirus software, new mal-ware code.

6. Immediately notifying to the system administrators to handle in the cases detecting but unable to kill viruses, malicious code.

7. No installing software self-willed without permission from the system administrator.

**ITEM 6. MEASURES OF ACCESSING MANAGEMENT**

**Article 22. Professional skill requirements for accessing control**

1. Building and implementing regulations on accessing management for users, user groups, guaranteeing to meet business requirements and safety, security requirements. Provisions on accessing management include the following basic contents:

a) Registration, issuance, renewal and withdrawal of access right of users;

b) Limitation and control of privileges accesses;

c) Management and allocation of passwords;

d) Review, examination and revision of access right of users.

2. Regulations on accessing management must meet the following requirements:

a) Password length must be six characters or more, made ​​up of numeric, text and other special characters if the system allows. Requirements of valid password must be checked automatically when setting up password;

b) The default password of the manufacturer installed availably on the equipment, software, databases must be changed right when put into use;

c) Password management software must have the functions: to announce to users for changing their passwords which are going to expire; to cancel the validity of the password expired; to allow changing immediately the password disclosed, to be in danger of being disclosed at the request of users; to stop the use the old password in a certain time.

3. Stipulating liability of users when being granted right to access: Using password in compliance with regulation, keeping confidential password, exiting from the system when not working on it or temporarily not working on it.

**Article 23. Management of internet access**

1. Promulgating regulations on use of the network and network services, the licensing procedures, removing the right to connect to the network and network services, the ways and means of network access, network services. In which specifying clearly:

a) The network and network services are permitted to use;

b) Conditions for being connected to the network.

2. Using appropriate measures to authenticate users connecting from outside into the unit's internal network ensuring safety, security.

3. Controlling the access to the ports used to configure and manage network devices.

4. Splitting the network into different network regions according to using object, purposes and information systems.

**Article 24. Control of operating system access**

1. Having procedures to control the access to operating system; provisions on managing password to access into operating system safely, securely.

2. Person who uses operating system must have a unique identifier and to be verified, identified, saved traces when accessing into the operation system.

3. Using more other authentication methods such as biometry or card for critical servers besides the authentication by password.

4. Providing for limits and strict control of the system utility which is able to affect systems and other applications programs.

5. Automatically disconnecting the working shift after a period of not using, to prevent unauthorized access.

6. Providing for time limits connected with the high risk applications.

**Article 25. Control of information access and application**

1. Managing and assigning the right to access to information and applications suitable to the functions and responsibilities of users:

a) Assigning the right to access to each folder, the function of program;

b) Assigning the right to read, write, delete, execute to information, data and program.

2. The important information system must be put in a private computer network environment. If the information systems together use common resources, they must be accepted by the system administrator.

**ITEM 7. RECEIPT, DEVELOPMENT, MAINTENANCE OF INFORMATION SYSTEM**

**Article 26. Requirements on safety, keeping secrets to the information systems**

When building new information systems or improving existing information systems, relative persons must offer requirements on safety, security, simultaneously with the offering of technical, professional requirements.

**Article 27. Ensuring safety, keeping secrets of applications**

The business applications program must meet the following requirements:

1. Checking the validity of data entered into the application, ensuring data is entered correctly and valid.

2. Checking the validity of data need to be handled automatically in the application to detect incorrect information due to errors in the course of processing or behaviors of modifying information deliberately.

3. Having measures to ensure the authenticity and protect integrity of data to be processed in applications.

4. Checking the validity of the output from applications to ensure the course of processing information of the applications is accurate and valid.

**Article 28. Management of encryption**

1. Stipulating and putting to use encryption measures and key management in accordance with national or international standards which have been recognized to protect the information of the unit. Using encryption algorithms such as:

a) AES: Advanced Encryption Standard;

b) 3DES: Triple Data Encryption Standard;

c) RSA: Rivest-Shamir-Adleman;

d) Other algorithms.

2. Data on customer passwords, user passwords and other sensitive data must be encrypted when transmitted over the network and stored.

**Article 29. Safety, keeping secrets system files**

1. Providing for management, installment, updating of the software on existing systems, ensuring safety for the file system.

2. Checking, testing data must be selected, protected, managed and controlled carefully.

3. The access to source program must be managed and controlled strictly.

**Article 30. Safety, keeping secrets in the process of support and development**

1. There must be regulations on management and change control of information system.

2. When changing the operating system must examine and review critical business applications to ensure the system operating stably, safely in the new environment.

3. The amendment of software packages must be managed and controlled strictly.

4. Supervision and strict management of hiring, purchasing external software.

**Article 31. Management of weak points on technology**

1. Having provisions for the assessment, management and control of technical weak point of IT systems in use. Periodically assessing and reporting on technical weak point of IT systems in use.

2. Developing and implementing solutions to overcome the technical weak point, limiting the concerned risks.

**ITEM 8. MANAGEMENT OF TROUBLES ON INFORMATION TECHNOLOGY**

**Article 32. Troubleshooting report**

1. Setting up the process of report, report templates and specifying clearly the reporting recipients for IT problems.

2. Clearly defining responsibilities of report of managers, staffs and third parties about the IT problems.

3. The unsafe incidents must be immediately reported to the competent persons and those relating to remedies in the shortest time.

**Article 33. Controlling and troubleshooting**

1. Promulgating procedures, responsibilities to overcome and prevent IT problems, ensuring incidents to be handled in the shortest time and minimizing the possibility of repeated incidents.

2. The course of handling troubleshooting must be recorded and stored in the unit.

3. Collecting, recording, preserving evidence and proof for examination, treatment, recovery and prevention of incidents. In the case of having IT incidents related to violations of law, the unit is responsible for collecting and providing evidence to the competent authorities in accordance with the provisions of law.

**ITEM 9. ENSURING OF CONTINUOUS OPERATION OF THE INFORMATION TECHNOLOGY SYSTEM**

**Article 34. Ensuring of continuous operation**

1. Depending on the size and importance level of each IT system for operation of the unit to select the critical IT systems, can significantly affect the operation of the unit.

2. Developing and implementing plans and processes to ensure continuous operation of critical IT systems.

3. Minimum every six months, inspecting, testing, evaluating and updating processes to ensure continuous operation of critical IT systems.

4. Plans, processes to ensure continuous operation must be examined, evaluated and updated when the system changes.

**Article 35. Acts of disaster prevention**

1. Building backup system for critical IT systems of the unit. The backup system must be away from the main system at least 30 kilometers calculating upon a straight line connecting the two systems.

2. Backup system must be able to replace the main system within four hours since the system has the unable to overcome problem.

3. Minimum every three months, the unit must move operations from the main system to the backup system to ensure the uniformity and availability of backup systems.

4. Minimum every three months, conducting inspections, evaluating operation of the backup system.

**ITEM 10. INTERNAL EXAMINATION AND REPORT**

**Article 36. Internal examination**

1. The units must self-organize to examine the compliance of the provisions of this Circular at least once a year.

2. Inspection results and recommendations must be made into the report.

**Article 37. Report**

The unit is responsible for submitting reports to the State Bank of Vietnam (Department of Information Technology) as follows:

1. Regulation of safety, IT security of the units:

a) For the units issued regulations on safety, IT security before the effective date of this Circular: The units send regulations of safety, IT security within 15 days from the effective date of this Circular.

b) For units not yet issued regulations on safety, IT security from the effective date of this Circular: The units must issue and sent the regulation on safety, IT security within six months from the effective date of this Circular.

2. Annual report:

a) The amendments, supplementation of IT security, safety regulations, if any, reports of internal inspection of units under the provisions of Article 36 of this Circular.

b) Deadline for sending report: before the 15th of March annually.

c) Forms and report form: Under the guidance of the State Bank of Vietnam (Department of Information Technology).

3. Irregular report:

Upon the occurrence of cases, the safety loss for IT systems and units shall send irregular report in writing, specifically as follows:

a) The deadline for submission of report: Within 10 days from the time the case is detected.

b) Contents of irregular report:

- Date, place where arises the case;

- The cause;

- Assessment of risk, impact on IT systems and operations at the place of incident and other relevant locations;

- The measures that the units were taken to remedy and prevent risks;

- Petition and proposal.

**Chapter 3.**

**IMPLEMENTATION PROVISIONS**

**Article 38. Handling of violations**

Organizations, individuals who commit violations of provisions of this Circular, depending on the nature and seriousness shall be handled according to provisions of law.

**Article 39. Effect**

1. This Circular takes effect after 45 days since the date of issuing and replaces the following documents:

- Decision No.04/2006/QD-NHNN dated 18/01/2006 of the Government of the State Bank on stipulating regulation of safety, keeping secrets IT system in banking field;

- Decision No.14/2000/QD-NHNN16 dated 07/01/2000 of the Government of the State Bank on stipulating regulation of management, use of IT system in banking field;

- Decision No.864/2003/QD-NHNN dated 05/8/2003 of the Government on amending, supplementing a number of Articles of management, use of IT system in banking field issuing together with this Decision No.14/2000/QD-NHNN16 dated 07/01/2000.

2. During the course of implementation, if any problems, difficulties arise, relative units promptly reflect to the State Bank of Vietnam for consideration, supplementation and modification.

**Article 40. Responsibility of implementation**

1. Department of Information and Technology is responsible for supervision, inspection of the implementation of this Circular of the Units.

2. The inspection agency, banking supervision are responsible for coordination with Department of Information and Technology to inspect the implementation of this Circular over the credit institutions, branches of foreign banks and handling administrative violations for the violations according to law regulations.

3. Department of Internal Audit is responsible for the implementing internal audit the implementation of this Circular for the units under the State Bank of Vietnam.

4. Heads of relative units under the State Bank of Vietnam; Directors of branches of the State Banks provinces, cities directly under the central; Chairman of management board, General Directors (directors) of the credit institutions, branches of foreign banks are responsible for deploying and inspecting the implementation at its unit in compliance with law regulations of this Circular.

|  |  |
| --- | --- |
|   | **FOR THE GOVERNORNguyen Toan Thang** |

------------------------------------------------------------------------------------------------------
*This translation is made by* ***LawSoft****, for reference only.* ***LawSoft*** *is protected by copyright under clause 2, article 14 of the Law on Intellectual Property.* ***LawSoft*** *always welcome your comments*