REGULATIONS

SAFETY AND SECURITY OF INFORMATION TECHNOLOGY SYSTEM OF EZLANDVIETNAM DEVELOPMENT JOINT STOCK COMPANY

Table of contents

CHAPTER I: GENERAL REGULATIONS

Article 1. Scope of application

Regulations on safety and security of Information Technology system (hereinafter referred to as IT security regulations) stipulate requirements for users as well as IT Department on basic security techniques of information technology systems at Ezland Vietnam to safely and effectively unify the management of the application of information technology to the Company's activities.

Article 2. Interpretation of terms

1. **Information technology system (IT):** is a structured collection of hardware, software, database and network systems serving one or more technical and professional activities.
2. **IT assets:** are equipment, information belonging to the IT system of the Company. Include:
    a. Physical assets are IT equipment, media and equipment for the operation of IT systems.
    b. Information assets are data and documents related to IT systems. Information assets are presented in paper documents or electronic data.
    c. Software assets include application programs, system software, databases, and development tools.
3. **IT risk:** is the likelihood of losses when carrying out activities related to IT systems. IT risks relating to management, use of hardware, software, communications, system interfaces, operations and human beings.
4. **Risk management:** coordinated activities to identify and control possible IT risks.
5. **Firewall:** is a collection of components or a system of equipment, software placed between two networks to control all connections from inside to outside the network or vice versa.
6. **Malware (malicious code):** is software that has harmful features such as viruses, spyware, adware or other similar forms.
7. **Technical weakness:** is the position in the IT system that is vulnerable when being attacked or illegally penetrated.
8. **Sensitive information:** are important information classified as confidential or confidential according to company regulations.
9. **Data integrity:** is the state of existence of the data as it is in the original documents and no change in data, structure or data loss.
10. **Storage:** means to make copies of software or data for the purpose of protecting against loss and damage of software and original data.
11. **Virus:** is a computer program capable of spreading, causing abnormal operation for digital equipment or copying, modifying or deleting information stored in digital equipment.

12. **Employees:** are the employees of the Company who are granted accounts to use the IT system resources of the Company.
13. **User account:** is a means to confirm and manage access to the IT system. The account includes the username and password.
14. **Authorization:** is a license granted to an individual according to the organization's pre-formed format to access and use an IT system program or process.
15. **Network security system:** is a collection of firewall devices, control devices, detection of illegal access, management software, monitoring and logging of network security status and another equipment, which functions to ensure network safety, all work in sync with a consistent network security policy in order to strictly control all activities on the network.
16. **Third party:** is a professional organization or individual hired or cooperated by the Company to provide technical goods and services to the IT system.

Article 3. General introduction on information security

1. Information security

Information security is to ensure information is kept confidential, not changed, lost, leaked and ensure readiness when any situation occurs.

2. Risk of information security

- Information system hazards can be classified as accidental or intentional, proactive or passive.
  a. Accidental threat: when users login the system in admin mode, they can freely modify the system. But after completing the work, they do not log back into the normal user mode to use the system, accidentally letting the bad guys take advantage.
  b. The threat that someone intentionally accesses the unauthorized system to sabotage or steal data.
  c. Passive threat: is a threat but not yet or does not affect the system directly, such as eavesdropping on packets.
  d. Proactive threat: the modification of information, changing the operational status of the system in order to steal information, sabotage normal operation of the system.
- For each information system, threats and potential consequences are enormous. It may arise from the following causes:
  a. From the user's side: illegal infiltration, stealing of valuable assets.
  b. In Information System Architecture: Organization of the technical system is unstructured or not strong enough to protect information.
  c. The information security policy: Do not approve the safety standards, do not specify the rights in the system access.
  d. Information in the system will also be vulnerable if there are no management tools, checks, and control systems.

e. The risk is in the hardware structure of the information equipment and software, systems and applications built by the manufacturer of spyware in the device, system software and applications.
f. From the outside: hackers.

Article 4: Information security requirements

1. **Information Security Requirements**
    a. Confidentiality: Information cannot be approached by people who do not have the authority.
    b. Integrity: Information cannot be modified, removed or supplemented by incompetent persons.
    c. Availability: Information that is available to meet the needs of the competent person.
    d. Undeniable: The initializing information cannot deny the liability for the information created by yourself.
    e. Authentication: Determining the origin of the information.

2. **Determining the security requirements of the IT system**
    The classification of the request, the level of investment for the company's IT system security is clearly defined based on the following factors:
    a. The role of the IT system in implementing the objectives of the company.
    b. Origin, risk of the risk occurring for IT systems.
    c. Risk of remediability.
    d. The acceptable degree of risk.
    e. Influence of the risk if it occurs for company activities.

Article 5. Employees responsibilities and rights

1. **Responsibilities:**
    a. Timely protection and reporting with IT management in case IT systems have signs of failure, trouble, loss of safety (considered signs that do not normally appear – warning signs...).
    b. Do not alter the program itself, remove Programs and specifications that IT manages to have installed. Do not install by yourself, using other programs in addition to programs that IT manages to have installed, except where permitted by the head of the department and approved by IT departments.
    c. To be legally responsible for the information you post, update to the IT system.
    d. Confidentiality of the user's access account information shall be responsible for changing the password periodically as prescribed when exposed or suspected to be exposed.
    e. Do not suspend operations, illegally exploit the resources of the company's IT systems.
    f. Do not impede the task of developing, deploying, constructing, maintaining and troubleshooting the company's IT systems.
    g. Do not take advantage of or conceal the abuse of the device, password and key code to access the company's IT system.

h. Do not disclose system architecture, algorithm... of the IT system.
i. Do not use of company IT equipment for personal purposes.

2. **Rights:**
   a. Exploit, use the company's IT system resources in the scope of permission, to serve the job requirements.
   b. Have the right to propose wishes, participate in the construction of the company's IT system completion.

Article 6: Regulations on Sanctions

Employees have violations of this policy and other relevant regulations, depending on nature, the extent will be handled in accordance with company regulations and law provisions.

CHAPTER II: SPECIFIC REGULATIONS

SECTION 1: MANAGEMENT OF IT ASSETS

Article 7: Regulations on IT asset management

The management of IT assets must ensure the requirements:

a. Statistics, inventory of the company's and subsidiaries' IT assets minimum of once per year. Asset statistics content must include the information: asset type, value, level of importance, the position of installation, backup information, information about copyright.
b. Sorting, prioritizing orders by value, importance level of IT assets for the protection of appropriate assets. To develop and implement regulations on management and use of assets.
c. To attach the use of assets to specific individuals or parts. Users of IT assets must comply with the regulations on the management and use of assets, ensuring that assets are used for the right purpose.

Article 8: Regulations on the safety and security of IT assets:

a. IT assets must be arranged, installed at safe and protected locations to minimize the risks posed by threats, hazards from the environment, or unauthorized intrusions.
b. IT assets must be secured for electricity and support systems when the main source is interrupted. Must take measures to fight overload or decrease voltage, lightning resistance spread; There is a grounding system, a backup generator system and a power-saving system that ensures the continuous operation of the device.
c. Cables that provide power source and communication cables used in data transmission or information support services must be protected from infringement or damage.
d. The equipment maintenance and upgrade must be accurate to avoid the situation in which the operation is not correct with the original design which impairs the operation of the company after the device upgrade.

e. All data storage devices must be inspected in order to ensure that important data and copyright software stored on the device are deleted or overwritten without the possibility of restoring before removal or reuse for other purposes.
f. IT assets are only taken outside the company with the permission of the competent level.
g. The equipment used for the operation of the installation outside the company's headquarters must have measures to supervise and protect the safety of unlawful access.
h. High value/risk devices (servers, valuable hardware, software) are located in the Server room separated from the working area and must have additional safety measures to protect such as the access control system and the camera.

SECTION 2: MANAGEMENT OF HUMAN RESOURCES

Article 9: Regulations on human resource management

1. Internal Human Resource management

1.1 Before hiring or assignment of tasks

a. Determine the responsibility for the IT safety, security of the employee. Clearly defining roles and responsibilities of employee through documents and texts to avoid errors.
b. A background check, a strict evaluation of ethics, professional qualifications when hiring.
c. The recruitment decision or contract (if any) must include the terms of responsibility for the safety and security of IT during and after work at the company. Positions that hold information security and sensitive information of information systems, before being officially recruited must sign the information security commitment to the company.
d. Probationers are only permitted to have limited access to the company's system and their activities must be monitored during the probation period.

1.2 In the process of working

a. Subsidiaries are responsible for disseminating and updating regulations on IT safety, security for employees. All employees, including employees in the probation period, are required to sign confidentiality agreements and must not disclose Company information.
b. Examining the implementation of regulations on IT safety and security of individuals and affiliated units at least once a year.
c. Apply disciplinary measures according to the Company's Regulations to employees who violate IT safety, security regulations.
d. All employee information will be strictly confidential and only shared basic information with the consent of the manager.

1.3 When terminating a labor contract or changing jobs

When the employee terminates or changes the job, the dependent units must:

a. Clearly define the responsibilities of employees and stakeholders on the IT system.

b. Making a handover record when handover assets to employees.
c. Revoke or change the access rights to IT systems, employees' assets.
d. The responsibilities and duties related to confidentiality agreement remain valid when the employee has left the job.

2. Management of the third party

2.1 Pre-deployment workflow

The focal unit working with the third party must:

a. Require the third party provides a list of personnel involved.
b. Legal examination and professional competence examination of the third-party personnel in accordance with the requirements of the business.
c. Require the third party to sign the non-disclosed agreement by which they will not disclose important information of Ezland Vietnam.

2.2 During work deployment

a. Provide and require the third party to fully comply with the regulations on the safety and security of Ezland Vietnam.
b. Monitor compliance with third-party personnel safety and security regulations.
c. In case of detection of signs of infringement or breach of security regulations, third-party information security, the focal unit working with the third-party should:
d. Suspend third-party activity depending on the level of infringement.
e. Officially announce the breach of IT safety and security of personnel to third parties.
f. Examination, determination and establishment of the level of infringement and report to the third party about the damages occurred.
g. Revoke access right to the IT system that has been granted to the third party.

2.3 At the end of the work

a. Require the third-party to hand over the assets used during the work deployment (if any).
b. Revoke the access to the IT system that was granted to a third-party immediately after the end of the work.
c. Change the keys, passwords received from third-party.

SECTION 3: ASSURANCE SAFETY ON PHYSICAL AND ENVIRONMENTAL

Article 10: Regulations on physical safety and environment

1. Processing areas, information retention and information processing media must be safely protected by wall or glass walls, controlled entrance gates.
2. The server room and placing areas, using the IT equipment must have rules, guidance on working and applying safeguards, control access, ensure that only those who have a new task are in those areas.

3. The work conducted in the server room must be logged daily working diary.
4. Measures to protect against the risk of explosion, flooding, earthquake and other disasters caused by nature and humans. Computer room must ensure hygiene: no water leaking, waterproofing; The equipment installed on the technical floor, not directly illuminated sunlight; Humidity, temperature meet the standards specified for the device and the server; Fully equipped with fire and explosion protection equipment and anti-illegal access.
5. The equipment used for the operation of external installations outside the Unit's headquarters must have measures to monitor, secure protection against illegal access and manage the use of such equipment.
6. The program, the data of the company which is likely to be used will have to be completely removed when delivering the equipment containing such program, data to the external party or when the asset is liquidated.
7. Power supply and cable system for IT system:
    a. The server room must be equipped with a separate power source with standards in accordance with the equipment installed in the engine room, connected to the UPS to ensure uninterrupted operation even during a power outage.
    b. The standby power source must meet standards, capacity for normal operation of the IT system during a main power failure.
    c. All cabling systems (electrical cables, telephone cables and network cables) must be placed within safety limits according to the manufacturer's detailed descriptions.
    d. Lightning protection filters must be installed in all outgoing communication lines.
    e. Flammable materials must be stored in a safe distance from the protected area.
    f. Fire alarm devices such as smoke detectors and fire extinguishing equipment are installed where appropriate and must be maintained.
    g. Train employees to operate firefighting and evacuation equipment in case of emergency.

SECTION 4: OPERATION MANAGEMENT

Article 11: Regulations on safety management and network security

a. Must register and be approved for use before accessing the network.
b. When detecting signs of loss of safety, immediately notify the IT management department.
c. Update new version of antivirus software and regularly scan the virus on the computer connected to the network. Do not make any changes, remove the programs, specifications that IT manages to have installed; Do not install it yourself, run illegal programs that affect the network system.

Article 12: Regulations on the prevention of computer viruses and malware

a. Regularly check and remove viruses;
b. Software, data and other media that are received from outside must be tested for viruses before use;

c. Do not open strange messages, attachments or links in strange messages to avoid viruses;
d. Do not visit websites which has no clear origin;
e. Do not arbitrarily share the folder on your computer with “everyone” permission for other computers to access;
f. Timely update new virus samples and anti-virus software;
g. In case of detecting but unable to remove the virus, immediately notify the IT management to handle it.

Article 13: Regulations on the workplace, computer screen

a. Documentation cannot be placed on printers, copiers, and fax machines. After use, the document must be removed from those devices.
b. The user must follow the IT staff's instructions to protect the computer by setting the password when opening the machine and the password for the standby screen mode.
c. When there is a need to leave the workplace, it is a must to lock the screen immediately (press "Windows key + L" to lock).
d. When there is no need for long-term work, users must shut down the computer completely, avoiding leaving standby mode.
e. Keep your workplace clean, do not put food and beverage next to the computer.

Article 14: Regulations on passwords

1. **General principles**
   a. All users’ passwords (e.g. mail, Web, desktop computer...) must be changed at least 01 time in 45 days.
   b. Never write the password to the paper or store it online. The password is also not allowed to be included in electronic mail or other forms of electronic communication. All user-level and system-level passwords must be correct with the Create password guidelines below. Complex password modes must also be used.
   c. Force the user to change the temporary password first when they sign in for the first time.
   d. Limit the number of failed sign-in attempts.

2. **Principles for setting a password**
   a. Password includes both uppercase and lowercase characters (a-z, A-Z)
   b. There are numeric characters and special characters (0-9, @ # $% ^ & * () _ +;?, {,}, ”, <,> ....)
   c. Minimum length of 08 characters.
   d. Not including information related to humans such as name, ID card number **...**

3. **Standards for password protection**
   a. All passwords are considered sensitive and confidential information of the company.
   b. Prevention is always the best security way.

c. Do not expose the password over the phone, in the title or the email content or share with anyone.
d. Do not use words reminiscent of passwords (such as: surname, first name....)
e. Do not share passwords with any person include member of the family, friend,… without permission of Ezland Vietnam.
f. Do not use the "Remember passwords" feature of applications (e.g. Outlook, browser, messenger)
g. Do not write passwords and store them anywhere in the office. Do not save passwords in files and leave computers without encryption.
h. If there is any doubt that the password has been exposed, immediately notify the admin and immediately change the password.

Article 15: Regulations on e-mail

1. **General regulations on email system of Ezland Vietnam**

- Ezland Vietnam's e-mail system provides employees to support the implementation of daily business transactions in the Company's operations. The e-mail system allows employees to communicate with the inside as well as outside individuals through the Internet.

- E-mail system is only used for business purposes. Ezland Vietnam employees should be aware that all emails sent, received or stored in the system will become the Company's intellectual property.

- Users must not use Elzand Vietnam 's e-mail to distribute:

a. Viruses or programs intended to harm the Company's computers or networks, customers and partners.
b. Information of an illegal nature, distorting or political issues, which is prohibited by Vietnamese law.
c. Information that is barbarism, libelous, insulting to individuals or other organizations, issues related to religion, racial discrimination, gender discrimination, obscenity, pornography ...

2. **Regulations on the use of the e-mail**

a. The mailbox name is set according to the standard with the user's signature.
b. Employees must be very careful when using internal mail boxes over the public Internet.
c. All employees must be more cautious about sending confidential information in the system via email system than other media (paper notices, paper letters, etc.) because e-mail can easily spread very large numbers of people in a very short time.
d. All confidential information in the email is not allowed to send to people or groups of people who do not have the right to know this information or forward to those who are not needed to know this information to avoid important information leakage.
e. Confidential or sensitive information is not allowed to send via email unless the content is securely encrypted through means of encryption (for example, using a password when opening a document).

f. Users are responsible for protecting their email accounts, not sharing their information and account data with others.
g. Do not forge or attempt to forge other people's emails.
h. Do not attempt to hide your identity or fake your identity when sending emails.
i. Do not use someone else's email account or another email account (not Ezland Vietnam's email account) to send to the internals.
j. Do not send mails that do not comply with daily work requirements including sending "spam" or advertising to recipients (which the recipient does not want).

Article 16: Regulations on Internet access

a. It is the responsibility of everyone to protect the company's network, be wary of the negative impact of the Internet. Be responsible in accordance with the law if covering or allowing other persons to use the equipment, your key code to perform criminal acts.
b. Use appropriate measures to authenticate users who connect from outside to the local network to ensure safety and security.
c. It is your responsibility to abide by the provisions of the contents of information brought on the Internet and commit to comply with those provisions.
d. Do not have the action that interferes with, disrupts the operation of the Internet. Do not affect other information systems, or infringe on the rights and honors of other individuals through the Internet.
e. Do not use tools, software and technical measures under any circumstances which causes capture bandwidth, causing network congestion.
f. Do not visit unhealthy sites, these weird links avoid viral infections that lose data and affect company operation.

Article 17: Regulations on data storage

1. **Storage System Requirements**
   a. Ensure the integrity and completeness of the data stored during the entire storage period.
   b. Proper storage and sufficient duration of each data type in accordance with the regulations of the company.
   c. The necessary data types for maintaining or restoring business operations when there is a problem must be stored at least in two separate locations.
   d. When necessary, the cached data must be converted to the original data format before saving.

2. **Responsibilities of the Data Administrator**
   a. Strictly implement the regulations governing the storage and preservation of data storage and be responsible for the subjective risks to the stored data.
   b. Do not grant permission for any organization or individual that exploits, uses stored data without the written consent of the competent person.
   c. In the event of risk or detection of risk with electronically stored data, must immediately report to the competent person to take measures to process and remediate promptly.

SECTION 5: MANAGING IT PROBLEMS

Article 18: Problems report

a. Report a problem following the IT troubleshooting process.
b. Clearly defined responsibilities for reporting employees and third parties about IT incidents.
c. Unsafe incidents must be immediately reported to the competent and relevant persons for remedial measures as soon as possible.

Article 19: Control and troubleshooting

a. Follow the IT troubleshooting process, ensuring the problem is handled in the shortest possible time and minimizing the likelihood of repeated problems.
b. The troubleshooting process must be documented and stored at the company.
c. Collection, record, preservation of evidence for the inspection, handling, remediations and prevention of incidents. In the event of an IT incident involving violations of the law, the company is responsible for collecting and providing evidence to the competent authorities in accordance with the law.