Direction of Information Security Standards for the Virtual Currency Industry

Chapter I	**General**
1.	The purpose of the Direction is to erect principles of information security management for the association corporate members (hereinafter referred to as "member") of the Bitcoin and Crypto Currency Development Association (hereinafter referred to as "Association") while engaging in virtual currency-related business activities. The virtual currency-related business referred to in the preceding paragraph is defined as the follows: (1) Exchange of virtual currency with New Taiwan Dollars, foreign currencies and currencies issued by Mainland China, Hong Kong or Macau. (2) Exchange of virtual currencies. (3) Transfer of virtual currency. (4) Safekeeping, managing virtual currency or providing related management tools. (5) Participating in and providing financial services related to the issuance or sale of virtual currency.
2.	Each member shall clearly construct the information security management policy, and maintain and operate the information security management system.
Chapter II.	**Information Security Management Policy**
3.	Members should formulate the information security management policy, which should include: (1) The definition, objectives, and scope of information security. The scope should include core systems (e.g. trading platforms, wallet systems, etc.). (2) The principles and standards of information security. (3) The organization shall be established for information security management related work, the organization's top person in charge, and the organization's responsibilities, etc. (4) Relevant standards and regulations that the employees should abide by. (5) Regulations and instructions related to notification of information security emergency.
4.	Information security management policy should be formulated with reference to relevant laws and actual business implementation needs.
Chapter III.	**Establishment of Information Security Management Organization**
5.	The information security management policy should specify the establishment, responsibilities and division of labor of the information security management organization; designate senior management personnel to be responsible for the coordination and promotion of information security management matters; and establish a cross-unit information security implementation promotion team to coordinate information security policy, plans, resource scheduling, etc.
Chapter IV.	**Information Security Management and Maintenance**
6.	Members should formulate relevant management and maintenance plans in accordance with the information security management policy, and regularly review the effectiveness of the plans.

7.	Members should conduct regular or irregular independent audits on the information system, including but not limited to internal self-audits, and make improvements based on the audit results.
Chapter V.	**Risk Management**
8.	Risk Management of information security management should be conducted by means of risk assessment, and effective control measures should be adopted.
9..	Risk management standards should include standards of risk tolerance and information risk assessment implementation.
10.	For virtual currency assets, members should prepare inventory or other forms available for identifying assets and should regularly review whether the content of the items is sufficient to reconstruct the company's virtual currency assets. The items should contain at least the following: (1) Asset item. (2) Asset importance or value. (3) Asset manager and the person in charge.
11.	Members should analyze the possibility of risk occurrence and afterwards consequence. The follows methods should be adopted to deal with and respond: (1) Reduce: Formulate and implement control measures to reduce risk. (2) Avoid: Cease the business operation. (3) Accept: Seek businesses outsourcing or external insurance.
12.	Targeting risks, management policies should be planned and implementation plans should be executed.
Chapter VI.	**Security management of virtual currency assets**
13	For virtual currency assets, the custody, authorization control and quota management mechanism should be established.
14.	Hot wallet and cold wallet structure should be planned according to the characteristics of virtual currency assets and the needs of organization operation.
15.	The management measures of the wallet system should take the follows in consideration: (1) System access authority management and control. (2) Multi-signature technique. (3) Hierarchical authorization management. (4) Transaction monitoring.
16.	The cold wallet system should be offline and properly preserved; relevant access records should be kept for future reference.
17.	The amount of virtual currencies in the wallet system should be inspected regularly to reduce the risk derives from excessive amount of the wallet system.
18.	Effective management process or mechanism should be established for the transfer of virtual currency between cold/hot wallets, and relevant records should be kept for future reference.
Chapter VII.	**System Development Security Management**
19.	When conducting information systems' development and improvement, security needs should be taken into consideration during the requirements phase of planning.

20.	Information systems should protect its confidentiality, preventing leakage or tampering, and the system should be protected by encryption techniques.
21.	The information system should have the following security-related functions: (1) Verifying the authenticity of the input data. (2) Verifying the integrity of internal data. (3) Data should be protected by encryption measures during process of transmission or custody. (4) Utilizing information authentication technique to inspect whether the data content has been tampered or destroyed without authorization.
22.	The information system should establish a testing environment and verification environment which are separated from the production environment, to prevent unauthorized access from occurring.
23.	The information system should establish aproduction environment amendment procedure, and the authorization process should be taken into consideration and strictly implemented, to ensure that the security of production environment from damage.
Chapter VIII.	**Personnel Security Management and Education**
24.	Employees who have access to confidential and sensitive information or the systems, should undergo appropriate security assessment procedures prior to assignment, such as: (1) Work records. (2) Criminal records. (3) Credit records. (4) Reference check.
25.	According to the needs of different occupations, information security education, training and promotion should be conducted regularly to improve employees' awareness of information security.
26.	The content of information security education and training should include information security policy, information security regulations, emergencies reporting procedures and how the information techniques /tools to be used properly.
Chapter IX.	**Network Security Management**
27.	A combination of multi-layered network security measures and defense-in-depth should be established (e.g. application firewalls, intrusion prevention/detection systems, two-factor authentication(“2FA”), internal access control, etc.) .
28.	A network security management mechanism should be established to ensure the security of data transmission through the network and prevent unauthorized access.
29.	For cross-company/organization network systems, network security management should be strengthened; relevant network security regulations should be negotiated.
30.	The security weaknesses of the network system should be inspected regularly, and proper protective measures should be adopted.
31.	When transmitting sensitive data through the Internet, virtual private network (VPN) should be used to ensure the confidentiality of the data.
Chapter X.	**Data security management**

32.	Information should be classified according to its degree of confidentiality and risk, and appropriate management measures should be adopted accordingly.
33.	Each member shall use encryption technique to protect the data with higher confidentiality or risk according to the data classification result during transmission and storage.
34.	Data access rights should be classified, and only accessible to those with occupational needs. Relevant records of access rights should be preserved to avoid unauthorized access from occurring.
35.	An off-site backup mechanism should be established to protect the availability of important data.
36.	When establishing an off-site backup mechanism, the recovery time objective (RTO) and recovery point objective (RPO) should be considered, and one of the following frameworks should be adopted after evaluation based on the construction cost, software/hardware requirements, communication requirements, and construction time has been conducted: (1) Cold backup station. (2) Warm backup station. (3) Hot backup station. (4) Mirror backup station.
Chapter XI.	**Emergency Management**
37.	Emergency management regulations, notification channels, procedures and work procedures should be formulated and drilled regularly.
38.	Scenarios for emergency drills should be formulated according to the actual situation, and should include: (1) Cyber-attack. (2) Internal-caused system fault. (3) External-caused system fault. (4) Data leakage. (5) Natural disaster. (6) Infectious disease.
39.	When an emergency occurs, the responsible unit and the competent authority shall be notified in accordance with the notification channels, procedures and work procedures formulated in advance.
Chapter XII.	**Information Security Management Policy Statement**
40.	Members may submit relevant documents within the scope specified in Article 3 in this document to the Association, including the information security management policy in accordance with the documents, materials and methods designated by the Association; afterwards, the statement of completion of information security management policy may be submitted to the Association. The Association will conduct a documentary review on the statement documents submitted by the members. If the Association has notified for making supplements and corrections to the statement procedure within a time limit, however no corrections are made within the time limit, the Association will not make the announcement mentioned in the third Paragraph. The Association will announce list of the companies who have completed the Information Security Management Policy Statement on the Association's website.

Chapter XIII.	**Other**
41.	The Direction was announced on October 1st , the 111th year of Republic of China, and implemented on January 1, the 112th year of Republic of China.