Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions

Article 1 These Regulations are enacted pursuant to Paragraph 2, Article 29 of the Act Governing Electronic Payment Institutions (referred to as the “Act” hereunder) as well as Article 39 and Article 40 of the Act, to which Paragraph 2, Article 29 applies *mutatis mutandis*.

Article 2 Electronic payment institutions shall comply with these Regulations in carrying out the information system and security management operations of their electronic payment business.

Article 3 The terms as used in these Regulations are defined as follows:

1. "Electronic payment business" shall mean shall mean businesses under the subparagraphs of Paragraph 1, Article 3 of the Act.
2. "Electronic payment platform" ("e-payment platform") shall mean application software, system software and hardware equipment relating to the electronic payment business.
3. "Electronic payment operating environment" shall mean e-payment platform, network, operating personnel, and any application software, system software and hardware equipment used the same network with the e-payment platform.
4. Networks come in the following types:
   (1) "Dedicated network" means using electronic equipment or communication equipment to transmit data via direct connection by dial-up, leased line, virtual private network (VPN), etc.
   (2) "Internet" means using electronic equipment or communication equipment to transmit data via an Internet service provider.
   (3) "Mobile network" means using electronic equipment or communication equipment to transmit data via a telecom service provider.
5. Data protection measures shall have the following attributes:
   (1) Confidentiality: It means data will not be intercepted or hacked for the resulting leakage that will harm the data secrecy.
   (2) Integrity: It means data will not be altered for the alteration will result in data inaccuracy, that is, data alteration will render the data invalid.
   (3) Authentication: It means data senders will not be able to send data under a false name.
   (4) Non-duplication: It means data content is protected against duplication.
   (5) Non-repudiation: It means the act of sending or receiving data is undeniable by the sender or recipient.

6. Commonly used cryptopattern algorithms are as follows:
   (1) "Symmetric cryptopattern algorithms" refer to Data Encryption Standard (DES), Tripe DES (3DES) and Advanced Encryption Standard (AES).
   (2) "Non-symmetric algorithms" refer to Rivest, Shamir and Adleman Encryption Algorithm (RSA) and Elliptic Curve Cryptography (ECC).
   (3) "Hash algorithm" refers to Secure Hash Algorithm (SHA).
7. "System operations/maintenance personnel" shall mean the operating personnel of e-payment platform who manage or operate the application software, system software, hardware, networks, database, call center, business promotion, account management or accounting operations in the operating environment.
8. "One Time Password" ("OTP") shall mean a password that is valid for only one-time use and generated by a security token, FISC-II card or other devices that use the OTP algorithm.
9. "Mobile device" shall been an equipment with communication and networking capabilities, including but not limited to smart phone and tablet computer.
10. "Sensitive data" include but are not limited to password, personal data, identity data, credit card number, credit card verification code, and personalized data.
11. "Near Field Communication" ("NFC") shall mean using point-to-point communication to enable a mobile device to carry out data transmission with other equipment at close range.
12. "Online To Offline" ("O2O") shall mean an electronic payment institution using mobile device or other portable equipment to provide services at physical channels for its electronic payment business.
13. "Payment via agreed linked deposit account" shall mean the service where in conducting its electronic payment business, an electronic payment institution gives a financial institution at where an user opens his/her account (referred to as "the financial institution holding the account" hereunder) an account payment deduction instruction according to the agreement between the user and the financial institution to transfer funds from the user's deposit account with the financial institution for the electronic payment institution to collect payment from the user and record the payment amount and the fund transfer activity under the user's electronic payment account ("e-payment account"). The mechanisms of the operation are as follows:
   (1) "Direct link mechanism" means the mechanism where an electronic payment institution gives a financial institution holding the account a payment deduction instruction directly to transfer funds from the user's

deposit account.

(2) "Indirect link mechanism" means the mechanism where an electronic payment institution gives a dedicated deposit account bank a payment deduction instruction indirectly through the financial information service enterprise or clearing house to which the bank is connected to transfer funds from the user's deposit account with the bank.

Article 4 When an electronic payment institution accepts user registration, it shall use the following security design for its identity verification process:

1. Verifying mobile phone number: Ensure the user can send and receive messages.
2. Ways to verify that the holder of the financial payment instrument matches with the user of the e-payment account are as follows:
   (1) Verifying the deposit account holder: The institution should check with the bank at where the deposit account is opened or verify the national ID card number or uniform business number of the deposit account holder with the bank; where an individual user does not have a national ID number, the institution should provide another identity document and its number for the bank to verify.
   (2) Verifying credit card holder: The institution should check with the credit card issuer or verify the holder's national ID card number.
3. Verifying the copy of identity document: The institution should obtain a complete and clearly identifiable image of user's identity document by upload or taking a photograph.
4. In-person identity verification: When the institution accepts in-person user registration, it should understand user's motive, verify user's telephone number and address, check identity document with a photo and keep a copy, retain user's seal or signature specimen, enter an agreement on limits of funds received/paid, and pay attention to the surrounding environment while the user opens an account.
5. Identity verification via electronic signature: The institution shall accept signature via certificate authority (CA), authenticate the validity of certificate, and confirm that the identity proven by the certificate matches that of the e-payment account user.

Article 5 An electronic payment institution shall conduct identity verification when a user logs on its e-payment platform; a user may use an account number and a fixed password to log on.

The security design for the account number and fixed password is as follows:

1. If the account number uses only explicit data (such as uniform business number, ID card number, mobile phone number, email address, and credit card number) for identification, a user code should be used for additional identification, which may not use any explicit data mentioned above.
2. The password shall comprise of no less than six characters.
3. The password shall not be identical to the account number or the user code.
4. The password should not be made up of identical alphanumeric characters, continuous English alphabets or numbers, with the exception of default password.
5. The password is recommended to be a combination of alphanumeric characters, and preferably contain upper case and lower case English alphabets or symbols.
6. When wrong password is inputted five consecutive times, access to e-payment platform should be restricted and the user must reapply for the setting of password.
7. Changed password shall not be the same as the previously set password.
8. If the password has not changed for more than one year, the electronic payment institution should take proper actions.
9. If the electronic payment institution issues a default password at the time the user registers, the user shall be required to change the default password when he/she logs in the first time.

Article 6 For different types of transactions, an electronic payment institution shall adopt the following security design based on different transaction limits:

1. For collecting and making payments for real transactions as an agent (including O2O transactions), the institution shall adopt the following transaction security designs based on different transaction limits when the user pays via his/her e-payment account or via the agreed linked deposit account, makes advanced payment request, cancels payment suspension or pays the stored value funds via the agreed linked deposit account:
   (1) Type A transaction security design shall be adopted when the per transaction amount is below an equivalent of NT$5,000, or the daily transaction amount is below an equivalent of NT$20,000, or the monthly transaction amount is below an equivalent of NT$50,000;
   (2) Type B transaction security design shall be adopted when the per transaction amount is at or more than an equivalent of NT$5,000 but less than an equivalent of NT$50,000, or the daily transaction amount is at or more than an equivalent of NT$20,000 but less than an equivalent of NT$100,000, or the monthly transaction amount is at or more than an

equivalent of NT$50,000 but less than an equivalent of NT$200,000; and

(3) Type C transaction security design shall be adopted when the per transaction amount is at or more than an equivalent of NT$50,000, or the daily transaction amount is at or more than an equivalent of NT$100,000, or the monthly transaction amount is at or more than an equivalent of NT$200,000.

2. When the user makes fund transfer between e-payment accounts, the institution shall adopt the following transaction security designs based on different transaction limits:

(1) Type C transaction security design shall be adopted when the per transaction amount is below an equivalent of NT$50,000, or the daily transaction amount is below an equivalent of NT$100,000, or the monthly transaction amount is below an equivalent of NT$200,000; and

(2) Type D transaction security design shall be adopted when the per transaction amount is at or more than an equivalent of NT$50,000, or the daily transaction amount is at or more than an equivalent of NT$100,000, or the monthly transaction amount is at or more than an equivalent of NT$200,000.

The Type D security design in the preceding paragraph may replace Type C security design, Type C security design may replace Type B security design, and Type B security design may replace Type A security design.

Article 7 An electronic payment institution shall carry out identity verification for executing transactions provided in the preceding article, and the security designs for different types of transactions shall comply with the following requirements:

1. Type A transaction security design means the security design that uses fixed password, pattern lock or gesture lock; in the case of fixed password, the security design shall comply with Paragraph 2 of Article 5 herein.
2. Type B transaction security design means the security design that uses OTP sent via short message to user's mobile device with an expiration time for the password set and measures taken to prevent the short message from being stolen or forwarded.
3. Type C transaction security design means any of the following security designs:

(1) For security design that uses FISC-II card, an unpredictable check code of terminal equipment should be dynamically generated for each transaction. For each transaction, the user must input his/her card password to generate a transaction authentication code (TAC) for authentication by the card issuing bank; the security design should also

include the prevention of third-party access.

(2) For security design that uses OTP, a physical equipment which is not for transaction execution should be used. The OTP has an expiration time set, and the device will be locked if wrong password is inputted three consecutive times and unlocked after proper identity verification. If the physical equipment and the equipment for transaction execution are the same equipment, transaction will be executed only after manual confirmation of transaction content at user end.

(3) If two factors authentication is used, the security design should have any two of the components below:

a. Information agreed between the user and the electronic payment institution, which is not known to any third party (e.g. fixed password, pattern lock or gesture lock).

b. A physical device in the possession of user (e.g. password generator, password card, IC card, computer, mobile device, and hardware cryptopattern module): The electronic payment institution should verify that such equipment is the physical equipment held by the user as agreed between the user and the electronic payment institution.

c. Biometric characteristic of the user (e.g. fingerprint, face, eye iris, voice, palm print, vein, and signature): The electronic payment institution should adjust the false acceptance rate of biometric characteristic based on its risk tolerance to effectively identify user identity, and if deemed necessary, increase the types of biometric characteristic for authentication purpose.

4. Type D transaction security design means any of the following security designs:

(1) When accepting in-person user transaction, electronic payment institution should check user's identity document and seal or signature.

(2) Security design that complies with the requirements set forth in the Electronic Signature Act.

When a user uses a physical device in the possession of the user specified in Item (3).b, Subparagraph 3 of the preceding paragraph to engage in transactions and the electronic payment institution uses the security design specified in Item (3) a. or (3)c., Subparagraph 3 of the preceding paragraph as the way to check user's identity when the user logs in the e-payment platform, the user may directly engage in Types A, B and C transactions.

Security design provided in Item (2), Subparagraph 4 of the preceding paragraph that complies with the requirements set forth in the Electronic Signature Act may use the certificate mechanism in compliance with the following

requirements:

1. Comply with the relevant operating rules of the certificate authority (CA);
2. Verify the legality, accuracy, validity, assurance level and use restrictions of the certificate; the certificate must be issued by a third-party certificate authority approved by the competent authority governing certificates;
3. When serving as the certificate registration authority to accept certificate registration or data change from users, the counter operation should add two factors authentication security design or have another staff at the counter to review the registration or change data;
4. For online update of certificate, user must use the existing, valid private key to sign for the certificate update information and send the information to the registration authority to apply for online update;
5. For certificates used in non-repudiation of the transaction, choose a certificate authority that agrees to be held liable and the certificate application allows the user to generate their own private key;
6. Any certificate issued by a government agency shall be used only for identity verification at the time of registration;
7. Each transaction must be signed to confirm the payment content and authenticate the validity of the certificate; and
8. Private keys for the certificate shall be stored in a hardware security module that complies with Common Criteria EAL 4+ (including at least AVA_VLA.4 or AVA_VAN.5), or FIPS 140-1 Level 2 or above, or other modules having the same security strength to prevent the private keys from being exported or duplicated. If the chip hardware and payment instruction generation use the same equipment, the transaction should be confirmed manually by user before it is completed, or two or more additional security features are added in the transaction process.

Article 8 Electronic payment institutions shall ensure that e-payment transactions meet the following security requirements for different types of network:

1. Dedicated network: Message protection measures should have the attributes of integrity, authentication and non-duplication. If transaction security design provided under Item 2, Subparagraph 4, Paragraph 1 of the preceding article is adopted, the protection measures should also meet the non-repudiation requirement.
2. Internet or mobile network: Message protection measures should have the attributes of confidentiality, integrity, authentication and non-duplication. If transaction security design provided under Item 2, Subparagraph 4, Paragraph 1 of the preceding article is adopted, the protection measures should also meet

the non-repudiation requirement.

Article 9 The security design of confidentiality, integrity, authentication, non-duplication, and non-repudiation referred to in the preceding article shall meet the following requirements:

1. Confidentiality: Adopt algorithm at or above 3DES 112bits, AES 128bits, RSA 2048bits, ECC 256bits, or other algorithms with same or greater security strength to undergo encryption.
2. Integrity: Adopt algorithm at or above SHA1, 3DES 112bits, AES 128bits, RSA 2048bits, ECC 256bits, or other algorithms with same or greater security strength for message authentication code (MAC) or encryption.
3. Authentication: Adopt algorithm at or above 3DES 112bits, AES 128bits, RSA 2048bits, ECC 256bits, or other algorithms with same or greater security strength for message authentication code (MAC), encryption or digital signature.
4. Non-duplication: Adopt transaction number or timestamp.
5. Non-repudiation: Adopt algorithm at or above SHA256 or other algorithms with same or greater security strength for message authentication code (MAC), and adopt algorithm at or above RSA 2048bits, ECC 256bits or other algorithms with same or greater security strength for digital signature.

Article 10 The design principle of the e-payment platform shall meet the following requirements:

1. Design requirements for Internet application system:
   (1) The device PIN should not be transmitted over the Internet and sensitive data shall be end-to-end encrypted during transmission over the Internet.
   (2) There should be session control and website session timeout mechanism in place that if the user does not take any action within ten minutes, the system should discontinue the session. However, if the user uses a physical device in the possession of the user specified in Item (3).b, Subparagraph 3, Paragraph 1 of Article 7 to engage in transactions, the timeout may be extended to thirty minutes.
   (3) The system should be able to identify external networks, the sources of transaction data sent therefrom, and the accuracy of transaction data.
   (4) The system should be able to identify the consistency between user input and payment instruction received.
   (5) When the user undergoes identity verification and transaction, the system should use one time random number or timestamp to prevent resend attack.

(6) When the user undergoes identity verification and transaction and it is necessary to use random number function for operation, the system should use secure random number function to generate the random number needed.

(7) When the user changes personal data, or agrees on or changes the bank deposit account which receives withdrawn funds from e-payment account, identity verification must be carried out first in accordance with any transaction security design provided in Subparagraphs 2 to 4, Paragraph 1, Article 7 herein.

(8) The system should be designed with masking function for the display of personal data.

(9) The system should be designed with access control, protective and surveillance measures for personal datafiles and database.

(10) A counterfeit and money laundering detection system should be established with risk analysis modules and indicators set up for instant alert and suitable actions when irregular transaction activities occur. The risk analysis modules and indicators should be examined and revised regularly.

2. Program design requirements for O2O services:

(1) Electronic payment institutions shall confirm the equipment used at physical channels and the confidentiality and integrity of data they send or receive.

(2) When carrying out fund transfer or making payment for real transactions, an electronic payment institution should ask for user confirmation if the payment instruction is recorded on picture, barcode or file. If the aforementioned medium is delivered to others via NFC, bluetooth, scan or upload, the electronic payment institution, if deemed necessary, should add access control (e.g. password) to prevent theft or alteration by others.

3. Design requirements for user-end application:

(1) The electronic payment institution should use digital certificate recognized by the operating system for code signing.

(2) At the time of executing a transaction, the system should first verify the authenticity of website.

(3) The electronic payment institution should avoid storing sensitive data, and if necessary, adopt relevant mechanism, such as encryption or scrambling, safekeep the encryption keys and take effective precautions against data theft.

4. Design requirements for mobile device application:

(1) There should be access control by setting the minimum access authority.

(2) The electronic payment institution should provide the name, version and download site of application for mobile devices on its website.

(3) When the mobile device application is opened, if the system detects that the mobile device could have been hacked, the system should remind the user to beware the risk.

(4) At the time the application is installed or opened, the system should remind the user to install anti-virus software on his/her mobile device.

(5) When the system adopts certificate authority for encrypted data transmission, the mobile device application should establish a list of trusted certificate authorities and authenticate the entire certificate chain and the validity of certificates issued.

(6) Before using NFC to transmit payment transaction data, the transaction should be confirmed manually by user.

5. Design requirements for reconfirmation:

(1) Upon receiving payment instruction from user where the payment will be made via online credit card charge or user's e-payment account or the agreed linked deposit account, the electronic payment institution should notify the payor for reconfirmation in a manner agreed in advance with the user (e.g. transaction confirmation webpage, mail or short message) and proceed with the transaction following reconfirmation.

(2) Where payment is made by other means not provided in the preceding item, it can be perceived as reconfirmation by payor.

Article 10-1 The design principle for payment via the agreed linked deposit account shall meet the following requirements:

1. The electronic payment institution uses direct or indirect link mechanism to provide the service of payment via agreed linked deposit account.

2. The electronic payment institution should apply to a financial institution for a financial certificate and enters an agreement with the financial institution that it will be the exclusive certificate for payment via the agreed linked deposit account operation. The application for agreed linkage or deduction instruction by/from the electronic payment institution should be effected through authentication of signature via certificate authority, and both parties should agree that this certificate authentication mechanism will serve as the undeniability of the transaction. The application for financial certificate shall be made in the following manner:

(1) Direct link mechanism: The electronic payment institution shall apply to the financial institution holding the account.

(2) Indirect link mechanism: The electronic payment institution shall apply

to the dedicated deposited account bank.

3. Agreed linkage procedure:
   (1) The user should apply to the electronic payment institution for account linkage and agree to have the electronic payment institution carry out transfer of funds on user's behalf. The user should apply to user's bank for account linkage in the following manner:
      a. Make application to the financial institution holding the account over-the-counter or through online banking.
      b. Make application to the financial institution holding the account through the electronic payment institution in accordance with the manner set out in the preceding subparagraph.
   (2) When the user applies for account linkage, the user should provide the financial institution holding the account with bank deposit account number, e-payment account number and other agreed information. The agreed linkage is effected after the user's bank has verified the user's identity.
   (3) The electronic payment institution should ask the financial institution holding the account to verify user's identity in accordance with the interface security design for transactions prescribed in the Standards for the Security Management Operation of Electronic Banking Business of Financial Institutions and limit the amount of fund transfer for transactions based on the type of risk applicable to the method used for identity verification.
   (4) When the user uses the payment service via agreed linked account offered by the same electronic payment institution, the aggregate amount of payment shall be limited to NT$300,000 per month.
4. Transaction procedure:
   (1) Direct link mechanism: The electronic payment institution gives the financial institution holding the account a payment deduction instruction according to user's payment instruction, and the institution disburses funds after authenticating the financial certificate agreed with the electronic payment institution and checking the relevant data of agreed linked deposit account.
   (2) Indirect link mechanism: The electronic payment institution gives the financial institution holding the account a payment deduction instruction according to user's payment instruction through the financial information service enterprise or clearing house that the dedicated deposit account bank is connected to. The dedicated deposit account bank will authenticate the financial certificate agreed with the institution, and the

financial institution holding the account will disburse funds after checking the relevant data of agreed linked deposit account and relevant information sent by the financial information service enterprise or clearing house.

5. Private key protection: Private keys for the certificate shall be stored in a hardware security module that complies with Common Criteria EAL 4+ (including at least AVA_VLA.4 or AVA_VAN.5), or FIPS 140-1 Level 2 or above, or other modules having the same security strength, and the key export function should be limited.
6. Access control: The electronic payment institution should establish control mechanism to restrict access to private keys and programs relating to agreed linked deposit account operation by unauthorized personnel or programs.
7. Notification mechanism: The electronic payment institution should ask the financial institution holding the account to establish a notification mechanism, by which, the institution will notify the user instantly after making fund transfer.
8. Risk control: The electronic payment institution should ask the dedicated deposit account bank or the financial institution holding the account to establish reasonable transaction flow control mechanism.
9. Application for termination of agreed linkage:
   (1) The user should apply for termination of agreed linkage in a manner provided under Item 3 (1) hereof or other manners agreed with the electronic payment institution or the financial institution holding the account.
   (2) The financial institution holding the account should notify the electronic payment institution when a user directly applies to it for termination of agreed linkage.
10. Simplified rules for institutions engaging concurrently in electronic payment business:
   (1) When the user's bank is an institution engaging concurrently in electronic payment business or Chunghwa Post Co., Ltd., the financial institution holding the account may verify user's identity and complete the agreed linkage and transaction procedures in accordance with these Regulations without being subject to the provisions of Subparagraphs 2 ~ 4 hereof.
   (2) For institutions engaging concurrently in electronic payment business or Chunghwa Post Co., Ltd. that are not the user's bank and adopt indirect link mechanism, the provisions of Item (2) of Subparagraph 2, Item (1).b of Subparagraph 3 and Item (2) of Subparagraph 4 hereof on agreement with the dedicated deposit account bank and authentication of financial

certificate do not apply.

Article 11 The information security policy, internal organization and asset management of an electronic payment institution shall meet the following requirements:

1. The information security policy should be adopted by resolution of the board of directors, the board of managing directors, or approved by managerial officer authorized by the board. For branches of foreign banks in Taiwan, the information security policy shall be signed off by their responsible officer.
2. The information security policy mentioned in the preceding subparagraph shall be published and conveyed to all employees and external stakeholders.
3. The electronic payment institution should establish information operation related managements and operating rules.
4. The information security policy mentioned in Subparagraph 1 hereof and management and operating rules mentioned in the preceding subparagraph shall be reviewed and revised every year, and examined when there are material changes (e.g. newly promulgated law or regulations) to ensure their ongoing suitability, adequacy and effectiveness.
5. The electronic payment institution should, in accordance with the operating procedure of e-payment platform, identify assets, including personnel, forms, equipment, software and systems, and establish a list of assets, operating procedures, network architecture, organizational chart and responsible persons, and take inventory periodically to maintain their accuracy.
6. The electronic payment institution should define the roles and responsibilities of personnel and segregate conflicting roles.
7. The electronic payment institution should, based on operational risk and professional capability, select suitable personnel to serve in their positions and provide them with necessary training regularly.

Article 12 The management of e-payment platform's system operations/maintenance personnel shall meet the following requirements:

1. The electronic payment institution should establish personnel registration, change and registration cancellation procedures for allocating proper access authority.
2. The electronic payment institution should examine the reasonableness of the accounts and access authority of operating personnel at least annually and swiftly remove the access authority of personnel who have departed or are transferred to another job to conform to the principles of segregation of duties and internal check.
3. Personnel accounts with highest access authority to hardware equipment,

application software and system software and accounts that have the authority to change program or parameters should be safekept with a list established; When accounts with highest access authority are used, the consent of the responsible executive must first be obtained and the audit trail shall be retained.

4. The electronic payment institution should confirm the identity and access authority of operating personnel, and where necessary, limit the machines and internet protocol (IP) they may use.
5. Where a personnel's computer stays idle for more than ten minutes, display of user's personal data on the screen should be restricted.
6. When an employee logs in the operating system to make system changes or access the database, related manual operational record should be saved and the password should be changed as soon as possible after use. Where the password cannot be changed for some reason, the electronic payment processing institution should establish monitoring mechanism to avoid unauthorized change and double check the operating record afterwards.
7. Employee accounts should be managed by one account per person in principle to avoid one account being shared by multiple persons. If it is necessary to establish a common account, other enhanced control measures should be in place with respect to account application and use with operating records saved and the identity of operators distinguished.
8. Where fixed password is used, the password should be changed periodically in accordance with Paragraph 2 of Article 5 herein; the password for accounts provided for use by personnel shall be changed at least once every three months; the password for accounts provided for system connection shall be changed at least once every three months or controlled by other enhanced methods (e.g. restrict manual login).
9. Encryption/decryption programs or utility programs with change authority established (e.g. database access program) should be managed with a list established and use restricted. The program should also have access authority set to prevent unauthorized access and have the audit trail retained.

Article 13 The personal data protection in e-payment operating environment shall meet the following requirements:

1. To uphold the security of personal data in possession, the electronic payment institution should adopt the following data security management measures:
   (1) Establish rules for the use of various equipment or storage media and proper measures for preventing data leak when such equipment or storage medium is scrapped or used for other purposes;

(2) For personal data in possession that need to be encrypted, adopt proper encryption measures at the time of data gathering, processing or use; and

(3) When it is necessary to make backup copy of personal data, implement proper protection for the backup data.

2. When personal data in possession are stored on papers, in magnetic disks, magnetic tapes, optical disks, microfilms, integrated circuits, computers, automated machines or other media, the electronic payment institution should adopt the following equipment security management measures:

(1) Implement appropriate access control;

(2) Draw up media safekeeping methods; and

(3) Establish proper protective equipment or technology based on the characteristics of media and related environment.

3. To uphold the security of personal data in possession, the electronic payment institution should, based on the needs of business conducted, set up access authority of personnel having access to personal data and control the access, and enter an agreement on confidentiality obligation with those personnel.

4. The electronic payment institution should take inventory of e-payment operating environment, including database, datafiles, forms and statements, documents, FTP servers and personal computers to see if they contain personal data and compile a list therefor, and carry out risk assessment and control.

5. The electronic payment institution should generate and save the audit trail (e.g. account login, system functions, time, system name, query command or results) or identification mechanism for personal data use to facilitate the tracking of personal data use situations, including files, screen images and lists when there is a personal data leak.

6. The electronic payment institution should establish data leak protection mechanism to control the transmission of personal data files via input/output device, communication software, system operations copied to webpage or network file or printing, and retain relevant records, trails and digital evidences.

7. The following records shall be retained if personal data in possession are deleted, or stopped processing or use:

(1) The method and time for deletion, or stop of processing or use.

(2) Where the personal data being deleted, stopped processing or use are transferred to other entities, the transferee, reason, method, and time of transfer and legal basis for the transferee to gather, process or use such data.

8. To continuously improve the maintenance of personal data security, the

personal data management unit or personnel of the electronic payment institution should produce related self-evaluation reports regularly and set up the following mechanisms:

(1) Inspecting and revising relevant personal data protection matters; and

(2) Planning and carrying out corrective and preventive actions if the self-evaluation report indicates possible regulatory violation.

9. The self-evaluation report provided in the preceding subparagraph shall be adopted by resolution of the board of directors , the board of managing directors or approved by managerial officer authorized by the board. For branches of foreign banks in Taiwan or electronic payment processing institutions without a board of directors, the self-evaluation report shall be signed off by their responsible officer.

Article 14 The confidentiality of e-payment platform's sensitive data and key management shall meet the following requirements:

1. A data confidentiality mechanism should be established in any of the following situations:
   (1) Sensitive data are stored in users' operating environment.
   (2) Sensitive data are transferred on Internet.
   (3) Users' identity verification data (e.g. password, personalized data) are stored in the system.
2. Where a fixed password is used for user identity verification, undergo non-invertible algorithm (e.g. hash algorithm) before storing such data. In addition, to prevent password cracking using pre-generated hash value, encrypt users' passwords or add inaccessible data computing. If encryption algorithm is used, the keys should be stored in the hardware security module with export function restricted.
3. Use hardware security module to protect the keys, which should be separately generated by two or more units other than the system development and maintenance unit (e.g. customer service, accounting, business administration) with the list of clear-text keys under dual control. In addition, the keys under dual control may be encrypted and exported to a secure device (e.g. IC card) or copied to a location under access control for emergency use by the maintenance unit.
4. Keep the locations of key storage at the minimum and allow only necessary administrators to access the keys to facilitate management and reduce the possibility of key leakage.
5. Replace the key when the duration of key is about to expire or when there is leakage concern.

Article 15 The physical security of e-payment platform shall meet the following requirements:

1. The computer facilities and the disaster recovery site should avoid being simultaneously situated on fault zone, coastlines, slopes, below sea level, underneath airport flight paths, landslide-prone areas, 100 year flood zones, nuclear emergency alert areas, or high-risk areas in the workplace, and there should be protective measures in place to prevent damages to the computer facilities and disaster recovery site in case of earthquake, tsunami, flood, fire or other natural or manmade disasters.
2. Operating equipment should be centrally located in the computer facilities with access control established to ensure that only authorized personnel are allowed to enter and exit the room. The entries and exits of non-authorized personnel should be logged and under the accompaniment and supervision of internal personnel. The entry/exit records should be examined regularly with proper actions taken if any abnormality is found.
3. The computer facilities and the disaster recovery site should have 24-hour monitoring equipment set up that does not have monitoring dead angles.
4. There should be measures that ensure sufficient supplies of electricity, water and oils for operations that when the supply is interrupted, the operations may be maintained for at least 72 hours. The system should also be connected with at least two telecom service providers that provide Internet service or two offsite lines for backup.
5. Oil sump storage and fire safety shall meet the relevant regulatory requirements.
6. There should be environment monitoring and control mechanism in place for the management of telecommunication, air conditioning, power, fire safety, access control, surveillance and temperature and humidity of the computer facilities that also sends out warning and notice automatically.
7. The control room for management of the computer facilities should have an operating environment comparable to the computer facilities or be equipped with independently control personnel operating the systems and equipment.

The control room mentioned in Subparagraph 7 of the preceding paragraph shall meet the following requirements:

1. The control room should have access control and be equipped with monitoring equipment with connection and usage logs retained and audit carried out regularly.
2. Only authorized system operations/maintenance personnel should be allowed to enter the control room to use the computer equipment inside; or system

operations/maintenance personnel may log in the computer equipment inside the control room using a one-time password through a designated equipment, the intranet and secure configuration for service control (e.g. firewall).

3. The connection process should be carried out through an intranet, a leased line or a virtual private network.
4. Where the network equipment and computer equipment in the control room constitute a part of the e-payment operating environment, those equipments shall comply with relevant provisions of these Regulations.

Article 16 The operations management of e-payment operating environment shall meet the following requirements:

1. Avoid installing source codes of applications in the operating environment.
2. Establish a regular backup mechanism and a backup list, and safeguard the backup media or files to ensure data availability and prevent unauthorized access.
3. Establish a mechanism for the testing of backup media to verify the integrity of backup and the suitability of storage environment.
4. Ensure to follow the established procedures for collection, protection and management of digital evidences, and relevant records shall be retained for at least 2 years.
5. Draft system security enhancement standards, and establish and implement security configuration measures for e-payment operating environment.

Article 17 The vulnerability management of e-payment operating environment shall meet the following requirements:

1. Detect changes to webpage and application, record the changes and inform relevant personnel to handle the situation.
2. Detect the linkage of malicious networks and periodically update the list of malicious networks.
3. Establish intrusion detection or intrusion prevention mechanism and periodically update malware behavioral features.
4. Establish virus detection mechanism and periodically update virus definitions.
5. Establish online control measures and restrict connection to non-business related websites to prevent the download of malware.
6. Grasp readily information security incidents by promptly undertaking investigation of high-risk or important items and taking response actions.
7. Conduct regularly social engineering email drill and training for system operations/maintenance personnel at least once a year.
8. Carry out vulnerability scan every quarter and undertake risk evaluation

based on the scan or testing results, draw up proper measures and set completion time for different risks, write up a report on evaluation results and actions taken, adopt proper measures and ensure that all operating systems and software applications are installed with tested security patches that are free of vulnerability concern.

9. Avoid using system software and application software that have stopped vulnerability patches or update, and if necessary, take necessary safeguard measures.
10. Carry out program code scan or black box testing before the e-payment platform goes online and for changed programs every half a year, and undertake risk evaluation based on the scan or test results, draw up proper measures and set completion time for different risks, conduct corrective actions, record handling situation and follow up on improvements.
11. The e-payment platform should have penetration testing conducted every year to enhance information security.

Article 18 The network management of e-payment operating environment shall meet the following requirement:

1. Networks should be zoned into Internet, demilitarized zone ("DMZ"), operating environment and other zones (e.g. internal office area), and use firewalls to establish access control between the zones. Sensitive data shall be stored in secure network zones only, which do not include Internet and DMZ. Internet services for outside parties can only be carried out through DMZ, and from DMZ to other network zones.
2. The connection between e-payment operating environment and other networks shall be put under control via firewall or router.
3. The system should open only necessary services and programs, whereas users can only access authorized networks and network services. Information on intranet and internal network framework shall not be externally disclosed without authorization.
4. Inspect firewalls and the setting of network equipment with access control list (ACL) at least once every year. For high-risk settings and firewall rules without traffic for six months, evaluate their necessity and associated risks; for offline systems, immediately stop the use of firewall rules.
5. When carrying out system management operations via remote connection, use encrypted communication protocol of sufficient strength, and do not save the passwords in the utility software.
6. Control the usage of internal wireless network, do not allow connection from the internal wireless network to the e-payment operating environment, and

adopt necessary protective measures for segregation.

7. Connection to internal network via the Internet to carry out remote system management works shall comply with the following rules:
   (1) Review the purpose of applications for remote use, durations, time segments, network segments, equipment used, destination equipment or services at least once a year.
   (2) Establish an authorization mechanism to make necessary authorization based on the application, and examine the authorization mechanism at least once a year.
   (3) Strengthen identity authentication for any change operations and adopt exchange of notes or two factors authentication security design and obtain superior's authorization for each login.
   (4) Define connectable remote equipment and ensure that necessary information security systems have been installed.
   (5) Establish monitoring mechanism and retain operating records for periodic review by the superiors.

Article 19 The system lifecycle management of e-payment operating environment shall meet the following requirements:

1. Draw up and implement information security development and design specifications.
2. For outsourced development of application software, implement supervision and ensure that the outsourced service providers effectively observe these Regulations.
3. Make sure system software and application software have installed the latest security patches.
4. For sensitive data used in testing, undergo data masking or control protection first.
5. From development stage to operational stage, handle changes in accordance with the established change control procedure and retained relevant records; changes to the operating environment (e.g. execution, review) shall be carried out by at least 2 persons for internal check.
6. For modification of system software, first undergo technical review and testing; do not attempt to modify software packages at own discretion and carry out risk evaluation first. Program version change or production of comparison report should not be at the discretion of development personnel; source code management should be established to conform to the principles of segregation of duties and internal check.

Article 20 The outsourcing management of e-payment operating environment shall meet the following requirements:

1. Before outsourcing, carry out proper security assessment of prospective service provider and undertake security control design based on the principles of least privilege and minimum disclosure.
2. The outsourcing contract or relevant documents should explicitly agree on the following particulars:
   (1) The outsourced service provider shall observe these Regulations and other suitable international standards and requirements for information security to ensure the security of data furnished by client.
   (2) Undertake proper supervision of the outsourced service provider in accordance with the provisions of these Regulations.
   (3) When the security of outsourced operation is breached, the outsourced service provider should take the initiative to promptly inform the client.
   (4) The outsourced service provider shall ensure that the system or program it delivers does not contain malware or backdoor, and any program placed over the Internet shall have passed the program code scan or black box testing.
3. Conduct information security audit of the outsourced service provider or ask the outsourced service provider to provide information security audit report at least once a year.

Article 21 The information security incident management of e-payment operating environment shall meet the following requirements:

1. Place logs and audit trails of operating systems, network equipment and information security equipment under central management, conduct abnormality analysis, set proper alarm indicators and review the indicators regularly.
2. Establish mechanisms for reporting and handling of information security incidents, responses and post-incident follow-up and improvement, and retain records on relevant operations.
3. In case of an information security incident, take proper care of the system transaction logs, system logs, and security incident logs, and heed the effectiveness of log records and retained evidences obtained in the handling process.

Article 22 The business continuity management of e-payment operating environment shall meet the following requirements:

1. Carry out business impact analysis, define maximum tolerable downtime, set

system recovery time objective and data recovery point objective, deploy necessary redundancy, and take into consideration that if the time for system recovery is restricted, set up offsite backup system at a safe distance to maintain service availability.

2. Establish response procedure for major information system incident or natural disaster and confirm corresponding resources to ensure that the impact of a major disaster on important business activities is within reasonable range.
3. Validate and conduct drill of business continuity control measures to ensure their effectiveness and retain related drill records and hold review meetings therefor.

Article 23 An electronic payment institution should take inventory of rules and regulations applicable to information security, incorporate relevant information security requirements into its internal control systems, and undertake self-evaluation of regulatory compliance regularly to ensure compliance with information security regulations.

An electronic payment institution should conduct periodic check of its information systems and security control items set out in these Regulations through its internal control systems, and shall appoint an accountant to examine and produce an information system and security control operation evaluation report when it applies for approval pursuant to Article 10 of the Act and before the end of April every year thereafter.

The evaluation report in the preceding paragraph shall contain at least the qualifications of the evaluator, scope of evaluation, deficiencies found in evaluation, severity of deficiency, type of deficiency, description of associated risks, concrete improvement suggestions and social engineering drill results. The evaluation should also be given to the internal audit unit for follow-up of improvement actions taken. The aforementioned report and documents on improvement of deficiencies shall be retained for at least 2 years.

To ensure the privacy and security of transaction data and to ensure that the accuracy of data transfer, exchange or processing is maintained, the competent authority may, if deemed necessary, require an electronic payment institution to raise the standards for its information system and step up its security management operations.

Article 24 These Regulations shall be in force on May 3, 2015.

The amended provisions of these Regulations shall be in force on the date of promulgation.