Appendix 1

Protection Plan of Critical Telecommunications Infrastructure of _____ (Company Name) (a reference format)

1、 Accordance

2、 Prospects and Objectives

(1) Security Protection Prospects

(Specifies instructions of the management team and supports the security protection prospects of telecommunications equipment room or internet data center in accordance with operating needs, relevant laws and regulations.)

(2) Security Protection Objectives

(A series of security protection policies for the telecommunications equipment room or internet data center shall be specified, approved by the management team, released and forwarded to staff and relevant external groups.)

3、 Organization of Manpower and Protection

(Clearly and definitely establishes an organizational framework that conducts and manages security protection and operations of telecommunications equipment room or internet data center.)

(1) Organization of Manpower

(Specifies the organization's structure, work force system, duties and security protection responsibilities.)

(2) Organization of Protection

(Duty and responsibility domains that are in conflict with each other shall be separated during organization protection in order to minimize possible unauthorized or unintentional amendment to or misuse of the organization's assets.)

4、 Asset Management

(Identifies the organization's assets and specify appropriate protection responsibilities; ensures the assets are appropriately protected according to their importance to the organization; and prevents assets being disclosed, removed or damaged with unauthorized actions.)

(1) System and Network Framework

(Framework diagram and descriptions; outbound routes; and spatial configuration diagram.)

(2) Equipment Inventory

(Lists equipment in the telecommunications equipment room / internet data center: name, quantity, capacity, function, location and applicable business of the equipment.)

5、 Risk Assessment

(Specifies and sets the schedule of regular risk assessment or re-assessment required when a significant change occurs to ensure the applicability, adequacy and validity.)

(1) Risk Identification

(Clearly identifies all assets, lists important assets, and ensures the list is well-maintained; prior to carrying out the identification work, information related to invalidity of telecommunications equipment and network congestion caused by disasters, accidents and social phenomena shall be collected and evaluated on a regular basis and key data shall be summarized accordingly.)

(2) Risk Estimation

(3) Risk Assessment

(Evaluates all types of direct and indirect risks that may be caused by natural disasters, terrorist attacks and network attacks; analyzes the vulnerability of the telecommunications equipment room / internet data center under threat of all types of damages.)

(4) Risk Handling

6、 Physical and Environmental Protection

(The ultimate aims of protection plan are to prevent facilities in telecommunications equipment room / internet data center being accessed, damaged or interrupted by an unauthorized action; to avoid assets being missed, damaged, stolen or deciphered; and to guard against interruptions of relevant operations.)

(1) Security Boundary

(Sets asset management rules and physical/environmental security guidance; security boundary shall be defined and adopted in order to guard the region where sensitive or important information and information processing facilities are installed.)

(2) Access Management

(Defines and applies access measures for the telecommunications equipment room / internet data center; appropriate access control measures shall be adopted to protect the safety zone. That is, only authorized people are allowed to enter / exit the space. In addition, plans regarding the physical security and safety of offices, rooms and facilities shall be conducted and implemented.)

(3) Safety and Security Measures for the Environment

(Stipulates fire fighting, water supply, electricity supply, seismic resistance, and air-conditioning safety and security measures. Measures concerning external and environmental threats are also required to be clearly established. For example, policies regarding the necessity of working in safety zone; receiving / delivering / loading / uploading zone; equipment installation and protection; supporting equipment; safety and security of cable works; equipment maintenance; removing assets; safety and security of equipment outside the telecommunications equipment room / internet data center; elimination of equipment or reuse of safe and available user equipment; and cleaning.

(4) Human Resource Security Management

(Defines the role and responsibility of employees, subcontractors and third parties, and the safety / security / management rules that they comply with. For example, the access, development and maintenance of information systems; policies for mobile equipment; remote working; management before and during the employment; termination and amendment to the employment; management of users' responsibilities; information security management of suppliers relations; supplier service delivery management; and reporting information security and weakness shall all be included.)

7、 Network Maintenance and Operations Management

(1) Operating Mechanism

(All operating procedures and activities of the equipment of telecommunications equipment room / internet data center shall be documented and maintained appropriately. Measures for security management shall be clearly established in regard to the organization's information, including telecommunications and operations management; access control; acquisition, development and maintenance of information systems; operating requirements for access control; user access management; access control for system and application system; password control measures; operating procedures and responsibilities; prevention against malware; system back up, records and monitoring; control of operating software; technology vulnerability management; information system audits; network safety management, information transfer and exchange; security requirements for information system; security during the development and support process; and testing data.)

(2) Dependency

(Specifies the importance of serving target; and sets the priority of rescuing targets should a disaster occur.)

(3) Back Up Mechanism

(A system network and electricity back up system, including the access, development and maintenance of information system, continuity of information security, and multiple configurations)

8、 Rescue Planning and Report / Response Operations

(Maintains contact with competent authorities, agencies, groups of special interests, and professional forums and associations related to the information and knowledge of security / safety.)

(1) Planning of Rescue Resources

(Internal resources: human resource allocation and contact methods; external resources: Fire fighting, security guard and medical support planning.)

(2) Report and Response Operations

(Prior to disaster major incident/ disaster: equipment preparation, detection and prevention; during the disaster: response and handling measures for providing status reports, compiling relevant information and maintaining effective communication; after the disaster: conduct restoration plans and reviews, set

management measures for information security incidents, and propose improvement measures.)

9、 Security Protection Trainings, Drills and Reviews

(1) Security Protection Trainings

(Educates employees and familiarizes them with reporting and handling procedures for disaster and information security incidents.)

(2) Security Protection Drills and Incident review

(Sets the drill plan and conducts regular drills; holds post-disaster management meetings, in which the effectiveness is evaluated from relevant experiences and information security incidents are reviewed in order to undertake improvements; and evaluate information security incidents to determine whether they will be classified as information security accidents.)

Remarks: please refer to regulations of CNS27001 and CNS27011 when completing the Critical Telecommunications Infrastructure Protection Plan.