Rules of Protecting System Security

1. General Rules

The Rules of Protecting System Security (the “**Rules**”) are basic procedure and measures made by EPEC E-commerce Co., Ltd. (the “**Platform Operator**”), the operator of EPEC International E-commerce platform (the “Platform”), in accordance with relevant laws and regulations and SINOPEC regulations about security of information management, which are designed to protect security of the Platform system.

2. Basic Requirements

2.1 Measures protecting website security

The Platform Operator will adopt technical measures and other necessary measures to ensure secured and stable operation of the network, prevent cybercrime activities, deal with cyber security incidents effectively, and ensure the security of e-commerce transactions. The Platform Operator will formulate cyber security incident emergency plans, implement the emergency plans immediately upon the occurrence of cyber security incidents, adopt the corresponding remedial measures, and report to the relevant competent authorities.

2.1.1 Website deployment

To better prevent threat against Internet security, the Platform exit adopts the structure with heterogeneous firewall hierarchy defense. The platform system adopts the principle of “vertical hierarchy and horizontal zoning”. The vertical hierarchy means that, as the Internet exit, external DMZ and internal DMZ goes deeper into the internal network, it provides enhanced ability of security protection. The horizontal zoning means making targeted configuration security tactics according to their respective abilities for different types of application in the same vertical zone. The system uses internal IP address and provides service for Internet by setting IP address change on the exit equipment.

The system adopts structural designs such as application release, content management and database separating functional modules while deploying different functional modules in corresponding security zones. The functional modules, in the vertical direction, are mainly deployed in external and internal DMZ zones. Based on the system characteristics, deploy User Visiting Web Service on external DMZ zone in horizontal direction. The internal DMZ zone includes Content Management Zone and Data Zone.

2.1.1.1 Deploy application release module

The application release module lies at the forefront of the system and receives visits made by Internet users or applications. The security protection of application release module focuses on identifying and preventing the attacks from Internet to ensure usability of the system and preventing contents from being manipulated and ensuring its completeness; the release module of applications is deployed in external DMZ zone.

2.1.1.2 Deploy service treatment module

The service treatment module is deployed in the Content Management Zone of internal DMZ, and is used to manage contents released by the management system to realize uniform management of content uploading, editing and verification. The security protection of service treatment module focuses on controlling the process of external release, verification of the identity of issuing people, and authenticity and effectiveness of released contents.

2.1.1.3 Deploy the system data module

The system data module is deployed in the system data zone in internal DMZ zone. The system data module provides backstage support for service contents in the application system, or provides data interaction via special service port. Security protection of system data module focuses on its own performance optimization, identity verification, operation auditing, counter-manipulation or security programming, etc.

2.1.2 Website protection

2.1.2.1 Border control

By deploying firewall system on the border of system’s security zone control visit to the system; the border visit control equipment defaults the refusal control tactics and only allows the passage of explicitly allowed data flow; the system realizes the visit control based on the connection state and prevents the active connection from low safety zone to high safety zone; the border visit control equipment makes the control visit in the region as accurate as the port level; the border visit control can automatically cut the 5-minute dialogue in the non-active time; according to needs, it can cut the established dialogues through the website border equipment.

2.1.2.2 Intrusion detection

The system deploys the intrusion protection system based on website or host machine to realize detection and protection of website attacks; the intrusion protection system can record the source IP, target IP, type and time of website attacks; the intrusion system can provide real-time alert against website intrusion and cut attacks according to tactics; the intrusion protection system can, on a regular basis, updates the feature library of intrusion protection equipment, thus realizing identification and prevention of new intrusions; the intrusion protection system can produce statistical and analytical report, which is used as the auditing basis and decision-making foundation for intrusions.

2.1.3 Security of service system

The security of Platform system focuses on protecting the security of all components in the application system, including the security configurations software, middleware, databank and operating system and the system's special needs for security protection.

2.1.3.1 Service configuration

Based on the principle of minimal installation, only install the functional units that support normal operation of system; do not use the unnecessary system service to prevent against security threat and occupation of resources that might be caused by such services; control the boot startup and only load necessary services based on needs; make security configuration of system service that needs to make external interactions, such as identity verification and encryption, etc. to prevent from misuse of system resources and information leakage.

2.1.3.2 Account password

Allocate accounts according to real needs to prevent from many sharing one account; delete or disable invalid account while modifying the default password for default account that needs to be maintained; the account password should contain at least eight in at least two kinds of the letters, numbers or special character; alter the account password every 90 days.

2.1.3.3 Login Management

Adopt the account locking tactics for 30 minutes for accounts with more than five failed log-in attempts; do not manage the system on a remote basis unless necessary; use safe telecom protocol to make remote management of the system; limit the scope of IP addresses that can make remote system management and the system accounts that can be used for remote management; force the account in login state but having no operation in ten minutes out of the login or lock the login page.

2.1.3.4 Authority allocation

Allocate authority to different accounts of operators and administrators; allocate the minimum needed authority, according to needs, to administration account and service account; set up the authority of visiting and using the key directory, document and program in the system.

2.1.3.5 Log auditing

Through auditing system, the system audits itself, including auditing and monitoring of the important operations of the user on the system and the operating state of the system; the auditing records the date, time, type, subject logo, object logo and outcome of the incident; the auditing system can effectively protect the auditing results, and prevent the unexpected visit, modification or deletion; the system can produce auditing log through the standard protocol.

2.1.3.6 Protection against loopholes

According to needs, the system installs the necessary system patches, makes installation tests before installing the patches, and verifies the operating state of applications carried on the system after the installation; make regular loophole scanning and the scanning report can classify, grade and make statistics about the loophole information that can be identified, point out the possible risks and propose how to improve them; identify the outcomes according to loopholes and repair system loopholes according to security tactics; after the loopholes are mended, scan again the system for confirmation until all unaccepted loopholes are mended.

2.1.3.7 Protection against virus

Deploy virus prevention equipment at the entry into Internet to effectively protect the malicious code from the Internet; deploy the virus prevention system of different manufacturers in host layer and website layer to improve the comprehensive protection ability; upgrade the virus bank on a timely basis and update the version of virus prevention system according to needs; use the malicious code to monitor on the real-time basis while regularly searching and killing virus so as to protect the security of the system.

2.1.3.8 Code security

The system provides effective protection of the authenticity and completeness of the dynamic and static web pages to prevent illegal manipulation. The backstage database uses the parameter enquiry to strictly define role and authority of the database users; the system makes strict legitimacy judgments of all forms, tables and parameters submitted by the Users and filters the illegal characters to prevent the attackers from conducting SQL statement injection, cross-site scripting, XML injection, HTTP Head injection and other injection attacks; the system must at first test the length of data input by Users to prevent the buffer zone premium loophole caused by excessive, allocate memory to judge the return values. The memory operations, in particular the memory copy, must check whether the length exceeds the allocated memory to prevent the memory stack from overflowing the loophole. The system does not recall the external order treatment program. It should verify the recall data and verify if the input data are legal when it is necessary to recall external treatment programs so as to prevent the external program recall loophole;

In source code development, it is necessary to follow the regulations of security development and prevent the malicious-structured catalog and file name loophole and other common loopholes.

2.1.3.9 Data security

The system makes encryption treatment of key data in storage and transmission process with the encryption calculation and password strength complying with relevant requirements; see system storage and backup rules in Rules of Storage and Backup.

2.2 Operation maintenance

2.2.1 It is imperative to make security check plan and program for system maintenance to make regular security review of the system while making security rectification according to the review result.

2.2.2 In special period or incident, make security check and rectification of the system to ensure the system is operated in a secure and stable way. When major alterations happen, make security check and rectifications to ensure the constant consistency of the security protection;

2.2.3 The security check should be made in accordance with security configuration baseline, loophole identification and compliance. Results of regular and irregular check should be reused according to relevance such as check contents and date;

2.2.4 Monitor the operating state and security state of the application system. Monitoring of operating state includes the application system’s usability and operating load; monitoring of security protection includes website attack, visit control, operation auditing and virus protection, etc.

2.2.5 Make alert, analysis and statistics of the operating state of the application system and information security incidents.

3. Supplementary Provisions

3.1 The Rules shall be effective from January 1, 2019.

3.2 The Rules shall be interpreted by the Platform Operator.

3.3 The Platform Operator reserves the right to amend the Rules or formulate the supplementary rules and publicize the amended rules or the supplementary rules from time to time based on the operation needs. The amended rules or relevant supplementary rules will be effective on the designated date in the public announcement. The Rules shall be legally binding on all relevant parties on the Platform from the effective date.