Information Security Policy

1 Objectives

This policy is duly enacted for the purpose of ensuring the confidentiality, integrity and availability of the information assets belonging to the Zyxel Group to comply with the requirements of relevant laws and regulations, in turn, protect the Group from internal or external threats, either deliberate or accidental ones.

2 Scope

The scope of the information security management covers a total of 13 managerial items to prevent potential man-made fault, willful or natural calamity and such factors to prevent potential results in misuse, divulgence, manipulation, destruction. Bring the subsequent potential risk and hazards to the organization. The issues of management are as enumerated below:

2.1 Enactment and evaluation of the information security policy.

2.2 Information security organization.

2.3 Classification and control over information assets.

2.4 Personnel management and educational and training programs.

2.5 Substance and environmental safety and security.

2.6 Management over communications and operation safety and security.

2.7 Safety and security in access control.

2.8 Safety and security in system development and maintenance.

2.9 Response and settlement of information security events.

2.10 Management over business operation continuity.

2.11 Consistency in laws and ordinances concerned and policies in the unit of execution.

2.12 Project management information security.

2.13 Supplier management.

3 Targets

Efforts to maintain confidentiality, integrity and usability of the Group's information assets and to safeguard the privacy of the user's information. The following targets shall be accomplished through the teamwork by the entire staff:

3.1 The effort to protect the information of business operation in the Group to prevent potential unauthorized access.

3.2 The effort to protect the information of business operation in the Group to prevent potential unauthorized amendment so as to assure accuracy and integrity.

3.3 The effort to set up the plan to assure continued business operation to assure sound and continued business operation of the Group.

3.4 The execution of the Group’s business operation should be consistent with laws and ordinances concerned or requirements by law.

4 Declaration

The effort to assure sound information security management and provide safe and reliable services.

5 Responsibility

5.1 The Group’s management should set up and review the present policy.

5.2 The information security management shall enforce such Policy through appropriate standards and procedures.

5.3 The entire staff and outsourced firms shall faithfully maintain the information security policy in accordance with the relevant safety and security management procedures.

5.4 All personnel shall assume the responsibility to report information security related events and already identified vulnerability.

5.5 On any act endangering the information security, the Group shall, as the actual situations may justify, investigate into the civil, criminal and administrative responsibilities or impose penalty in accordance with the relevant provisions of the Group.

6 Educational and training programs

The entire staff shall accept and complete the information security related educational and training programs or publicity in each and every year. All personnel within the applicable scope of the present system shall possess relevant skills to as to upgrade information security awareness, concept and capability of protection to, in turn, minimize the loopholes of information security so incurred by human factors.

7 Document record and management

All the System related documents shall be promulgated into enforcement after a representative review process.

On method of control over the System related document s and records, appropriate methods for access and custody shall be duly enacted.

8 Internal audit

To check and make sure the faithful implementation and appropriateness of the information security specifications, the Group shall conduct one internal audit of information security as the minimum per annum so as to continued improvement of the present system.

9 Review by the management echelon.

The Group shall conduct at least one managerial review every year to check and make sure the necessity to update the policy so as to accurately reflect the very update of the government laws, know-how and business operation and, meanwhile, check and make sure of all sorts of business operation in the aspect of information security to assure sound appropriateness, usability and validity of the System in the continued operation so as to, in turn, assure the Group's sustainable business operation.

10 Information management and risk management

The Group shall conduct at least one inventory check and risk evaluation of the information assets every year and shall, exactly based on the result of risk evaluation, map out distribution of resources in the aspect of risks with consideration of law compliance so as to launch risk management and improvement in real time.

11 Policy measures

The control measures to be adopted to accomplish the very targets of the policy, e.g., the applicable items amidst the "Declaration on Applicability".

12 Enforcement

12.1 Management over the information security policy with coordination of the review meeting and verification of the information security policy.

12.2 This Policy is to be put into enforcement after being approved by the information Security head. This same provision is applicable mutatis mutandis to an event of amendment.