Information Security Policy

1 Purpose
Universal University of Science and Technology (hereinafter referred to as the University) belongs to the confidentiality, integrity and availability of information assets and comply with the requirements of the relevant laws and regulations, harmless from any suffered external, deliberate or accidental threat.
2 Scope
Information Security Management covers 11 management matters, to avoid due to human error, deliberate or natural disasters and other factors, leading to improper use, the information leakage, tampering, destruction, and other violations occur, to bring all possible risks and hazards on the school. Management issues are as follows:
2.1 Information security policy setting and evaluation.
2.2 Information security organizations.
2.3 Information asset classification and control.
2.4 the safety of personnel management and training.
2.5 physical and environmental safety.
2.6 Communication and Safety Management.
2.7 access control security.
2.8 System development and maintenance of security.
2.9 Information security incident response and handling.
2.10 business continuity operations management.
2.11 of the regulations and the implementation of unit policy compliance.
Our internal staff and outsourcing vendors and visitors should all abide by this policy.
3 Goals
To maintain the confidentiality, integrity and availability of school information assets in accordance with the Personal Data Protection Act to protect personal data privacy. By the joint efforts of all my colleagues to achieve the following objectives:
3.1 protect the activities of the school business information from unauthorized access.
3.2 Protection of school business activities information and prevent unauthorized modification, to ensure its accuracy and completeness.
3.3 IT business continuity plan of operation to ensure the continued operation of the school of business activities.
3.4 school implementation of operational activities shall comply with the requirements of relevant laws or regulations.
4 Responsibility
4.1 the school's management of the establishment and review of this policy.

4.2 Information security managers to implement this policy through appropriate standards and procedures.

4.3 All staff and outsourcing services vendors are required to maintain information security policies in accordance with the relevant safety management procedures.

4.4 All staff have a responsibility to report information security incidents and any identified weaknesses.

4.5 Any acts that jeopardize the security of information, depending on the seriousness to be civil, criminal and administrative responsibility, or in accordance with the relevant provisions of the school punished.

5 review

The policy should at least review once a year, to reflect the latest government regulations, technology and business development, as to ensure sustainable school operation and academic network service.

6 implementation of the

6.1 Information security policy with the management review meetings to audit information security policy.

6.2 policy approved by the Information Security Committee, the implementation of the revisions.