Kuantum Papers Ltd

The Paper Makers

Information Security Policy

INFOTECH

Contents

Purpose

The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of Kuantum Papers. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for any organization to recover. This information security policy outlines Kuantum's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the company's information systems.

Kuantum is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which Kuantum is responsible

The objectives of this policy are outlined below:

- Provide a framework for establishing suitable levels of information security for all information systems (including but not limited to computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Provide the principles by which a safe and secure information systems working environment can be established for authorized users.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect Kuantum from any liability or damage through the misuse of its IT facilities
- Respond to changes in the context of the organization as appropriate, initiating a cycle of continuous improvement.

Thus, through this policy, Kuantum will be able to maintain:

- **Confidentiality** – data and information assets must be confined to people authorized to access and not be disclosed to others;
- **Integrity –** keeping the data intact, complete and accurate, and IT systems operational;
- **Availability –** an objective indicating that information or system is at disposal of authorized users when needed.

Data classification

- The organization classifies data/information into three categories:
  a. **Confidential:**
     It includes data/information assets which are highly sensitive and may have legal and policy regulations e.g. Payroll, personnel, financial, biometric data
  b. **Private:**
     It includes important data which is not as sensitive as 'Confidential' information but is discreet enough to be not treated as 'Public' e.g. Agreement documents, unpublished

reports, etc.

c. **Public:**

It includes data/information that can be freely disseminated e.g. brochures, published reports, other printed material, notices, circulars, operational achievements etc.

- Different protection strategies must be developed by the IT department for transmission/ sharing of the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.
- Certain confidential data can be encrypted when transmitted over insecure channels.
- All mail communications and operational data/information must be backed up on a regular basis as per the rules defined by the IT Department at that time.

Authority and access control policy

- Access to the network, servers and systems in the organization is to be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.
- Physical access to high security areas (Server Room) is controlled with proper security (Access Card Control System)
- Access to all computing and information systems and peripherals is restricted through firewall as well as security software
- Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
- Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.
- Access to ERP should be regulated through a well-defined ERP Password Policy.

Data support and operations

Adequate procedures are deployed to ensure backup of:

- **File Backup System:**
  - Organization will be installing a file server for backing up all operational data of ERP. All employees are expected to keep official data on the file system.
  - All employees will login to the file server through Active Directory user ID and password. The relevant application(s) should have a dedicated backup process in place.
  - The access to such backup should be restricted to the Authorized System Administrator.
- **Server backup:**
  - IT Dept. is expected to maintain an incremental backup of all servers at periodic intervals. The periodicity should be defined on the basis of available resources.
  - Tape backup of all running servers will be offline and it should be maintained on daily basis

- The organization should have a clearly defined Backup and Recovery policy.

- **Movement of Data:**
  - The movement and exchange of official data should be through official e-mails and shared network drives only
  - The copying and movement of official data on removable storage devices is strictly prohibited, except with approval from appropriate approving authority.

Security awareness and behavior

- Regular IT Security Training workshops should be organized to communicate and educate Users on IT Security Policy.
- The same should be conducted to include all relevant users; especially the new joiners.
- The content of the training modules should cover topics such as educating on IT Security policy, DO's and DON'Ts , measures to ensure data privacy and security at individual level, e-mail etiquettes, process for communicating any system security issues, latest threats prevalent in cyber-world and mitigation thereof, data management etc.