Kinergy

Kinergy Advancement Berhad
Kinergy Group
Kinergy/ the Group

Basic Code of Information Technology Policy

BASIC CODE OF INFORMATION TECHNOLOGY POLICY

1. Information Security Mission Statement

Kinergy Advancement Berhad and its Group of Companies ("Kinergy" or **"the Group")** is committed to protecting Kinergy's information and information systems assets from failure of availability, confidentiality, and integrity, while at the same time, ensuring that important internal controls are in place throughout Kinergy's data center operations and other processing facilities globally.

2. Obligation to Safeguard Business Information Assets

All individuals granted access to Kinergy's business information assets, including, without limitation, employees, contractors, consultants, vendors, business partners, and temporary employees) are hereby obligated to:

- Handle, store, and use such information assets solely for authorised business purposes;
- Protect the confidentiality, integrity, and availability of these assets at all times;
- Comply with all applicable laws, regulations, contractual obliations, and Kinergy's information security policies and procedures;
- Immediately report any actual or suspected breaches, unauthorised access, or misuse of business information assets.

Failure to comply with these obligations may result in disciplinary action, contractual remedies, or legal proceedings, as deemed appropriate by Kinergy.

3. Policy Principles

3.1 Legal, Statutory, and Regulatory Compliance

All Kinergy employees, contractors, and other third parties must comply with the legal, statutory, and regulatory requirements, both domestic and international, pertaining to the protection, sharing, or disclosure of Kinergy information.

3.2 Timely and Accurate Reporting

All employees, contractors, and other third parties are required to report information security violations, problems, or threats to the human resources ("HR") Department without delay.

3.3 Enforcement and Compliance

All Kinergy companies, divisions, subsidiaries, business partners, managers, or any personnel are responsible for proactively enforcing the information security policies, standards, and procedures.

Individual who violates the policy may be subject to disciplinary action up to and including termination and may incur criminal or civil liability

HR department to ensure that employees are informed and understand the disciplinary action that will take place upon non-compliance with the Information Technology policies.

3.4 Third Party Services and Service Centres

Third parties that have access to Kinergy's information must guard it with the same diligence as Kinergy.

4. Computer Use Policies

Kinergy communications systems, including e-mail, voicemail, and computer systems, are group property and should be used for business purposes only.

4.1 Waiver of Privacy

Users of Kinergy's facilities waive all rights to privacy in anything they create, store, send, or receive on Kinergy computers or through Kinergy's connections to the Internet. Kinergy reserves the right to monitor any and all aspects of its computer system and network to ensure compliance with Kinergy policies. Monitoring includes, but is not limited to, tracking the sites that users visit on the Internet, monitoring chat groups and newsgroups, and reviewing material downloaded or uploaded.

All computers and laptops remain the sole property of the group and must be surrendered immediately upon request or instruction by the HR Department or Management for checking, inspection, or any other purpose deemed necessary by the group.

4.2 Personal Use of the Internet and E-mail

While Kinergy recognises that individuals who use computer systems may occasionally need to use the Internet or e-mail for personal reasons, users should understand that such usage is not considered private. All personal use must not interfere with Kinergy's business.

4.3 Unauthorised Activities

Kinergy's resources must not be used for any of the following activities:

- Receiving, viewing, sharing, or distributing any materials that may be deemed offensive, or which is prohibited by the group policy.
- Commercial or personal advertisements.
- Solicitations or promotions of any outside business.
- Political lobbying or promoting political activities.
- Any commercial purpose other than official Kinergy business.
- Distribute chain letters or solicitation e-mails to others using group email systems.

4.4 Unauthorised Software and Hardware Tools

Employees and others with access to Kinergy's network are prohibited from using any software without HR Department and Management approval. Any use of external software or hardware tools must obtain approval from HR Department and Management in advance.

4.5 Portable Computer Physical Security

- Portable computers must be kept physically secure. Employees assigned to a portable computer by Kinergy must assume all responsibilities of the security of the portable computer and the information/programs/data stored in it.
- Users must assume responsibilities of the security of all removable media (disks, power adaptors, etc.).

4.6 Backup of Local Computers

Employees or others using Kinergy's desktop/laptop computers are responsible for ensuring that all locally held Kinergy's information is properly backed up and recoverable.

All data stored on portable computers should be backed up on at least a bi-weekly basis to a centralised server or removable media (such as external drivers, pen drive and/or any storage media). Users or owners of the information stored in portable computers are responsible for ensuring the timely and accurate backup of their data.

In addition, employees are strictly prohibited from deleting, removing, downloading, copying, or altering any company information, files, or data stored on Kinergy's computers, servers, or storage systems during their employment or while serving notice, unless prior written approval is obtained from Management. Employees are also not permitted to download, save, transfer, or retain any of the Group's information for personal use under any circumstances.

4.7 Backup of Local Server

Local server should be set up for auto-backup between 12.00a.m. to 2.00a.m on daily basis. IT personnel (outsourced) shall ensure the auto-backup function properly on weekly basis.

5. Logical Access

5.1 Access to Information

Access to information must be granted based on an individual's job responsibilities and/or a valid need-to-know. Unauthorised access or use of an individual's account is prohibited.

5.2 Protecting Passwords

- Passwords should be considered personal and must be well protected.
- Passwords must not be written down and left in a place where unauthorised persons might discover them.
- Passwords should not be sent through internet e-mail unless securely encrypted.
- Passwords must not be disclosed or shared with anyone.
- In general, users should never disclose their password to anyone in any circumstances.

5.3 Clear Desk Policy

Sensitive documents, or removable media containing sensitive information, should not be left unattended where someone could easily pick it up, such as in the copying machine, printer, fax machine, or in an unsecured office or workspace.

5.4 Unattended Computers and Information

Systems must have a feature that protects access to the information on the screen and to further data in the machine if being left unattended after a defined time (at the longest 20 minutes) and must not allow access until released by a valid password.

6. Internet Connection Policies

6.1 Internet Access

All outbound access to the Internet must be made through a proxy server. Direct connections outbound to the Internet must not be allowed.

6.2 Inappropriate Internet sites

Access to inappropriate sites through Kinergy facilities and equipment is prohibited. Examples of such sites may include but are not limited to:

- Sexually explicit sites; or
- Hacker sites; or
- Any pirated software or hacker tools related sites; or
- Sites that may conflict with Kinergy's policies and/or business interests

6.3 Prohibited Internet Activity

- Downloading or installing of freeware and/or shareware is prohibited unless approved by the HR Department and Management.
- Employees must not use the internet for playing online games and watching videos which is not related to business activities.
- Sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the network.
- Any way that violates federal, state, or local laws or statutes.

6.4 Externally Reachable Websites

All web sites available to the public or entities outside of the Kinergy must be approved by the HR Department and Management. Publishing personal websites using Kinergy's equipment of network is prohibited.

7. Virus Protection

Anti-virus software must be installed and activated on each desktop, laptop, and server with real-time scanning enabled at all times. Any external data storage (pen drive, hard disk or etc.) or other media to transfer data into a computer must be scanned for viruses.

8. Copyright Policies

The loading of pirated (unlicensed) software on Kinergy's machine/equipment is prohibited.

9. Contact Information

For questions, please email your enquiry to the HR Department to: it@kinergyadvancement.com

10. Review

This Policy is subject to periodic review and refinement to ensure ongoing relevance, effectiveness and alignment with emerging regulatory requirements, industry best practices and stakeholder expectations. This Policy was approved by the Management of Kinergy on 24th November 2025.