

IJM CORPORATION BERHAD

GROUP IT POLICY

1. Scope

The IT policy covers all IJM employees who have access to any of the IJM computing resources, including but not limited to:

- Business application system
- Database system
- Electronic mail system
- IJM INTRANET portal
- INTERNET access
- File & print service
- Desktop PC and notebook
- Printer, plotter, scanner, and CD/DVD drive
- Office automation software and productivity tools

The access and use of these resources is a privilege provided by IJM. Failure to abide by the policy may result in forfeiture of the privilege.

2. Ownership and Rights

All computing equipment, media, software, systems, and data shall remain the properties of IJM.

IJM reserves the rights to monitor, inspect, audit, and scrutinize the data and systems in its computing equipment at any time as and when it so wishes.

3. Licensed Software

It is the policy of IJM to use only licensed products.

The installation, replication, or use of any unlicensed software or product is strictly prohibited. Disciplinary and legal actions can be taken against employees who breach the policy.

4. Access Control

All accesses to IJM computing resources shall be permitted only to authorized staff approved by the respective Head of Department, subject to final endorsement by the Head of Information Systems Department upon reviewing their job functions, duties, and needs.

Once access is granted, the user shall be responsible for all activities associated with the access.

The use of any system without permission is considered to be unauthorized and is strictly prohibited. Disciplinary action may be taken against such unauthorized access.

5. Identification and Authentication

Each user shall have a unique user-ID assigned by the Information Systems Department according to an established access control procedure.

The system shall require a user to be identified with the assigned user-ID before he is permitted to perform any action on the system.

A user shall be authenticated by correctly providing a password for his user-ID.

A user-ID and password must never be shared, publicized in any way, or otherwise kept in a place or manner that would make it obtainable by an unauthorized person.

6. User Responsibilities

A user shall be held accountable for all actions resulting from the usage of his user-ID regardless of whether the actions were performed himself or executed on his behalf.

A user shall act responsibly when handling and using IJM's computing resources in his possession.

A user must keep his password confidential.

A user shall properly log out from the system before leaving it unattended or for use by another individual.

7. Manager Responsibilities

A manager can be held accountable for all actions done via the user-ID assigned to a member of his team regardless of whether the employee performed the actions himself or the actions were done on his behalf.

A manager should ensure that members in his team meet all the requirements as described in the section "User Responsibilities".

The manager should immediately inform the Information Systems Department whenever actual or potential security exposures have been identified.

The manager should take immediate action to notify the Information Systems Department whenever a user transfers, terminates, or no longer requires access to a system.

8. Electronic Mail System

The e-mail facility provided to a staff must be used for IJM related business communications only.

Once an electronic mailbox is granted, the user shall be responsible for all activities associated with the mailbox. At all times, the user is required to adhere to the following practices:

1. Do not submit, publish or transmit information or data that contain false, abusive, discriminatory, obscene or illegal material.
2. Do not distribute or propagate unsolicited or unauthorized messages, whether voluntary or involuntary.
3. Do not intercept, disclose or view e-mail messages that are not addressed to the user.

9. INTERNET Access

Access to public INTERNET via IJM's networking infrastructure is confined to staff whose duties require it for their normal business activities.

Once access is granted, the user shall be responsible for all activities associated with the access. At all times the user is required to abide by the following:

1. Do not disclose or disseminate any sensitive information over the network, whether voluntary or involuntary.
2. Do not deliberately attempt at infringing another organization's network.
3. Copyrighted software or materials in the network should not be duplicated or modified unless it is expressly allowed. Do not copy when in doubt.
4. Do not access, maintain or propagate materials that are offending, pornographic or illegal.

10. Data Protection

A user handling company data shall be responsible for ensuring the data is safe and secured against any loss or theft.

As a mean of protection against any unforeseen event, data should be backed up on a regular basis. The backup cycle may include daily backup, weekly backup, monthly backup and yearly backup.

All daily, weekly, monthly and yearly backups should be stored in an off-site location away from the computing equipment, except when they are required for restoration purposes.

The integrity of the backups should be tested as frequent as necessary or at least once a year, by restoring the backup data to a test environment.

ooooOOOoooo