

MANAGEMENT INFORMATION SERVICES (MIS) POLICY

This policy details out company principles regarding the usage of MIS facilities and technologies.

1. Email

Email is to be used for Company business purposes only. Company confidential information must not be shared outside of the Company, without authorization, at any time.

2. Prohibited and Restricted Software

Usage of any unauthorized copies of the software in the organization will not be tolerated. Employees who illegally install, use, or reproducing software can be subject to civil and criminal penalties including fines and imprisonment. An employee who makes use of, or acquires unauthorized software takes full responsibilities of the consequence of violating copyright law requirement.

3. Security

3.1 User Account Creation, Modification and Deletion

ND provides its employees with access to various computing resources. MIS Department is responsible to provide access to computing resources upon authorization by respective management.

3.2 Password

Passwords are the front-line protection for user accounts. A poorly chosen password may result in unauthorized access and/or exploitation of ND's resources or the entire corporate systems. It is employee's responsibility to always keep their password confidential, update their password periodically and avoid choosing weak passwords.

3.3 Malicious Protection

Malicious protection is necessary to safeguard the availability, performance and security of ND MIS resources, which are essential to ND's daily operations. All employees are responsible to ensure anti-virus product is enabled at all time.

3.4 User Access Control

Application access control policy authorizes users to perform a set of actions on application systems within ND. MIS Department is responsible to grant the privilege access to the resources only after explicit authorization by respective management is provided.

3.5 Security and Privacy

Company reserves the right to review, monitor and/or capture any content residing on, or transmitted over, its computers or network at its sole discretion. Company also reserves the right to limit access to its computers or network, and to remove or limit access to material residing on its computers or network.

4. Network Access

Employees shall not share the network wi-fi password to third parties. MIS retains the right to enforce MIS policy for mobile phone connected to the company Wi-Fi network. Internet Access is allocated to according to user authorization level or based on special requests.

5. Asset

MIS is responsible for the requisition, designation, issuance, tracking, transfer and disposal of MIS assets. MIS is also responsible to define controls necessary to mitigate information security risks affecting ND's desktops and laptops.

6. Bring Your Own Device (BYOD)

Staffs are allowed to use personal electronic devices for company purposes. Personal laptops, computers, smartphones or any electronic devices that utilizes company facilities & technologies are the responsibility of the employees themselves to ensure that all software intended for use on behalf of the company is properly licensed.

1. Email, 2. Prohibited and Restricted Software, 3. Security and 4. Network Access policy will be automatically applied to BYOD devices once connected to the company network or utilizing company facilities & technologies.



DATO' AZIZ AYOB

PRESIDENT

1st MAY 2019