Information Technology and Cyber Security Policy

N.D. Rubber Public Company Limited

"Information Technology and Cyber Security Policy"

N.D. Rubber Public Company Limited (the "Company") and its subsidiaries have established this Information Technology Security Policy to define operational procedures and guidelines. This policy aims to prevent data loss and protect both software and hardware assets in the event of IT emergencies. The details are as follows:

Internet and E-mail Usage Policy (IT-Internet)

1. During working hours, Internet access is permitted only for authorized websites or those directly related to professional duties.
2. E-mail system passwords must be at least 8 characters in length, consisting of lowercase letters, uppercase letters, and numerical digits. The IT Department is solely responsible for assigning initial passwords and installing Outlook for users.
3. Employees are prohibited from using corporate e-mail addresses for personal registrations on the Internet, such as posting personal product advertisements or sales listings.
4. External agencies or third parties requiring access to the Company's Internet network must obtain prior authorization from the IT Department or relevant personnel via the IT Service Request Form.

Antivirus Protection Policy (Sophos Antivirus)

1. Sophos Antivirus shall be installed on all user systems and kept up to date with the latest virus patterns.
2. Users are authorized to perform virus scans on local drives only.
3. To prevent virus infections, the use of external storage media with Company computers is strictly prohibited.
4. In the event of a virus infection, users must immediately contact the IT Helpdesk at extension 110.
5. The IT Department shall provide ongoing communication and education regarding virus prevention.

Password Policy (IT-Password)

System passwords must be configured according to the following standards:

1. Operating System Passwords: Must be at least 8 characters in length, comprising lowercase letters, uppercase letters, and numbers (e.g., It123456, Admin678), excluding special characters such as @, #, $, %.
2. Password Expiry: Passwords shall expire every 90 days. Users are prohibited from reusing any of their last 5 consecutive passwords.
3. Password Masking: Passwords must be shadowed or masked (*) during entry and shall not be displayed or printed in plain text.
4. Initial Passwords: Default passwords must be changed immediately upon the user's first login.
5. System Defaults: Default passwords provided with the system and unused user accounts must be locked and disabled.
6. Account Lockout: After 5 failed login attempts, the user account will be locked. The user must contact IT personnel to unlock the account.

Personal Computer and Laptop Usage Policy (IT- Computer/ Laptop)

1. Employees are not authorized to install any software on their assigned Computers or Laptops. Any software required for work purposes or other activities must be requested via the IT Service Request Form and approved by the respective supervisor. IT personnel will perform the installation following such approval.
2. In the event that an employee utilizes unauthorized or non-official software, the employee shall be solely responsible for all associated costs and damages, including but not limited to copyright infringement or any resulting technical issues.
3. Employees are prohibited from storing images, video media, or any files that are illegal, immoral, or unethical on their computers or Laptops. Should any issues arise, such as copyright infringement or other damages, the employee shall be solely liable for all costs and consequences incurred.
4. Users must lock their computers or log off every time they leave their desks. Computers or Laptops must not be left accessible to others in the employee's absence. Failure to comply will result in the logged-in user being held responsible for any actions or damages occurring during that session, as if they had performed the actions themselves.
5. Computer monitors must be turned off when not in use for an extended period. Additionally, both the Computer/Laptop and its monitor must be completely shut down before leaving the office each day.

Administrator Operational Policy (IT-ADMIN)

1. System administrators must perform thorough testing before installing software or implementing configuration changes on production systems.
2. Do not leave any external media, such as disks or CDs, in computers or laptops when not in use.
3. System administrators must log off from the system immediately after completing tasks on server consoles.

IT Intrusion Detection Policy

1. Operating System Logging: System access logging must be enabled, and log data must be secured against unauthorized modification or deletion.
2. Antivirus Alerts and Logging: Antivirus notification functions and activity logging must remain enabled at all times.
3. Internet Traffic Logs: In accordance with the computer-Related Crime Act B.E. 2560 (2017), internet usage logs must be retained for a minimum period of 90 days.
4. Firewall Security Features: APT Blocker and Gateway Antivirus features must be activated on the firewall to protect the network against cyberattacks.

Data Backup Policy (DATA-BACKUP)

1. he IT Department shall perform data backups for documents and files stored on shared network drives (Mapped Drives), specifically within public folders, at least every three days. Please be advised that data stored locally on Drive C: D: or E: (such as "My Documents" or "Desktop") is not included in the automated backup system. In the event of data loss in these local areas, the IT Department will attempt recovery using appropriate software; however, there is no guarantee that the data can be recovered partially or in its entirety.
2. Should a user experience data loss, they must report the incident to the IT Department in person only. This is to facilitate a thorough inquiry regarding the nature of the issue and the original file location before the loss occurred. Recovery procedures will be initiated immediately upon notification.
3. Backup storage media and devices must be kept in a secure location. Ideally, backups should be stored in more than one physical location to ensure maximum data security and redundancy.

IT Equipment Maintenance Policy (IT-Maintenance)

1. If IT personnel identify hardware issues or determine through visual inspection that equipment is excessively dirty or prone to future operational failure, corrective cleaning or preventive measures must be taken immediately, even if the equipment remains functional at that time.
2. A comprehensive maintenance plan for both hardware and software must be implemented every four months. This involves physical inspections of hardware components (noting that certain parts may not be cleanable) and software performance evaluations conducted via user interviews and the official maintenance checklist.

Access Review Policy

Access Rights Review: System access rights and permissions must be audited and reviewed at least once per year.

Data Classification Policy (Data Share Policy)

Objective The purpose of this policy is to establish guidelines for the appropriate management and protection of company data. It aims to prevent data breaches that could result in damage to the organization. By classifying data based on priority and sensitivity, the company can implement security measures proportionate to the nature of each data type.

SL1: Top Secret Refers to highly sensitive information that must not be disclosed. Access is strictly restricted. Unauthorized disclosure would result in exceptionally grave damage to the company.

SL2: Confidential Refers to sensitive information that should not be disclosed. Access is restricted to specific authorized groups only. Unauthorized disclosure would adversely affect the company’s interests or operations.

SL3: Internal Use Refers to information intended for use solely within the organization. Usage must be controlled, and external distribution is prohibited without prior authorization.

SL4: Public Refers to information that can be disclosed to the general public without causing any damage to the company.

This Information Technology and Cyber Security Policy were considered and approved by the Board of Directors at the Board of Directors Meeting No. 4/2026, held on May 14, 2026.

(DATO' Alex Surname: Kang Pang Kiang)

Chairman of the Board of Directors

N.D. Rubber Public Company Limited