Purpose

Tong Thai Rubber Group is committed to maintaining a secure, efficient, and professional working environment. This policy establishes the guidelines for using our digital resources, including:

1. Internet Use
2. Email Use
3. Social Media Use
4. Cybersecurity Measures

This policy is designed to protect our company's data, systems, and reputation. It is also established to protect Tong Thai Rubber Group's digital assets, IT systems, networks, and data from unauthorized access, disclosure, alteration, damage, or disruption. It provides guidelines for employees, contractors, and third-party users to maintain a secure and resilient IT environment. All employees, contractors, and sub-contractors are required to adhere to the following standards.

Scope of Application

This policy applies to all individuals with access to Tong Thai Rubber Co., Ltd.'s digital resources. It governs the use of company-provided internet, email, and social media accounts, as well as the procedures related to cybersecurity, data protection, and overall IT system integrity.

This policy also applies to all employees, contractors, and third-party service providers who access, manage, or use Tong Thai Rubber Group's IT resources, including but not limited to:

- Desktop and laptop computers, mobile devices, tablets, and other computing equipment
- Network systems and connections (wired, wireless, and remote access)
- Cloud services and storage
- All data, including confidential, proprietary, and personal information

Definitions

- **Information Assets:**
  All data, systems, and technology resources owned or managed by Tong Thai Rubber Group
- **Confidential Information:**
  Any non-public data, including trade secrets, client data, and internal communications.
- **Security Incident:**
- Any event that compromises the confidentiality, integrity, or availability of Tong Thai Rubber Group's information assets.
- **Access Control:**
  Mechanisms restricting system access to authorized users and processes only.

- **Social Media:**
  Any internet-based platform that allows for the creation, sharing, and interaction of content. This includes, but is not limited to, social or business networking sites (e.g., Facebook, LinkedIn), video and photo sharing websites (e.g., YouTube, Instagram), personal and corporate blogs, microblogs (e.g., Twitter), chat rooms, and forums

Roles and Responsibilities

- **All Users:** Adhere to this policy, report suspicious activities, and use IT resources responsibly.
- **IT Department/IT Specialist:** Implement and maintain security controls, monitor network activities, manage access rights, and respond to security incidents.
- **Management:** Support security initiatives, ensure policy compliance, and provide necessary training and resources.

1. Internet Use

- **Purpose and Permissible Use:**
  The company's internet access is provided primarily for business-related activities. Limited personal use is permitted only if it does not interfere with work responsibilities. Inappropriate content, including but not limited to pornography and gambling is strictly forbidden.

- **Monitoring and Compliance:**
  Management reserves the right to monitor internet usage to ensure adherence to this policy. Excessive or inappropriate personal use may result in disciplinary action up to and including termination. Employees should be aware that violations may also lead to legal consequences.

2. Email Use

- **Business Communications:**
  Email accounts are provided for formal business correspondence only. All outgoing emails must contain the approved company disclaimer.

- **Security and Confidentiality:**
  Employees must safeguard sensitive information. Emails containing confidential data should be properly archived and stored offsite when necessary. Care should be taken to ensure that information does not inadvertently reach unauthorized recipients.

- **Personal Use:**
  While limited personal use is allowed, it must not disrupt work responsibilities. Management maintains the authority to review email communications to verify compliance.

- **Content Guidelines:**
  To protect Tong Thai Rubber Group from the potential effects of the misuse and abuse of email, the following instructions are for all users:

  1. No material is to be sent as email that is defamatory, in breach of copyright or business confidentiality, or prejudicial to the good standing of Tong Thai Rubber Group in the community or to its relationship with staff, customers, suppliers and any other person or business with whom it has a relationship.
  2. Email must not contain material that amounts to gossip about colleagues or that could be offensive, demeaning, persistently irritating, threatening, and discriminatory, involves the harassment of others, or concerns personal relationships.
  3. The email records of other people are not to be accessed except by management (or people authorized by management) ensuring compliance with this policy, or by authorized staff who have been requested to attend to a fault, upgrade or similar situation. Access in each case will be limited to the minimum needed for the task.
  4. When using email, a person must not pretend to be another person or use another person's computer without permission.
  5. Excessive private use, including mass mailing, "reply to all" etc. that are not part of the person's duties, is not permitted.
  6. Failure to comply with these instructions is a performance improvement offense and will be investigated. In serious cases, the penalty for breach of policy, or repetition of an offence, may include dismissal.

3. Social Media Use

Tong Thai Rubber Group expects its employees to maintain a certain standard of behavior when using Social Media for work or personal purposes.

- **Work Use of Social Media**

  1. Applicability
  This policy applies to all employees, contractors and sub-contractors of Tong Thai Rubber Group who contribute to or perform duties such as:

1. maintain a profile page for Tong Thai Rubber Group on any social or business networking site (including, but not limited to, LinkedIn, Facebook, Instagram, Twitter and Snapchat);
2. make comments on such networking sites for and on behalf of Tong Thai Rubber Group;
3. write or contribute to a blog and/or comment on other people's or business' blog posts for and on behalf of Tong Thai Rubber Group; and/or
4. post comments for and on behalf of Tong Thai Rubber Group on any public and/or private web-based forums or message boards or other internet sites.

2. Authorized Representation

- **Approval Requirement:**
  No individual may represent Tong Thai Rubber Group on social media without prior written approval from the managing director(s).

- **Professional Conduct:**
  When directed to engage in social media on behalf of the company, you must always act professionally and in the best interests of Tong Thai Rubber Group.

3. Confidentiality and Content Restrictions

- **Confidential Information:**
  Do not disclose any information in the public domain regarding Tong Thai Rubber Group, its clients, business partners, suppliers, or employees. This includes, but is not limited to, confidential trade documents, transactions, or internal discussions.

- **Content Guidelines:**
  Refrain from posting any content that:
  - Violates the privacy or publicity rights of any individual or organization.
  - Contains confidential or proprietary information without proper authorization.
  - May insult, offend, intimidate, or humiliate Tong Thai Rubber Group, its clients, partners, or suppliers.
  - Is defamatory or could damage the reputation, viability, or profitability of the company or its associates.

- **Personal Use of Social Media**

1. Separation of Identity:
While you retain the right to express personal opinions on public platforms, you must not identify yourself as being associated with Tong Thai Rubber Group unless explicitly authorized.

2. Responsibility:

Recognize that your online behavior, even on personal accounts, can reflect on Tong Thai Rubber Group. Avoid sharing any material that could be construed as inappropriate or damaging to the company's reputation.

4. Cybersecurity Measures

1. Roles and Responsibilities

- All Users: Adhere to this policy, report suspicious activities, and use IT resources responsibly.
- IT Department/IT Specialist: Implement and maintain security controls, monitor network activities, manage access rights, and respond to security incidents.
- Management: Support security initiatives, ensure policy compliance, and provide necessary training and resources.

2. Acceptable Use of IT Resources

- IT resources must be used only for legitimate business purposes.
- Unauthorized activities—such as installing unapproved software, bypassing security controls, or sharing credentials—are prohibited.
- Personal use of company devices or networks must comply with this policy

3. Protecting Personal and Company Devices

- Employees using digital devices to access company emails or accounts introduce additional security risks. To mitigate these risks, all users must:
- Keep all devices (company-issued and personal) password protected.
- Install and regularly upgrade comprehensive antivirus software.
- Avoid leaving devices exposed or unattended in public or insecure areas.
- Apply security updates for browsers and operating systems monthly or as soon as they are available.
- Access company accounts and systems only via secure, private networks.

4. Email Safety

Emails are a common vector for scams and malicious software. To protect against these threats, employees must:

- Avoid opening attachments or clicking links from unknown senders or if the email content does not align with expected communication.
- Be wary of clickbait titles or emails offering unexpected prizes.

- Verify the legitimacy of senders by checking email addresses and looking for inconsistencies (e.g., grammatical errors, unusual punctuation).
- Immediately report suspicious emails to the IT Specialist for further investigation and potential sender blocking.

5. Password Management

Passwords are a critical line of defense against unauthorized access. Employees are required to:

- Choose passwords with at least six characters that include a mix of uppercase, lowercase, numbers, and symbols, avoiding easily guessed information.
- Memorize passwords rather than writing them down; if a record is necessary, it must be kept confidential and destroyed when no longer needed.
- Exchange credentials only when absolutely necessary—preferably by phone if in-person verification is not possible.
- Change passwords regularly to reduce the risk of compromise.

6. Data Transfer Security

Transferring data can introduce security risks. To ensure data is protected during transit, employees must:

- Avoid transferring sensitive data (e.g., customer information, employee records) unless absolutely necessary; consult the IT Specialist for mass data transfers.
- Share confidential data only over the company network or secure systems—not over public Wi-Fi or unsecured connections.
- Confirm that recipients are authorized and maintain adequate security policies.

7. Reporting Scams, Breaches, and Hacking Attempts

Timely reporting of potential security threats is critical. Employees must:

- Report any perceived scams, privacy breaches, suspicious emails, or hacking attempts immediately to the IT Specialist.
- Cooperate with IT in investigating and resolving any security issues, and heed any companywide alerts issued as a result.

8. Additional Security Measures

To further reduce the risk of security breaches, employees are instructed to:

- Lock devices or turn off screens when leaving desks unattended.
- Report stolen or damaged equipment immediately to management.

- Change all account passwords promptly if a device is stolen.
- Report any perceived threats or weaknesses in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on company equipment.
- Avoid accessing suspicious websites or downloading software without management authorization.

9. Remote Access and Mobile Device Security

Remote employees must adhere to all aspects of this policy when accessing company systems from outside the office:

- Use approved VPNs or secure connections to access company networks.
- Ensure that any device used remotely is secure and updated, and that the private network is protected by appropriate security measures.
- Seek guidance from the IT Specialist if unsure about the security of their remote access setup.

10. IT Specialist Responsibilities

The IT Specialist is tasked with maintaining a robust security posture by:

- Installing and maintaining firewalls, anti-malware software, and access authentication systems.
- Ensuring all downloaded software is authorized by management and properly licensed.
- Applying security updates for browsers and systems promptly.
- Arranging regular security training sessions for all employees.
- Keeping employees informed about new scam emails, viruses, and best practices for mitigation.
- Investigating security breaches thoroughly and taking appropriate remediation actions.
- Blocking email accounts from sending/receiving messages in response to multiple false login attempts or unusually high email volumes.

11. Security Incident Management

- All users must report any suspected or actual security incidents immediately to the IT Department.
- Tong Thai Rubber Group will maintain an Incident Response Plan that outlines procedures for assessing, containing, and remediating security breaches.
- Post-incident reviews will be conducted to improve policies and prevent future occurrences.

12. Training and Awareness

- Regular cybersecurity training and awareness programs will be provided to ensure all users are informed about current threats, safe practices, and their responsibilities under this policy.
- Additional training will be mandated for roles with elevated access or exposure to sensitive data.

13. Monitoring, Auditing, and Compliance

- Tong Thai Rubber Group reserves the right to monitor and audit all IT systems and user activities to ensure compliance with this policy.
- Periodic audits will assess the effectiveness of security controls and overall policy adherence.

14. Enforcement and Disciplinary Action

All employees, contractors, and subcontractors are required to adhere strictly to this policy. Any breach of this policy will be taken seriously and may result in disciplinary actions, which include:

- Formal warnings
- Suspension from duties
- Denial of access to company networks (temporarily or permanently)
- Termination of employment or non-renewal/termination of contractual arrangements

Signature

General Manager of
Tong Thai Rubber Group
Ms. Shi Ching Chien
Date: 10/01/2025