Protecting Physical, Financial, IT and IP Assets

Part 1/3

We protect TMICC’s assets, guarding them from misuse, fraud and theft and approving only activities within our role and responsibilities. We safeguard TMICC’s intellectual property by ensuring our brands and innovations are protected. We respect valid third-party intellectual property rights by obtaining the relevant licences and approvals.

Why is it important?

TMICC’s technology and information are vital tools that allow employees and trusted partners to perform their roles effectively. When these assets are misused, stolen, damaged or handled carelessly, the impact can be serious – disrupting operations, breaching legal and privacy obligations, and harming our reputation. By protecting our assets and handling our information with the right level of care and classification, we keep our operations running smoothly, safeguard financial stability, preserve innovation and competitive advantage, protect individual’s rights and meet our legal and regulatory obligations.

What must I do?

All assets:

- Handle TMICC’s physical assets – for example factory equipment, products, buildings, computers and vehicles – with care, to avoid damage, misuse, or loss.
- Report theft or loss to site SHE Managers promptly.
- Do not remove TMICC assets, except TMICC issued laptops and phones, from any site unless authorised, and do not use TMICC assets inappropriately or for unauthorised personal benefit.
- Identify and manage potential hazards to assets on site, reducing risks to an acceptable level.
- Guard TMICC’s financial assets – such as cash, bank accounts and credit cards – against misuse, loss, fraud or theft, and immediately escalate any red flags to my Line Manager.
- Approve financial transactions only within my limits, as defined by my role, and in compliance with the **Global Schedule of Authorities.**
- Address cyber security risks by embedding cyber security standards and controls. This particularly applies if implementing or purchasing technology solutions.
- Beware of cyber security risks on any devices used for TMICC business:
  - **Avoid** opening attachments, unless I know the sender and have verified the accuracy of the email address.
  - **Avoid** visiting websites that may not have adequate security certificates.
  - **Use** multi-factor authentication and strong passwords on devices.

Protecting Physical, Financial, IT and IP Assets

Part 2/3

What must I do?

Intellectual Property (IP):

- Do not use TMICC's IP, except for TMICC's benefit.
- Report suspected counterfeit products or potential IP infringements – such as those related to trademarks, patents, designs, copyrights and domain names – to the Business Group or IP General Counsel.
- Ensure checks and filings are completed for patents, trademarks and other IP rights when launching new brands, sub-brands, products, services or other materials.
- Use contracts with appropriate clauses to protect TMICC's IP when working with third parties.
- Refrain from using valid third-party IP without the appropriate licenses, for example Music, Video, Technology etc. If unsure what is valid, speak with my Legal Business Partner.
- Do not train third party GenAI or any other third party LLM with TMICC IP or confidential information, including trade secrets, designs, patents and trademarks.

Information:

- Classify information, documents, and emails in line with the Information Classification Standard: Public, Internal, Confidential, Restricted.
- Follow the requirements outlined in the Information Handling Standard, which sets out what types of information can be shared with whom. Take personal responsibility for how information is used, shared, stored, protected, and disposed of.
- Share TMICC information only on a need-to-know basis with individuals and authorised third parties for legitimate business purposes, or as required by law.
- Do not forward TMICC information to personal email or storage accounts, sync TMICC data on devices not managed by TMICC or use removable media (i.e. USBs).
- Do not engage in contract negotiations, discuss substantive issues with regulators, address due diligence red flags, or share any non-public TMICC information on unapproved technology or on collaboration and messaging tools (WhatsApp, Signal, etc.).
- Understand that, in accordance with our Business Integrity Principles and applicable laws, all information processed by, or stored on, TMICC-issued or owned systems and equipment (and TMICC information on personal devices) may be monitored, inspected or removed by TMICC without prior notification.

TMICC may monitor, log, diagnose, investigate and assess activity and data including messages and other communications sent, received, and stored on TMICC's network, systems and equipment to the extent permitted by applicable laws, to ensure this policy is being followed and TMICC's technical environment is optimised and risk managed.

Life tastes better with Our Code.

Protecting Physical, Financial, IT and IP Assets

Part 3/3

What must I do?

Equipment & technology:

- Use only TMICC-approved technology to share and manage information and take additional care when working in public places.
- Install only approved applications and use only approved services, including Software as a Service and AI.
- Ensure work equipment is used appropriately and kept protected from damage, theft or loss.
- Secure equipment and documents when not in use. Lock any device with a password or PIN when unattended, irrespective of location.
- Do not share TMICC access credentials with anyone, use TMICC passwords anywhere else or use TMICC identities for non-business-related activity.
- Ensure personal use of TMICC technology does not materially impact performance, such as excessive storage or data usage.
- Report any suspected cyber issues or suspicious activity by raising a security incident, such as unauthorised information sharing or unexpected authentication notifications.
- Report lost or stolen devices (TMICC or personal) used to access TMICC information immediately as a security incident.

Malicious activity:

- Do not intentionally access TMICC technology or TMICC information that is not intended for my role, or after leaving TMICC employment.
- Do not disable, bypass or interfere with security controls, for example, browser configuration, anti-virus, privileged access, firewalls or system logs.
- Do not use systems for any illegal activities, or that could cause serious or widespread offence or are associated with violence, terrorism, pornography or insulting content.

If I own, procure or run technology, or manage a third party, what do I need to do?

- Address cyber security risks through the correct application of the Cyber Security Standards and follow the cyber processes detailed on the Cyber Security Zone.

What is the Information Classification Standard?

- Public: Information already available to the general public may be freely distributed.
- Internal: Only shared within TMICC and authorised third parties with a genuine business need.
- Confidential: Only shared on a need-to-know basis with a genuine business need.
- Restricted: Only shared with named individuals who are on the relevant Restricted Information List.

Where do I go for more information?

Chief Information Security Officer, Local SHE Manager or Legal Business Partner, Intellectual Property Standard, Cyber Security Standards, Cyber Security Zone (including to report a Cyber Incident).