8.1.4 Monitoring of compliance with the corporate governance policy and guidelines

Disclosure and Transparency

The Board of Directors have examine and support timely disclosure of the company's business information including financial information and financial reports according to the disclosure regulations of the Securities Exchange of Thailand. Such information is available both in Thai and English for investors, shareholders, and concerned parties to have equal and transparent access to. Also disclosed are auditors' reports, financial figures, and notes to the financial statements. The company also discloses the duties of the Board of Directors and the sub-committees, the number of meetings attended, and directors' remuneration information. The investor relations section is set up to be responsible for providing important information for investors and other concerned parties. The company's information is also disseminated via the Securities Exchange of Thailand and the company's website so investors and stakeholders can have access to its financial and operational information at all times.

According to company regulations, directors and the top four executives after the Chief Executive Officer, and those in management positions in accounting or finance from the sectional level up or equivalent, are required to report their interests and stakes using the interest disclosure report form without delay when a certain transaction may be regarded as having an impact relating to their interests. The reports made shall be in care of the company's secretary.

Inside Information control

The company's measures and guidelines regarding confidentiality and use of inside information to prevent the misuse of such information for the advantage of the company's executives and personnel are summarized below.

1. The Board of Directors, management team, employees and staff of the company shall keep the company's secrets and/or inside information confidential.

2. The Board of Directors, management team, employees and staff of the company shall not disclose or seek advantage from the company's secrets and/or inside information for their own benefit or for the benefit of any other party either directly or indirectly whether or not any benefit is actually received.

3. The Board of Directors, management team, employees and staff of the company shall not buy, sell, transfer, or acquire the company's securities via the use of the company's secrets and/or inside information and/or carry out any act using the company's secrets and/or inside information which may cause direct or indirect damage to the company. This stipulation also applies to spouses and children under legal age of the Board of Directors, management team, employees and staff. Any violation shall be considered a serious offence.

4. The Board of Directors and the executives who acquire the company's financial information shall not take advantage of the information within one month before it is disclosed to the public. The company shall notify directors and executives of the prohibition to purchase or sell the company's securities before the financial statements are revealed to the public.

5. If board of directors and top executives intend to buy or sell shares, they must notify the Board of Directors through the Company Secretary at least one business day in advance before making the transaction.

Statistics on Rule Violations in 2025: There were no violations regarding the misuse of internal information for personal gain that contradicts criteria from regulating bodies and corporate governance principles. Moreover, no directors or executives were found to have traded the company's shares during restricted periods.

For Monitoring and Compliance in 2025, the company has communicated and ensured understanding among board of directors, executives, and employees. The Company Secretary has communicated through email the policies and practices of the misuse of internal information, along with reviewing internal information access protocols.

Additionally, new executives and employees receive this information during orientation and review policies on the use of internal information and confidentiality. A 100% of directors, employees, and executives have been trained this information through e-learning.

The practice not to violate the intellectual property.

The company has set the policy to use and control licensed software to make the employees aware and not violate intellectual property and make the announcement to all levels of employees. The IT department of the company inspects the software programs of the employees once a year to prevent the violation of the licensed software.

Information Technology Security, Cybersecurity, and Data Protection Policy

Stars Microelectronics (Thailand) Public Company Limited places the highest priority on maintaining the Confidentiality, Integrity, and Availability (CIA) of information, as well as ensuring the operational continuity of our information technology systems and the systems supporting critical business processes. Our objective is to prevent unauthorized access to sensitive information, mitigate risks from cyber threats, and protect personal data in compliance with relevant laws and practices. To enhance governance and internal controls, the company has established key policies and measures including:

- **Identity and Access Management (IAM) Policy**: To ensure that users can access only the systems and information authorized for their specific roles and responsibilities under a designated timeframe and subject to periodic access reviews.
- **User Authentication Policy through Multi-Factor Authentication (MFA):** Including username and password requirements to increase security for accessing critical systems.
- **Cyber Threat Prevention Measures**: Covering continuous monitoring, incident management, protection against malware and phishing, regular security patch updates, and the control of information system usage based on risk level.
- **Personal Data Protection Measures**: To prevent the unlawful access, use, disclosure, or loss of personal data in accordance with legal requirements.

In terms of governance, the company is overseen by **the Risk Management Committee and Senior Management**, with progress-tracking meetings conducted on a quarterly basis. Reports are submitted to the Board of Directors to provide updates on risk status, significant incidents, operational performance, and the progress of enhancement plans for cybersecurity controls and personal data protection.

2025 Performance Results

1) Network and Corporate Information System Security

- In 2025, there were a total of 0 (zero) Information Security Incidents. Any potential issues were addressed according to the incident management process, and **they caused no significant damage to the organization.**
- The Company continuously communicates and campaigns to foster information security awareness among employees, covering topics such as personal data care, threat prevention guidelines, safe system usage practices, and understanding relevant laws and regulations, including the Personal Data Protection Act (PDPA).

2) Cybersecurity

- In 2025, the company conducted a total of **4 online cybersecurity training courses**. Participation accounted for 98% of the total target group, and **100%** of participants successfully passed the assessment.
- 2025, **no breaches of information security systems or severe cybersecurity incidents** that caused damage to the company **were discovered.**
- In 2025, **no significant incidents involving the leakage, theft, or loss of personal data were uncovered.**
- In 2025, **no employees were fined or penalized** due to violations of information security systems or actions related to cybersecurity incidents.

3) Personal Data Protection

- In 2025, **no substantiated complaints** regarding personal data breaches **were uncovered.**
- In 2025, **no significant incidents involving the leakage, theft, or loss of customer data were uncovered.**

Progress in Enhancing the Information Security Management System according to ISO/IEC 27001:2022 and the 2026 Certification Plan

To elevate information security management to international standards, the company has commenced the establishment and development of an Information Security Management System (ISMS) **in alignment with the ISO/IEC 27001:2022 standard**. The objective is to create a systematic information risk management framework covering policy formulation, control processes, monitoring and evaluation, and continuous improvement.

Key Guidelines and Activities Implemented/In Progress (Aligned with ISO/IEC 27001:2022)

The company has operated in alignment with the core principles of the ISO/IEC 27001:2022 standard in key areas such as:

- **Establishing the ISMS governance framework and defining the roles and responsibilities** of relevant parties, including monitoring and oversight by senior management.
- **Information Security Risk Assessment & Treatment** to determine control measures appropriate to the risk levels.
- **Preparation/Review of Policies, Standards, Procedures, Work Instructions** to ensure they are clear, auditable, and aligned with actual operations.
- **Strengthening Access Control** through IAM/MFA frameworks, the principle of least privilege, and periodic access reviews.
- **Incident Management**, including guidelines for incident logging, root cause analysis, establishing corrective/preventive action plans, and following up on issue closure.
- **Awareness & Training** to ensure that employees understand their roles, responsibilities, and information security guidelines.
- **Internal Audit & Management Review** to evaluate the adequacy of controls and establish continuous improvement plans.
- **Supplier & Third-Party Security Management** by assessing risks and defining appropriate information security requirements.

Certification Plan

The company aims to achieve **ISO/IEC 27001:2022 certification within the third quarter of 2026**. The key operational guidelines for 2026 include:

- Closing gaps and enhancing key controls to full completion in accordance with the risk management plan.
- Conducting internal audits and management reviews according to the schedule to verify readiness prior to the certification audit.
- Preparing operational evidence for the Certification Audit and following up on the revisions (if any) until completion.
- Enhancing the measurement and reporting of information security performance to be more systematic in order to reflect control effectiveness and continuous improvement.

Internal control and Conflicts of Interests

The company considers it important to set a standardized internal control system to build acceptance and reliability among shareholders, investors, as well as stakeholders. To help achieve this, it has set up the Audit Committee, an independent committee whose duties are to ensure the accuracy, completeness, and reliability of the company's internal control system and financial reports. The Audit Committee also ensures the efficiency and effectiveness of the internal control system as well as the transparency and accountability of the working system with special regard to conflicts of interests. The Audit Committee meets with the company's management auditors to consider and make recommendations regarding improvement of the company's internal control system.

In addition to this, the company has set up the Internal Audit Department, which is an independent unit reporting directly to the Audit Committee. The Internal Audit Department duties are to examine the various work systems to ensure that they operate appropriately and in accordance with related rules, regulations, and laws. It then reports the investigation results to the Audit Committee as scheduled in the annual plan.

In 2025, the Audit Committee and the Board of Directors evaluated the company's internal control and opined that the internal control is sufficient. In the Board of Directors' meeting No. 1/2569 on 26 February 2026, the Board of Directors evaluated the company's internal audit system from the report of the Audit Committee and concluded that the company has enough internal control in 5 factors: control environment, risk assessment, control activities, information and communication monitoring.

Currently, the head of internal audit team is Miss Sunan Wongmutthavanich. She is the Director of Internal Audit Department. In year 2025, the Internal Audit Department performed the audit smoothly and completely according to audit plan which approve by the Audit Committee.

Policy on Reporting Interests of Directors and Executives

Stars Microelectronics (Thailand) Public Company Limited (the "Company") requires directors, executives, and related persons to report their interests concerning the management of the company and its subsidiaries in accordance with Section 89/14 of the Securities and Exchange Act B.E. 2551 (2008) and the Securities and Exchange Commission Announcement No. TorJor. 2/2552 regarding the reporting of directors', executives', and related persons' interests. The Board of Directors are designated to determine the guidelines and methods for such reporting as follows:

Directors, executives, and related persons must report their interests to the company using the "Declaration of Directors' and Executives' Interests Form" (as attached) within the specified timeframe:

- Initial Report: Within 15 days from the date the Board of Directors approves the criteria and reporting methods of the Directors' and Executives' interest.
- Report of Changes in Interests: Within 3 business days from the date of any changes, specifying the number of sequences for that change.

The Company Secretary is designated to be responsible for maintaining records of directors' and executives' interest reports and submitting copies to the Chairman of the Board and the Chairman of the Audit Committee within 7 business days of receiving the report. Furthermore, the disclosure of directors' and executives' interests must be included in the company's annual report (One Report).

Prevention of involving in corruption.

The company assigns the Risk Management Committee to take responsibility for evaluating risk of corruption constantly. The RCM evaluates, reviews and improves the measures against corruption and report to the company's Board of Directors to

In order for the operation of Stars Microelectronics (Thailand) Public Company Limited to be in line with good governance and ethics of the Responsible Business Alliance (RBA) and to be in line with international standards against corruption, the company has set the policy against fraud and corruption. The company has announced the policy as the guideline of practice for management team and employees as follows.

1. The company never accepts gifts, fraud or any benefit, which aims to persuade any action unlawfully.

2. The company has ethics and determination to prevent any fraud and set the guidelines for practice against corruption. The company investigates and reviews the guideline on a regular basis.

3. The management team and employees are responsible for preventing any fraud. If any inappropriate conduct is found, they must report to the supervisor by letter via suggestion boxes in the company's canteen.

4. External persons, who find that there may be any fraud or any acts that may lead to illegal matters, can inform the company via email : complainbox@starsmicro.com

5. The company guarantees the safety for anyone who reports any misconduct and will assign an officer to investigate every matter. The company will treat each matter as highly confidential.

Direction of evaluation in line with the direction of corruption prevention.

The company has set the direction as follows:

1. Executives and employees must act and evaluate themselves according to the direction of the business ethic of the company, code of conduct and code of conduct of RBA (Responsible Business Alliance) announced by the company and international standard of corruption prevention.
2. The Risk Management Committee must evaluate the risk of corruption and gathers important issues to present to the Audit Committee and the Board of Directors.
3. The Audit Committee and the Board of Directors must investigate, order to correct and assign the Risk Management Committee to follow up and report continuously.
4. In 2025, The Company has communicated and provide training to employees on corruption prevention including related policies on an ongoing basis including business ethics and gift acceptance policy continually.

In 2025, the company had no penalties nor was any fraud found. Due to the company's good governance, no non-executive company directors resigned. In addition, the company directors' monitoring and follow-up resulted in no acts which have damaged the company's reputation.

In 2025, the company had no any complaint about human rights violation from employees, business partners and neighboring communities. Which the company will encourage employees and executives adhere to universal human rights principles Continuously.