ESG Review

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

GOVERNANCE

HEINEKEN Malaysia maintains a governance structure rooted in ethical conduct and accountability, fostering integrity across all levels of the organisation. These principles guide our daily operations, from frontline employees to senior leadership, ensuring operational excellence, ethical sourcing and supply chain integrity. Together, we build trust and encourage responsible corporate leadership which is essential for success in the competitive brewing industry.

Material Sustainability Matters

2 Regulatory Compliance

4 Corporate Governance and Anti-Corruption

8 Data Privacy and Cybersecurity

10 Risk Management

Key Highlights

ZERO
substantiated non-compliance incidents with applicable laws or regulations

ZERO
substantiated complaints concerning breaches of customer privacy and losses of customer data

100%
employees underwent training on anti-bribery and anti-corruption

Corporate Governance and Anti-Corruption

Legal compliance and ethical conduct are central to HEINEKEN Malaysia's governance and anti-corruption efforts. To maintain the highest standards of integrity and transparency across our operations, the Group maintains the following codes and policies.

HEINEKEN Code of Business Conduct (HeiCode)

The HeiCode was updated in 2023 to address evolving business needs and emerging challenges. Organised into four key areas – Caring for People and Planet, Maintaining Business Integrity, Protecting our Assets and Engaging Responsibly – the revised Code has been enhanced to clarify critical issues, including harassment and corruption. Regular reviews ensure its continued relevance and support our industry leadership. Compliance is mandatory, and violations may result in disciplinary action, termination of employment, or legal action where appropriate.

To read the HeiCode, please visit https://www.heinekenmalaysia.com/corporate-governance/

ESG Review

HEINEKEN Policy on Bribery

Our anti-bribery policy maintains a firm stance against bribery and corruption. We ensure full legal compliance, implement robust internal controls, offer periodic training and promote a culture of integrity and transparency to maintain the highest ethical standards across our operations.

ZERO
incidents of corruption reported

100%
Board members and employees received anti-bribery and anti-corruption training

HEINEKEN Speak Up Policy

As part of the Speak Up Policy, we provide a confidential reporting channel for our employees and stakeholders to report their concerns regarding unethical practices. Reports can be submitted online or by phone and are managed by an independent third party under the oversight of the HEINEKEN Global Integrity Committee. The Speak Up Policy ensures confidentiality for those reporting misconduct, including cases of fraud, corruption, harassment or discrimination. This service operates on a 24/7 basis, providing timely responses to all concerns.

14
reports received via Speak Up Channel

100%
cases resolved successfully

NONE
of the Speak Up cases has caused any material financial impact to the Group

HEINEKEN Policy on Fraud

Recognising the significant financial and reputational risks posed by fraud, we have a Fraud Policy that clarifies what constitutes fraudulent activity and provides guidance for its identification and mitigation. Maintaining transparency, accuracy and completeness in all records, both financial and non-financial, is essential for mitigating these risks and upholding stakeholder confidence.

Fully implemented
fraud risk assessments

Risk Management

The Group has established a comprehensive system of risk management and internal control, drawing from the COSO Enterprise Risk Management and Internal Control Reference model which is a key component of our HEINEKEN Business Framework.

The HEINEKEN Risk Management Framework (RMF) provides guidance for identifying and mitigating risks.

Type of Risks	Our Actions
Responsible Commercial Communication	
Risk of adverse public reaction to external communications/activities and potential change in regulations.	▪ Managed external activities and communications across commercial teams. ▪ Stepped up communications to enhance the Group's reputation. ▪ Corporate Affairs and Marketing teams explore partnership with Grab Malaysia for responsible consumption campaigns. ▪ Introduced a new responsible marketing code e-learning in FY2024. ▪ Engaged key government stakeholders on the Group's socio-economic contributions and corporate responsibility activities.

ESG Review

Type of Risks	Our Actions
Safety	
Uncontrolled events which lead to serious injuries or fatalities impacting the communities, potentially followed by business disruption, losses, reputational or legal claims.	▪ A safety workshop was conducted with the Management Team. ▪ A fire drill alongside an emergency evacuation drill for a chemical leak, was conducted in Sungei Way Brewery in collaboration with the Fire and Rescue Department (BOMBA). ▪ A driving restriction hour was imposed for the commercial team. Additionally, mandatory safety e-learning sessions, focusing on LSC, were rolled out across the organisation.
Non-Compliance with Environmental Regulations	
Occurrences of excessive waste, pollution, or any other non-compliance with legal and regulatory requirements or stakeholder expectations may result in legal claims, reputational damage, or the revocation of the operational license.	▪ Upgraded the Wastewater Treatment Plant with the employment of qualified personnel. ▪ Completed the inspection and repair of underground drainage in 2021. ▪ Proactive measures were taken to minimise the volume of scheduled waste within the brewery.
Violation of Human Rights	
Significant alleged or actual non-compliance with the Human Rights policy arising from our business activities within our operations or value chain, may result in claims, fines and reputational damage.	▪ Adopted the HeiCode e-learning initiative to enhance awareness of human rights issues. ▪ Spot checks on contract workers' payroll are conducted by the People Function and Internal Audit Department to ensure compliance. ▪ The annual Control Self-Assessment conducted on internal controls related to human rights has been rated effective.
Cyber Security Incident	
Cyber-attacks targeting the Group for the purposes of disrupting, disabling, destroying or stealing its critical data leading to potential loss of intellectual property, fines, legal expenses, loss of public confidence, business disruption, reputational damage, financial losses and loss of our license to operate.	▪ Implemented the HEINEKEN Global Cybersecurity Framework, including firewall, network and security operations centre. ▪ Adopted the HEINEKEN Information Security Maturity Assessment Framework as part of the internal controls to protect and detect threats against information systems, with quarterly assessments conducted to evaluate the effectiveness of the Group's information security management system and cyber security measures. ▪ Conducted monthly scanning of applications through the HEINEKEN Global Information Security vendor. ▪ Launched the annual Cybersecurity Awareness programme. ▪ Launched Cyber Security e-learning to raise awareness. ▪ Conducted a Cyber Crisis Preparedness tabletop exercise.
Sustainability Goals	
Failure to fulfil BaBW's goals could result in substantial damage to our reputation and heightened scrutiny of our sustainability programmes.	▪ A sustainability governance structure is in place. ▪ Management Team and the Board are updated quarterly on sustainability progress. ▪ Non-financial reporting controls have been implemented since 2022 to track our progress and achievements of the BaBW goals.
Sustainability Disclosures	
Inaccurate reporting or unbalanced disclosure of non-financial indicators and BaBW goals could undermine transparency and accountability.	▪ Proactive measures were taken to mitigate the risks associated with the goals of BaBW. ▪ Consultants have been appointed to benchmark the standards, with the process currently ongoing.
Data Breach	
Accidental or deliberate loss of sensitive or critical data leading to fines, brand damage, adverse media exposure, loss of customer confidence and possibly loss of revenue.	▪ Reviewed data and reporting system access controls. ▪ Assessed the detection of unauthorised file transfer. ▪ Modified Access Profiles for production interfaces. ▪ Activated a phishing campaign across the organisation to enhance awareness of phishing and its attack methods with a 1.22% click rate recorded. Digital and Transformation team will continue to run this campaign to increase awareness. ▪ Recognised an opportunity to address potential consumer data leakage, safeguarding our reputation. ▪ Monitored Data Privacy regulation to embed compliance in SOPs.

ESG Review

Type of Risks	Our Actions
Disruption of Sourcing Continuity	
Adverse change or high volatility in currency rates leading to deterioration of revenues and/or increase in input costs and reduced margins and/or liquidity.	▪ Continued to manage the Group's foreign currency exposures and align with HEINEKEN Global on hedging strategies and requirements.

Data Privacy and Cybersecurity

We prioritise the protection of both personal and business data to maintain trust and meet regulatory requirements. Safeguarding this information minimises the risk of data breaches, preserves our reputation and strengthens relationships with clients, enabling continued operational performance and compliance.

In compliance with the Personal Data Protection Act (PDPA) 2010, our Privacy Policy governs data management activities across the Group. The HEINEKEN Information Security Maturity Assessment (ISMA) framework, now known as Security Control Effectiveness Assessment (SCEA), was established by Heineken N.V. in compliance with the NIST Cybersecurity Framework. The NIST Cybersecurity Framework (CSF) is a set of guidelines developed by the U.S. National Institute of Standards and Technology (NIST) to help organisations manage and mitigate cybersecurity risks. All this information is stipulated in the HEINEKEN Cyber Security Policy. The framework is designed to fortify our information systems against potential threats. The efficacy of our cybersecurity risk management measures and the robustness of our information security management system undergo quarterly assessments through the SCEA evaluations.

ZERO

substantiated complaints concerning breaches of customer privacy and losses of customer data

In FY2024, all employees completed mandatory training through the Data Privacy e-learning course to strengthen their cybersecurity awareness. To further enhance vigilance, a series of simulated phishing email exercises were conducted, focusing on recognising phishing tactics and attacks. Additionally, we engaged external specialists to perform network penetration tests, simulating real-world cyberattacks to identify vulnerabilities in our computer network. These tests not only help pinpoint weaknesses but also offer valuable recommendations for improving our security measures.

Data Security Measures in 2024

- Email Phishing Exercise
- Disaster Recovery Drill for Production Systems
- SCAM ME - QR Phishing Campaign
- Physical Cyber Security Training with Live Hacking Demos
- Secure Brew - Cyber Security Newsletter
- Cyber Security Awareness Day
- Continuous Education on WhatsApp Phishing Scam Alert
- Phishing Recognition Game 2.0
- Security Awareness Training 2024
- How to Identify Phishing Attacks Training