Motus

Business conduct management approach

Supplement of the ESG report
for the year ended 30 June 2025

For Motus, integrity means always acting with honesty, fairness and transparency; conducting our business with diligence; and respecting each other, our customers, original equipment manufacturers, suppliers and other stakeholders as well as the communities in which we operate.

Priorities

Ethics

Our board-approved Code of Ethics and governance structures set the standard of ethical conduct that we expect from our board members, employees, suppliers and service providers. The Code and our leaders, standard operating systems and Group values guide employees on how to exercise good judgement and obtain advice on appropriate business conduct. Business segment and regional CEOs and management are responsible for ensuring that our employees are aware of the Group's commitment to acting with integrity.

Our ethical promises

Nothing but the truth

- Create an environment where honesty and accountability flourish and compliance is a central focus.
- A commitment across the Group to maintain the highest ethical standards in all business dealings.

Everyone, everywhere

- Every employee representing or working for the Group is expected to follow the Code of Ethics at all times.
- All persons, including service providers, sub-contractors and business partners, are required to act consistently with the Code of Ethics when acting on the Group's behalf.

Higher standards for managers

- All managers have additional responsibilities to create an open environment in which employees feel comfortable to ask questions, raise concerns and report misconduct.
- Leaders with integrity are valued.

We are a member of the Gordon Institute of Business Science Ethics and Governance Think Tank in South Africa (SA), which gives us access to thought leadership on ethics management.

Training and awareness

Ethics training is delivered online and is included in our induction and Financial Intelligence Centre[1] (FIC) education and training. This training is also provided to our YES learners[2] who make up a large part of our non-permanent workforce in SA. Ethics training is mandatory for all employees in SA who have access to a computer and will be made mandatory for those who do not have electronic access in 2026.

[1] *The FIC is SA's financial intelligence unit, mandated to assist in identifying the proceeds of crime, and in combatting money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction, thereby helping to make the country's financial system intolerant to abuse.*

[2] *Youth Employment Service – a national youth employment drive in SA.*

Training and awareness is delivered on the following:

- The content and principles of our Code of Ethics.
- How to responsibly use the Motus whistle-blowing hotline (see page 3).
- The Ethics Self Declaration Programme implemented in SA (see page 4).
- Motus' anti-bribery and -corruption policy.
- Regulatory compliance and the associated obligations placed on the Group and employees as individuals.
- Emerging industry trends and upcoming regulatory changes.
- Competition Act.
- The Protection of Personal Information Act (POPIA) and the due care required when processing personal information.
- Cyber resilience, information security and protecting the Group's assets.

Priorities (continued)

Fraud prevention

Unethical and fraudulent behaviour is not tolerated. On becoming aware of an incident of fraud and/or corruption, every employee is required to immediately report it to their management team. Decisive action is taken when misconduct is brought to our attention. All confirmed incidents of fraud are reported to the relevant authorities. Where appropriate, resources are provided to support the criminal prosecution process.

The four pillars of our fraud prevention framework

1 **Governance**
- Policies.
- Defined roles and responsibilities.

2 **Prevention**
- Fraud and ethical conduct assessments.
- Controls.
- Awareness.
- Employee screening.

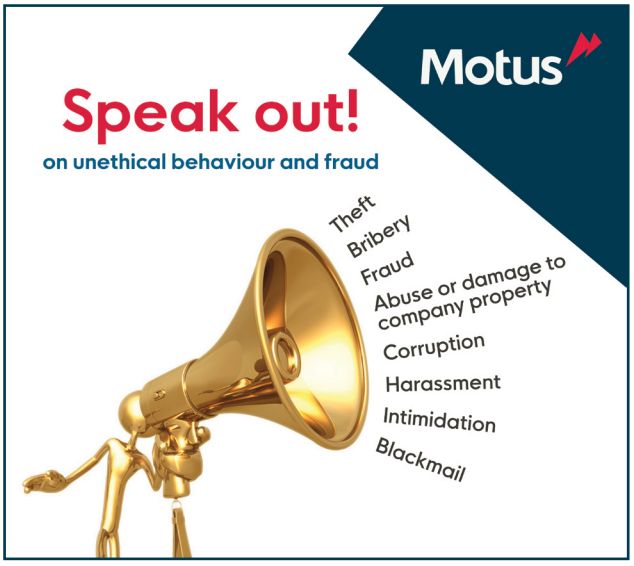
3 **Detection**
- Monitoring customer and supplier transactions.
- Whistle blowing.
- Data analysis.

4 **Response**
- Investigations.
- Legal counsel.
- Regulators.
- Disciplinary and remedial action.

Whistle blowing

All reports of alleged misconduct and non-compliance are taken seriously, investigated and resolved in line with our internal policies. This applies to tip-offs received through the whistle-blowing hotline, other reporting mechanisms and incidents reported to management or received through any other compliance oversight channel. Reports are closed only after having been discussed with the appropriate managers. Where we identify weakness in our controls we take corrective actions to strengthen our systems and processes. Concerns relating to unlawful, dishonest, disrespectful and environmentally unfriendly behaviour can be reported.

An independently managed whistle-blowing hotline (Tip-Offs Anonymous) for our African operations supports anonymous reporting by all stakeholders. Additional anonymous reporting mechanisms for employees include Safecall in the United Kingdom (UK) and the Speeki app and website in Australia.



Available
24 hours a day, 365 days a year

Hotline details (Africa)
Tel: 0800 666 005
Email: motus@tip-offs.com
Website: www.tip-offs.com

Safecall details (UK)
Tel: 0800 915 1571
Website: www.safecall.co.uk/report

Speeki app (Australia)
Download the Speeki mobile app from the Apple App, Google Play or Microsoft stores.

Priorities (continued)

Conflicts of interest

The declaration of interests is a standing board and sub-committee agenda item, ensuring that any declarations relating to topics discussed in the meeting are recorded. The register of interests is shared with directors quarterly before every board meeting to allow directors sufficient time to consider and confirm its accuracy and/or make amendments, where necessary.

Select employees in SA annually self-declare conflicts of interest and their compliance with key policies and ethical standards. This online Ethics Self Declaration Programme applies to the Group's Code of Ethics, anti-bribery and -corruption policy, conflicts of interest policy, supply chain code of conduct, and policy statement on relationships in the workplace. The process allows participants to raise matters of non-compliance and ask for policy training for themselves. The programme applies to all Group Executive Committee members and their direct reports (business segment and regional executives), and employees in certain roles, for example, all employees working in our financial service provider (FSP) businesses. Where the completion rate of the programme falls below 90% for an employee group, additional awareness and training is conducted.

In the UK and Australia, conflicts of interest are reported at divisional meetings.

An online Gifts and Conflicts of Interest Register (accessible on personal computers and mobile phones) makes it easy for financial directors in SA to authorise employee declarations of gifts and conflicts.

Human rights

We stand against all forms of human rights abuse. We adhere to the principles embodied in the Universal Declaration of Human Rights, the South African Constitution and the International Labour Organization's Declaration on Fundamental Principles and Rights at Work. We expect our employees to work together free from incidents of harassment and discrimination, regardless of identity or position. In line with regulatory requirements, we provide an annual anti-modern day slavery statement on our website in the UK, and in Australia, we report annually against the requirements of the Modern Day Slavery Act.

We reserve the right to terminate or re-negotiate agreements and relationships with suppliers who contravene international human rights standards.

Supply chain

Our original equipment manufacturers (OEMs) and suppliers are required to adhere to our Code of Ethics, supply chain code of conduct (adapted for each region) and all applicable laws and regulations in all jurisdictions of operation. When local legislation is lower than the international standards outlined in the supply chain code of conduct, suppliers are required to adopt the higher standards.

The supply chain code of conduct outlines our requirements for procedural compliance, social and environmental stewardship, guarding against bribery and corruption, conflicts of interest and fair business practices. Suppliers are expected to prevent any contravention of human rights, ensure that there are no discriminatory practices in their organisations, employ practices that reduce health and safety risks as far as reasonably possible, and prevent or mitigate environmental impacts that their business activities may cause or contribute to, or which may be directly linked to their operations, products or services by their business relationships.

We reserve the right to audit suppliers, whether by an internal team or a third party, to verify conformance to the supply chain code of conduct. However, the assessment of suppliers on their compliance with our code of conduct, regulatory compliance and environmental, social and governance (ESG) performance is limited.

Aftermarket Parts has access to Nexus' supplier vetting service for both current and new suppliers. This service includes audits on supplier standards, specifications and processes aligned with European Union (EU) standards, covering labour legislation, health and safety, and corruption. While the business segment's use of this service is limited, a start has been made in assessing non-OEM parts manufacturers in SA on their contractual liabilities and responsibilities and their maturity in terms of managing their ESG-related risks.

Furthermore, social, environmental and fair economic business principles are considered in our business award decisions both for new and existing suppliers. For example, in SA, broad-based black economic empowerment compliance and/or contribution to enterprise and supplier development are additional criteria considered in supplier selection.

Priorities (continued)

Regulatory compliance

The Group's businesses are responsible for ensuring compliance with all regulation applicable to their operations, as well as our adopted non-binding codes and standards. This includes engaging with, and marketing to, customers in compliance with legislative requirements. When making acquisitions, regulatory compliance is a key part of the due diligence process.

Our risk management and compliance programmes, applicable to all FSPs and entities deemed to be high-value goods dealers[1] in SA, set out our customer due diligence processes, which include controls to guard against money laundering and terrorist financing.

Among our tools to ensure compliance, is the quarterly regulatory compliance self-assessment in SA. The tool gauges the level of knowledge and understanding of, and compliance with, key legal and regulatory requirements associated with newer legislation. Each business segment responds to a bespoke question-set on the laws that are applicable to it. The feedback supports the development of targeted training and awareness initiatives per business segment that is more effective than the blanket roll out of generic training.

Employees who fail to adhere to our policies and controls face appropriate disciplinary action.

We regularly scan the regulatory horizon to identify upcoming changes that may impact the Group and to understand the extent of their impact. We update the Group's compliance universe on an ongoing basis, ensuring that we have a complete view of the key legislation that impacts each business segment and regional operation, and that responsibility for compliance has been assigned without creating duplication of effort.

Regulated products and services

Our FSPs are subject to a professional code of conduct when giving advice or providing intermediary services to customers of certain financial products. We regularly review our processes and policies relating to regulated products and services to ensure that commissions and disclosures are transparent in the sales process. Our call centres are subject to quality assurance assessments. External advisors are engaged, if necessary, to ensure that all regulated products and services comply with applicable legislation.

The Financial Sector Conduct Authority (FSCA) in SA, and the Financial Conduct Authority (FCA) in the UK, assess our compliance to their 'fit and proper' and certification requirements. All employees who are subject to 'fit and proper' requirements receive training and continuous professional development to maintain their accreditation to advise on and offer intermediary services. Our insurance partners train and examine our insurance product representatives before they are allowed to sell these products.

In SA, F&I Management Solutions (FAIMS) provides finance and insurance (F&I) services to our retail dealerships, and limited services to select non-Motus independent dealerships. Every deal transaction file for a vehicle sale must contain several key documents. As part of its licence conditions, FAIMS is required to conduct at least one audit for every F&I business manager annually, during which FAIMS also audits a sample of deal transaction files. Similar processes are in place in the UK.

In the UK, the FCA's Consumer Duty aims to create a higher standard of care from regulated organisations, placing a duty on our F&I managers to ensure good customer outcomes (providing the right information about financial products and the people and institutions involved). The Consumer Duty holds boards, or the equivalent, responsible for assessing whether an organisation is delivering good customer outcomes. An internal report on Consumer Duty is provided to the UK operation's board quarterly.

As part of our Point-of-Sale Agreement[2] in Australia, the financial services institutions to whom we are contracted are responsible for ensuring that our F&I team is appropriately trained, accredited and up to date with the latest legislation and regulatory requirements, including those related to combatting money laundering, terrorist financing and fraud, and ensuring privacy and responsible lending.

The above mentioned audits, self-assessments, processes and reports help us identify any gaps with compliance and assign accountability for remediation, providing the board and executive committees with the assurance that business sites are compliant with legal and regulatory requirements.

Stakeholder engagement

Our business forum and industry association memberships are critical to understanding how changing regulations will impact the Group and our industry, and what we need to change to comply. We actively participate in regulatory consultation processes, either directly or through our memberships, to comment on, and contribute to, the shaping of automotive policy and proposed regulatory changes, and to explore possible solutions where uncertainties exist.

Global FX Code

The Global FX Code is a set of global principles (55 in total) developed to promote the integrity and effective functioning of the foreign exchange market. Motus is a signatory to the Code and complies with all 27 of the principles that are applicable to the Group.

Political contributions

The Group does not make contributions to political parties.

[1] *High-value goods dealers are defined as entities that sell goods that are valued at over R100 000.*
[2] *Point-of-Sale exemption means that our Australian F&I teams do not fall under the direct licensing or scope of the regulator.*

Priorities (continued)

Systems and information security

We align with COBIT[1], an international framework and best practice for developing, implementing, monitoring and improving IT governance and management practices to ensure that the Group IT strategy aligns with business goals, delivers value and manages risks effectively. In parallel, we adopt the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, an internationally recognised standard that supports ethical, transparent and effective management of cyber risks and data protection. This combined approach ensures that we invest in the most relevant security controls for our systems, critical infrastructure and end user devices and comply with regulatory, audit and customer data protection requirements, including those of POPIA[2] and the EU's General Data Protection Regulation.

Our cybersecurity and data protection processes are aligned with the Group's integrated risk management framework and business continuity planning. We prioritise realistic, business-relevant safeguards based on risk likelihood and impact. We protect our data and systems against the risks associated with data compromise, IT system abuse and fraud and/or cyber-extortion.

Employees play a vital role in protecting our systems and data. We aim to promote a culture of security and shared responsibility across the Group, providing employees with regular cybersecurity and data protection training, tailored to their responsibilities. This includes guidance on safe data handling, password management, phishing awareness and the requirements of POPIA.

Cybersecurity

Our multi-faceted cybersecurity framework supports our commitment to responsible business conduct and encompasses people, processes and technology. We invest in advanced cybersecurity applications and our alignment with the NIST Cybersecurity Framework provides a practical reference for identifying, protecting, detecting, responding to and recovering from cyber threats.

The Group-wide Information Security Management System (ISMS) provides the foundation for systematically managing cybersecurity risks. This governance tool ensures that we implement, monitor and continually improve our cybersecurity controls to limit the impact of potential threats. The ISMS encompasses independent reviews, ongoing risk assessments, adherence to established guidelines, robust monitoring and regular testing of our incident response capabilities as well as targeted initiatives in high-risk areas such as dealerships and customer-facing platforms. Our incident response process focuses on clear escalation paths, rapid containment and cross-team co-ordination. While we follow NIST guidance, we have adapted our response process to suit operational realities.

We also use BitSight cyber risk assessment tools to identify potential exposures, prioritise investments and communicate transparently with stakeholders, thereby strengthening accountability and protecting our expanding digital ecosystem.

Additional measures to safeguard the Group include quickly integrating acquisitions into our high standards of information security, strictly enforcing the separation of work and personal devices, and rigorous IT security screening of potential service providers to ensure that they share our commitment to strong cybersecurity practices.

We work closely with cybersecurity specialists to remain vigilant against evolving threats, enhance our expertise and reinforce our security posture. Where feasible, threat intelligence is shared across the Group and with our trusted partners, reflecting our belief in collective responsibility for cyber resilience.

[1] *Control Objectives for Information and Related Technologies.*
[2] *POPIA promotes the protection of personal information in line with international standards. It covers individuals and business clients, and limits the rights of businesses to collect, process, store and share personal information. It also makes businesses accountable for protecting the privacy of this information.*

Priorities (continued)

Data protection

Protecting personal and sensitive information is a business priority for Motus. As technology evolves, we remain committed to safeguarding the data of our customers, employees and partners through a combination of governance, risk management and employee awareness.

Our data protection policies ensure that we maintain strict compliance with data privacy regulations. They align with the NIST Cybersecurity Framework, which covers the secure handling, storage and disposal of personal information. Policies are reviewed and updated to reflect regulatory changes and changes in the risk landscape. Best privacy practices are embedded in the design specifications of systems and business processes. This includes conducting privacy impact assessments before launching new systems or enhancing existing ones.

Responsibility for protecting information rests with every information owner and user within the Group. Employees are bound by confidentiality to the extent permitted by law. We ensure that they have the right level of access to the information needed to do their work and meet customer expectations.

Effective personal computer encryption, software updates and end-of-life processes (governed by an equipment disposal policy) are key priorities for the Group. We also work with technology and financial partners as well as independent advisors to develop integrated data security solutions.

Data privacy and protection clauses along with security assessment criteria, are incorporated into our service provider contracts, covering their connection and access to our systems and their compliance with POPIA. Where contractual documents are deemed inadequate, third parties are required to sign a data processing and transfer agreement that complies with POPIA requirements. We ensure that agreements with IT vendors are well-defined and our expectations are well-understood.

We report annually to the Information Regulator in SA on our compliance with the Promotion of Access to Information Act.

Artificial intelligence

Our policy on the acceptable use and governance of AI covers ethical aspects, including confidentiality, copyright, regulatory compliance and security risks. It requires our IT security and legal and compliance functions to review all AI-enabled systems prior to utilisation.

Governance and management framework

Key internal frameworks and policies

- Ethics and fraud prevention framework.
  - Code of Ethics.
  - Group anti-bribery and -corruption policy.
  - Conflict of interest policy.
  - Supply chain code of conduct.
- Artificial intelligence policy.
- Policies relating to modern day slavery (UK and Australia).
- Data protection framework, including numerous cyber- and POPIA-related policies, standards and procedures.
- The Promotion of Access to Information Manual for SA.

Board oversight

- **Social, Ethics and Sustainability (SES) Committee:** ethics and compliance matters and data privacy.
- **Audit and Risk Committee (ARC):** compliance matters, IT incidents, data protection and cybersecurity.

Management oversight

- Group Executive Committee.
- Finance and Risk Review Committees (FRRCs)[1].
- IT Executive Committee.
- Chief Information Officer (CIO) Forum.
- Group IT Security Steering Committee.
- UK Regulatory Compliance Committee.
- Group legal and compliance function.

Operational teams

- Business segment and regional legal and compliance teams.
- Protection of personal information working group (SA).

[1] *FRRCs are in place for all Import and Distribution businesses, SA Retail, UK Retail, Australia Retail, SA Vehicle Rental, Mobility Solutions, SA Aftermarket Parts and International Aftermarket Parts.*

Compliance

In SA, the Group centralised legal and compliance function as well as business segment and divisional legal and compliance departments oversee and monitor our FSPs, where compliance risk is high. Our compliance programmes are driven by dedicated compliance officers. At Mobility Solutions, including FAIMS, all managers and key individuals attend monthly compliance meetings. In the UK, the governance of F&I products is the responsibility of a specialist compliance sub-committee of the FRRC, which meets quarterly.

Incidents of non-compliance are escalated to senior management and reported to the relevant management and board committees, including the FRRCs.

Systems and information security

Our governance structures are designed to ensure sustained visibility and accountability for cyber and data-related risks. Group IT, under the leadership of the Group's CIO, is responsible for the Group-wide cybersecurity framework and governance, and oversees the Group's IT infrastructure, shared applications and compliance with data protection and cybersecurity policies and standards. A dedicated Chief Information Security Officer (CISO) oversees our multi-faceted cybersecurity framework. Business segment CIOs in SA, the UK and Australia ensure adherence to Group standards and governance processes, while overseeing their respective IT operations. Oversight is reinforced through the Group IT Security Steering Committee, chaired by the CISO.

Each business segment and regional operation reports to the centralised Group IT function, which oversees Group-wide trends and identifies areas of concern. A consolidated IT report, including reports from the CISO, is submitted quarterly to the CIO Forum, FRRCs and ARC.

In SA, the Group's Privacy Officer/Information Officer, supported by the protection of personal information working group and information officers from each business segment, oversees the implementation of the Group's data protection framework. All information officers are registered with the Information Regulator in SA and participate in monthly compliance meetings. In the UK and Australia, matters relating to data protection are reported to regional CEOs.

How we measure our performance

	Key metrics and aspects	Highest level of oversight	Frequency
	Ethical business conduct		
Group	• Ethics, compliance and human rights risks	Internal audit	Three-year rolling cycle
	• Whistle-blowing reports	Board	Quarterly
	• Employees' perception of integrity, honesty and transparency at Motus	Board and/or internal review	Ad hoc employee engagement surveys
	F&I compliance audits and self-assessments		
Group	• Audit scores and incidents of non-compliance	Board	Quarterly
SA	• Business manager and deal transaction file audits	FAIMS internal audit	At least once a quarter (random)
	• LiquidCapital and MotorHappy audits	Mobility Solutions internal audit	Monthly
	• M-Sure audits	Insurer	Regularly
UK	• Regulated consultant and manager self-assessments	FRRC	Every six months
	• Regulated consultant, manager, dealership and deal transaction file reviews	Insurer	Quarterly
Australia	• Dealership audits	External FSP	Regularly
	Systems and information security		
Group	• Protection of personal information	Internal audit	Three-year rolling cycle
	• Data breaches	Board	Quarterly
	• Cybersecurity measures	Independent assessment Internal assessment	Twice a year Quarterly
	Customer satisfaction		
Group	• Ombudsman reports	Board	Quarterly

Review of 2025 business conduct performance

2025 ESG report.

2025 Integrated report.