



Motus 

Business conduct impact
management approach 2023

Business conduct management approach

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

Our priorities

Ethics management

Divisional CEOs and management are responsible for ensuring that our employees are aware of the Group's values, Code of Ethics and commitment to acting with integrity. Our Code of Ethics, leaders, standard operating systems and Group values guide employees on how best to exercise good judgement and obtain advice on appropriate business conduct, when needed.

Unethical and fraudulent behaviour is not tolerated.

The four pillars of our fraud prevention framework include:

- **Governance:** policies, defined roles and responsibilities.
- **Prevention:** fraud and ethical conduct assessments, controls, awareness and employee screening.
- **Detection:** monitoring customer and supplier transactions, whistle blowing and data analysis.
- **Response:** investigations, legal counsel, regulators, disciplinary action and remedial action.

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 matters relating to unbecoming conduct are brought to our attention. All confirmed incidents of fraud are reported to the relevant authorities and, where appropriate, resources are provided to support the criminal prosecution process.

Our ethical promises

<p>Nothing but the truth</p>	<ul style="list-style-type: none"> • 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.
<p>Everyone, everywhere</p>	<ul style="list-style-type: none"> • 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.
<p>Higher standards for managers</p>	<ul style="list-style-type: none"> • 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.

Training and awareness

Our training and awareness initiatives are key tools that help our employees understand the behaviours we expect of them. Ethics training is available online and is included in our induction and Financial Intelligence Centre (FIC) education and training, and extends to YES learners, who make up a large part of our non-permanent workforce. In addition, the Group CEO's leadership presentations remind our leaders of the importance of ethical behaviour.

Training and awareness is delivered on the following issues:

- The content and principles of our Code of Ethics.
- How to responsibly use the Motus whistle-blowing hotline.
- The Ethics Self Declaration Programme implemented in South Africa.
- Our anti-fraud, -bribery and -corruption policies.
- Regulatory compliance and the obligations this places on the Group and employees as individuals.
- Emerging industry trends and upcoming regulatory changes.
- The Protection of Personal Information Act (POPIA) and due care required when processing personal information.
- Cyber resilience, information security and protecting the Group's assets.

Business conduct management approach (continued)

Whistle blowing

All reports of alleged misconduct are taken seriously, investigated and resolved in line with our internal policies. This applies to tip-offs received through the whistle-blowing hotline, reported to management or received through any other compliance oversight channel. Reports are closed only after having been discussed with the appropriate managers.

An independently managed whistle-blowing hotline supports anonymous and confidential reporting by all stakeholders. Concerns relating to unlawful, dishonest, disrespectful and environmentally unfriendly behaviour can be reported without fear of retribution.

Hotline details

Hotline tel: 0800 666 005

Hotline email: motus@tip-offs.com

Additional reporting mechanisms include Safecall in the United Kingdom (UK), for employees to anonymously raise issues of concern with top management, the Speeki app and website in Australia for employees to report anonymously, and a dedicated email address for the Rest of Africa operations, which is directly accessed by the operation's CEO.

Ethics Self-Declaration Programme

Selected employees in South Africa annually self-declare conflicts of interest and their compliance with our policies and ethical standards. The 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 relating to non-compliance and ask for policy training for themselves. The programme applies to all Executive Committee members and their direct reports (Group and business segment executives), and employees occupying certain roles, for example, all employees working in our financial service provider (FSP) businesses. In the UK and Australia, conflicts of interest are reported at divisional meetings.

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.

Sustainability in the supply chain

Our OEMs and suppliers are required to adhere to our Code of Ethics and supply chain code of conduct. The supply chain code of conduct outlines our requirements for procedural compliance, human rights, environmental stewardship, labour practices, guarding against bribery and corruption, conflicts of interest and fair business practices. The supply chain code of conduct is adapted for each region. We reserve the right to audit suppliers, whether by an internal team or a third party to verify conformance to our standards.

Suppliers are expected to comply with all laws and regulations that apply to them in all jurisdictions of operation. When legislation is lower than the international standards outlined in our supply chain code of conduct, suppliers are required to adopt our higher standards. Our suppliers are also 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.

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

Our assessment of supplier ESG performance is currently limited. Aftermarket Parts has access to Nexus' supplier vetting service for both current and new suppliers, which includes audits on their standards, specifications and processes. Vetting is aligned to European Union (EU) standards, and covers labour legislation, health and safety, and corruption. Mobility Solutions' eProcure system, recently implemented, will include a process to onboard and vet new suppliers, including on their management of ethics and responsible sourcing.

Regulated products

Our FSPs are subject to a professional code of conduct when giving advice or providing intermediary services to consumers 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. External advisers are engaged, if necessary, to ensure that all regulated products and services comply with applicable legislation.

All employees in South Africa and the UK who are subject to 'fit and proper' requirements receive the necessary training and continuous professional development to maintain their accreditation to advise on and offer intermediary and binder services. All product representatives are trained and examined before being accredited by insurers to offer products.

In South Africa, the Financial Sector Conduct Authority (FSCA), and in the UK, the Financial Conduct Authority (FCA), assess our compliance to their 'fit and proper' and certification requirements.

In South Africa, our F&I Management Solutions (FAIMS) business, provides finance and insurance (F&I) services to our retail dealerships and limited services to select non-Motus independent dealerships. As part of its licence conditions, FAIMS is required to conduct at least one audit for every F&I business manager annually. In addition, every deal transaction file for a vehicle sale must contain several key documents and be stored on a secure central platform. As part of the F&I business manager audit, FAIMS selects a sample of deal files, which include the F&I sale, to audit for compliance. Similar processes are in place in the UK.

As part of our Point-of-Sale Agreement¹ 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.

Regulatory compliance

All of the Group's businesses are responsible for ensuring that they comply with all regulation applicable to their operations. We invest in the development and implementation of effective action plans that ensure compliance. Employees who fail to adhere to processes and controls face appropriate disciplinary procedures. Non-compliance is escalated to senior management and reported to the relevant management and board committees, including the Finance and Risk Review Committees (FRRCs).

Our Risk Management and Compliance Programmes, applicable to all FSPs in South Africa, set out our customer due diligence processes, which include controls to guard against money laundering and terrorist financing.

We scan the regulatory horizon on an ongoing basis to identify upcoming changes that may impact the Group and understand the extent of their impact.

A quarterly regulatory CSA questionnaire will be launched in 2024 for all South African operations covering FICA, POPIA, the Guidelines for Competition in the South African Automotive Aftermarket and any other key legislation.

Cybersecurity and protection of information

Responsibility for protecting information rests with every information owner and user within the Group. Best privacy practices are embedded in the design specifications of new and existing systems and business processes. This includes privacy impact assessments before a new system or enhancements to an existing system are launched. Effective encryption of personal computers is a key priority for the Group as is reporting on software updates and end-of-life.

Our employees are bound by confidentiality to the extent permitted by law. We ensure that they have the right level of access to the information they need to do their work and meet customer expectations. Data protection awareness programmes are ongoing in the form of training, posters and reminders on computers.

¹ Point-of-Sale exemption means that our Australian F&I teams do not fall under the direct licensing or scope of the regulator.

Business conduct management approach (continued)

Data privacy and protection clauses and security assessment criteria in our supplier contracts ensure that our data management responsibility is extended to third parties, covering their connection and access to our systems. Where contractual documents are deemed inadequate, third parties are required to sign a data processing and transfer agreement that complies with POPIA¹ requirements.

The Group-wide Cyber Resilience and Information Protection Programme complies with international standards and best practice, including POPIA requirements and the EU’s General Data Protection Regulation rules. It ensures that we invest in the most relevant security controls for our systems, critical infrastructure and end user devices, and that we maximise our return on investment and meet regulatory, audit and customer requirements.

We work with technology and financial partners as well as independent advisers to develop integrated data security solutions and reduce cyber risk for our customers and businesses. Our systems and those of our suppliers and partners in the financial services industry comply with POPIA. We ensure that our agreements with IT vendors are well-defined and expectations are well-understood.

We protect our data and systems against the risks associated with data compromise, IT system abuse and fraud and/or cyber-extortion. Other operational security measures include vulnerability assessments, periodic network and application security testing, event monitoring and incident tracking.

Ongoing cyber-threat assessments analyse our cybersecurity controls as well as prevailing industry and regional conditions and threats. Where feasible, threat intelligence is shared across the Group and with our partners.

In the event of a data leak, our systems and data backup and recovery capability ensure business continuity and prevent further exposure.

Our cybersecurity performance is measured against an internationally recognised standard – the National Institute of Standards and Technology cybersecurity framework – similar to ISO27001.



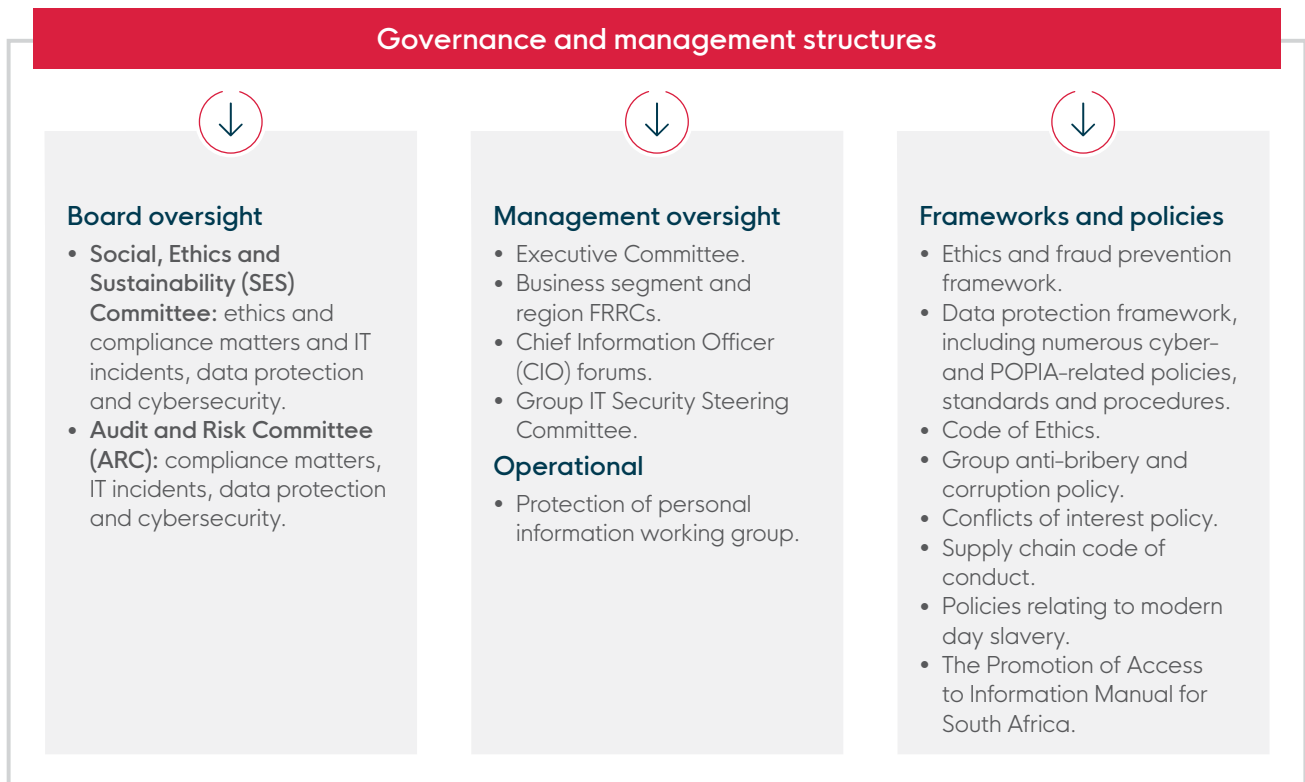
¹ POPIA promotes the protection of personal information in line with international standards. It covers individuals and business clients, and limits the rights of businesses to collect, process, store and share personal information. It also makes businesses accountable for protecting the privacy of this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

Stakeholder engagement

Our memberships in industry bodies and business forums allow us to engage more broadly on key matters such as the detection, monitoring and elimination of corruption, fraud and criminal activities, and are critical to understanding how changing automotive 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 contribute to the shaping of upcoming automotive policy and to explore possible solutions where uncertainties exist.

🔗 Contribute to improving economic and social inclusion: page 100 of the ESG report.

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



In South Africa, a 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, 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.

Group IT oversees the adherence of business segments in South Africa to our data-related policies and standards. Two Chief Information Technology Officers manage a central register of IT incidents, including security incidents. A consolidated IT report for South Africa is produced monthly and submitted quarterly to the CIO Forum, FRRCs, ARC and SES Committee. During the year, we formed a Group IT Security Steering Committee to provide additional oversight.

The protection of personal information working group in South Africa and the Group CIO are responsible for the implementation and management of the Group's data protection framework and are supported by information officers in each business segment. All information officers are registered with and approved by the Information Regulator and attend monthly meetings. The SES Committee and ARC oversee the management of system and data protection.

In the UK, the Head of IT manages the central register of IT incidents, and cyber risks and incidents are reported monthly to the operation's CEO and CFO. All matters in the UK and Australia that relate to data protection are reported to the Group CIO.

Business conduct management approach (continued)

How we measure our performance

Ethical business conduct

Group: compliance, risks relating to bribery and corruption, unethical business practices and human rights, and ethics communication. **Internal audit:** three-year rolling cycle

Group: whistle-blowing hotline reports. **Internal review:** quarterly

Group: employee engagement survey results (all surveys include a question on integrity, honesty and transparency). **Internal review:** when surveys are conducted

Regulated products and regulatory compliance

South Africa: every F&I business manager and a sample of their deal transaction files. **FAIMS internal audit:** at least once every quarter (random without pre-warning)

South Africa: LiquidCapital, MotorHappy and M-Sure. **Mobility Solutions internal audit:** monthly
Insurer audit of M-Sure: regularly

UK: competency of regulated consultants and managers. **Internal assessment:** regularly

UK: regulated consultants and managers, dealership compliance to F&I regulatory requirements and deal transaction files. **Third-party compliance service provider:** regular monitoring

Australia: dealer F&I compliance. **Independent audit:** regularly by the financial service providers

Group: F&I compliance audit scores, and fines or penalties for non-compliance. **Internal review:** quarterly

Data protection and cybersecurity

Group: protection of personal information **Internal audit:** three-year rolling cycle

Group: data breaches (including loss of personal computers or devices with access to personal information) and encryption of personal computers. **Internal review:** quarterly

Group: cybersecurity measures. **Independent assessment:** twice a year
Internal assessment: quarterly

Customer satisfaction and complaints

Group: customer satisfaction survey results on new vehicle sales, workshop servicing and parts. In South Africa, customer satisfaction surveys may be conducted on the sale of pre-owned vehicles. **Internal review:** monthly
Importer OEM assessment: ongoing


South Africa: all cases concerning Motus reported to an ombudsman, including the Motor Industry Ombudsman, the Insurance Ombudsman and the National Consumer Tribunal. **Internal review:** quarterly

Link to remuneration

The short-term incentives of certain executives are linked to the implementation of changes to meet new regulatory requirements impacting the Group.

Review of 2023 performance

 2023 ESG report

 2023 integrated report