



# Motus

---

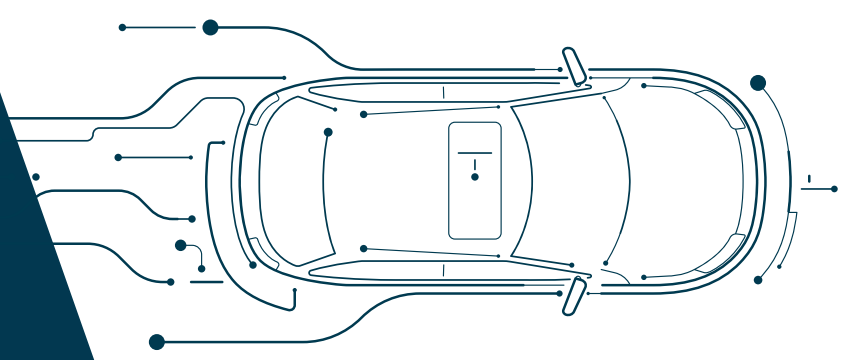
## Business conduct management approach 2024

Supplement of the ESG report for the year  
ended 30 June 2024

# Contents

---

Key business conduct management activities	1
Governance and management structures	5
How we measure our performance	6



# 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, original equipment manufacturers (OEMs), suppliers and other stakeholders as well as the communities in which we operate.

## Key business conduct management activities

### Ethics management

Our Code of Ethics, standard operating systems and Group values guide employees on how to exercise good judgement and obtain advice on appropriate business conduct. Business segment and divisional 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

Our training and awareness initiatives help our employees understand the behaviours we expect of them. Ethics training is delivered online and is included in our induction and Financial Intelligence Centre (FIC) education and training. Ethics and compliance training is also provided to YES learners<sup>1</sup>, who make up a large part of our non-permanent workforce in SA. 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 SA.
- Our anti-fraud, -bribery and -corruption policies.
- Regulatory compliance and the obligations placed on the Group and employees as individuals.
- Emerging industry trends and upcoming regulatory changes.
- 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.

### 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 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.

<sup>1</sup> Youth Employment Service – a national youth employment drive in SA.


# 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, 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. Concerns relating to unlawful, dishonest, disrespectful and environmentally unfriendly behaviour can be reported.

An independently managed whistle-blowing hotline (Tip-offs Anonymous in SA) supports anonymous and confidential 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. For the Rest of Africa operation, a dedicated email address allows employees to report directly to the operation's CEO.

**Hotline details**  
**Hotline tel: 0800 666 005**  
**Hotline email: [motus@tip-offs.com](mailto:motus@tip-offs.com)**  
**Website: [www.tip-offs.com](http://www.tip-offs.com)**



**FreeCall: 0800 666 005**  
**Email: [motus@tip-offs.com](mailto:motus@tip-offs.com)**  
**Website: [www.tip-offs.com](http://www.tip-offs.com)**

FreeCall: 0800 00 77 88 | Freeport: KZN 138, Umhlanga Rocks, 4300

**Deloitte**

## Conflicts of interest

Select employees in SA annually self-declare conflicts of interest and their compliance with key 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 Group 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.

Declaration of interest 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 on a quarterly basis before every board and sub-committee meeting to allow directors sufficient time to consider and confirm its accuracy and/or to amend, where necessary.

We also operate an online Gifts and Conflict of Interests Register that financial directors use 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.

# Business conduct management approach continued

## Sustainability in the supply chain

Our OEMs and suppliers are required to adhere to our Code of Ethics, supply chain code of conduct (adapted for each region) and all laws and regulations that apply to them in all jurisdictions of operation. 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. We reserve the right to audit suppliers, whether by an internal team or a third party, to verify conformance to our standards.

When legislation is lower than the international standards outlined in the supply chain code of conduct, suppliers are required to adopt our higher standards. They 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 SA, broad-based black economic empowerment compliance and/or contribution to enterprise and supplier development are additional criteria considered in supplier selection.

Our assessment of the environmental, social and governance (ESG) performance of our suppliers 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. While the business segment's use of this service is limited, plans are in place to start assessing non-OEM manufacturers from 2025.

## Regulatory compliance

All of the Group's businesses are responsible for ensuring that they comply with all regulation applicable to their operations. Our Risk Management and Compliance Programmes, applicable to all FSPs in SA, set out our customer due diligence processes, which include controls to guard against money laundering and terrorist financing.

We invest in the development and implementation of effective action plans that ensure compliance. Our quarterly regulatory compliance self-assessment questionnaire in SA gauges the level of knowledge and understanding of, and compliance with, key compliance and legal matters. The tool is used to develop targeted training and awareness initiatives per business segment.

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.

## Regulated products and services

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 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 the training and continuous professional development needed to maintain their accreditation to advise on and offer intermediary and binder services. Insurance product representatives are trained and examined before being accredited by insurers to sell these products.

In SA, 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 transaction files to audit for compliance. Similar processes are in place in the UK.

As part of our Point-of-Sale Agreement<sup>1</sup> 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.

<sup>1</sup> 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

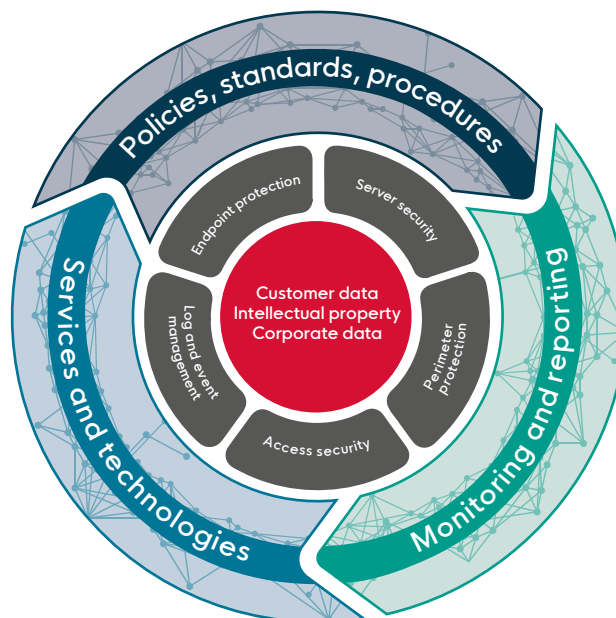
## Stakeholder engagement

Our business forum and industry association memberships 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.

## Securing our information assets

We safeguard our IT operations and environment in line with industry standards, and ensure regulatory compliance through a robust risk management and assessment framework. The Group-wide Cyber Resilience and Information Protection Programme complies with international standards and best practice, including POPIA<sup>1</sup> 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.

### Cyber Resilience and Information Protection Programme



## 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 personal computer encryption, software updates and end-of-life processes 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.

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.

Data privacy and protection clauses and security assessment criteria in our supplier contracts extend our data management responsibility 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 POPIA requirements. We ensure that agreements with IT vendors are well-defined, and our expectations are well-understood.

<sup>1</sup> 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.

# Business conduct management approach continued

## Cybersecurity

We protect our data and systems against the risks associated with data compromise, IT system abuse and fraud and/or cyber-extortion. Our multi-faceted strategy to cybersecurity covers people, processes and technology. We invest in new and improved cybersecurity applications, and adhere to the cybersecurity framework established by the National Institute of Standards and Technology (an internationally recognised standard for combatting cybercrime that is similar to ISO27001<sup>1</sup>). The Group-wide Information Security Management System consists of a set of policies, procedures and operational practices for the systematic management of cybersecurity risk within Motus. It is a critical governance tool to proactively limit the impact of potential cybersecurity breaches, and drives the implementation and continual enhancement of our cybersecurity controls. Our cybersecurity approach also includes external reviews, ongoing risk assessments, adherence to guidelines, and cyber incident monitoring and response capabilities as well as the testing of these capabilities.

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

We engage with cybersecurity specialists to keep abreast of evolving threats, support our cybersecurity initiatives, and enhance Motus' overall security posture over time. Where feasible, threat intelligence is shared across the Group and with our partners.

In the past year, we have also implemented the BitSight cyber risk assessment tools across our platforms. BitSight allows us to identify exposure, prioritise investment, communicate with stakeholders, and mitigate cyber risk to protect our expanding digital ecosystem. Our current BitSight rating exceeds industry standards.

### Governance and management structures

#### Board oversight

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

#### Management oversight

- Group Executive Committee.
- Business segment and region Finance and Risk Review Committees (FRRCs).
- Chief Information Officer (CIO) Forum.
- Group IT Security Steering Committee.

#### Operational

- Protection of personal information working group.

#### Frameworks and policies

- Ethics and fraud prevention framework.
- Code of Ethics.
- Group anti-bribery and corruption policy.
- Conflicts of interest policy.
- Supply chain code of conduct.
- 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.

## Ethics and compliance

In SA, 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.

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

## Securing our information assets

Group IT oversees the adherence of business segments in SA 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 SA is produced monthly and submitted quarterly to the CIO Forum, FRRCs and ARC. The Group IT Security Steering Committee provides an additional level of oversight.

The protection of personal information working group in SA 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 in SA, 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.

<sup>1</sup> ISO27001 – the International standard for information security management systems.

# Business conduct management approach continued

## How we measure our performance

### Metrics and oversight

Metric	Oversight type	Frequency
<b>Ethical business conduct</b>		
<b>Group:</b> compliance, risks relating to bribery and corruption, unethical business practices and human rights, and ethics communication.	Internal audit	Three-year rolling cycle
<b>Group:</b> whistle-blowing hotline reports.	Board review	Quarterly
<b>Group:</b> employee engagement survey results (all surveys include a question on integrity, honesty and transparency).	Internal review	When surveys are conducted
<b>Compliance and regulated products</b>		
<b>Group:</b> F&I compliance audit scores, and fines or penalties for non-compliance.	Board review	Quarterly
<b>SA:</b> every F&I business manager and a sample of their deal transaction files.	FAIMS internal audit	At least once a quarter (random)
<b>SA:</b> LiquidCapital, MotorHappy and M-Sure.	Mobility Solutions internal audit Insurer audit of M-Sure	Monthly Regularly
<b>UK:</b> competency of regulated consultants and managers.	Internal assessment	Regularly
<b>UK:</b> regulated consultants and managers, dealership compliance to F&I regulations and deal transaction files.	Third-party compliance service provider.	Regular monitoring.
<b>Australia:</b> dealer F&I compliance.	Independent audit by the financial service providers	Regularly
<b>Data protection and cybersecurity</b>		
<b>Group:</b> protection of personal information.	Internal audit	Three-year rolling cycle
<b>Group:</b> data breaches (including loss of personal computers or devices) and encryption of personal computers.	Board review	Quarterly
<b>Group:</b> cybersecurity measures.	Independent assessment Internal assessment	Twice a year Quarterly
<b>Customer satisfaction</b>		
<b>Group:</b> customer satisfaction survey results (new vehicle sales, workshop servicing and parts) and for SA, in certain instances, this includes the sale of pre-owned vehicles.	Internal review Importer OEM assessment	Monthly Ongoing
<b>SA:</b> cases reported to an ombudsman.	Board 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 2024 performance

 2024 ESG Report.

 2024 Integrated Report.