Practice

Our ambition: Embracing stewardship to embed sustainable and innovative ways of working that foster customer (and stakeholder) trust

Our Practice pillar is about governing with purpose and implementing the principles of stewardship, stakeholder engagement, risk mitigation and opportunity management through:

- Customer trust and experience
- Data security and privacy
- Ethical leadership
- ESG-related financial frameworks
- Stakeholder management
- Supply chain management

Business stewardship

Ethical leadership and conduct

Telkom has zero tolerance for unethical behaviour, fraud and corruption. Our Group Code of Ethics articulates principles and practices related to:

- Confidentiality and the protection of information and assets
- Ethics
- Gifts and entertainment
- Conflicts of interest
- Prevention of fraud and corruption
- Whistle-blowing

The Board sets the tone from the top. The Code includes an ethical leadership pledge that is signed by the Board Chairperson on behalf of Board Members and by the Group CEO on behalf of Group Exco Members. The pledge is cascaded to the respective subsidiary CEOs and their board chairs. Employees commit to this pledge annually through an electronic platform.

Find our Group Code of Ethics at https://group.telkom.co.za/documents/governance/EthicsHandbook-Group.pdf.

We combat corruption and enhance an ethical culture in our broader operating environment through:

- Ethics policies related to conflicts of interest, gifts and entertainment, prevention of fraud and corruption, and whistle-blowing
- The Whistle-blowers and Investigation Participating Parties Protection Procedure, which provides physical, financial, reputational and psychological protection to whistle-blowers, as well as support for civil and criminal actions
- The Group risk appetite statement and the fraud policy detail Telkom's zero tolerance appetite for fraud and corruption
- The Telkom Group Forensics (TGF) charter mandates TGF to manage all aspects of fraud risk management
- Our Ethics Office has an ethics mailbox where employees can voice concerns or report unethical or unlawful behaviour. The mailbox is not anonymous, but is confidential and accessible only by the Ethics Office
- Monthly induction sessions
- Online ethics and anti-fraud training modules were developed and launched in November 2025 in collaboration with TGF
- The Ethics Office and TGF are part of the combined assurance awareness forum, a combined assurance initiative that drives training and awareness across the Group
- Employees must declare any interests, conflicts and work outside the scope of their duties to ensure the Group's interests take precedence over personal interests. Gifts and entertainment activities must be declared to avoid any undue influence
- Through Group Revenue Assurance and Fraud Management and the credit management function, we proactively monitor areas that are vulnerable to fraud and conduct fraud detection reviews where the need arises

Find our ethics-related policies on our website at https://group.telkom.co.za/sustainability/Sustainability.html.

The use of reporting mechanisms increased by 21% to 1 494 incidents reported (FY2025: 1 239). This indicates increased confidence in our mechanisms, which is supported by the fact that 96% of reporters were willing to reveal their identity, while 64% of forensic reviews were confirmed or substantiated.

The outcomes of these reports led to recovery of fraud losses and consequence management against implicated third parties and employees, including the opening of criminal cases.

The ethics advice provided helped to improve our ethics and risk culture and control environment. The ethics advice and guidance were provided to second-line assurance providers such as TGF, management and employees.

Ethics support and advice

Telkom's Group Ethics Office is available to all employees. It provides ethics advisory support and information, enabling the Group to resolve ethical dilemmas in a sound and consistent manner, based on our values. The Group Ethics Office is one of several channels that internal and external stakeholders can use to seek advice or report unethical behaviour. It is supported by business unit Ethics Champions.

The Group Ethics Office conducts regular awareness initiatives to embed a Group-wide ethical culture and promote ethical behaviour by employees and suppliers.

Tax management and practice

The Group's tax strategy undergoes annual review by both management and Board to ensure alignment with regulatory requirements and corporate objectives. The Board retains ultimate accountability for tax governance, reinforcing its role in safeguarding compliance and ethical standards.

Complementing this, the Group's formal risk management framework provides structured guidance for identifying, evaluating, and prioritising risks. Through this process, the Board and management receive a thorough and integrated assessment of all principal risks facing the business. This enables informed decision-making, proactive mitigation, and long-term sustainability.

The Group tax strategy is to take a responsible approach to the management of all taxes whenever and wherever we do business, recognising the economic and reputational penalties for non-compliance and supporting the principles of transparency and active, constructive engagement with key stakeholders to deliver long-term sustainable value.

The strategy is underpinned by the principles of integrity in compliance and reporting, and controlling and managing tax risks in line with the OECD recommendations for responsible business conduct in a global context.

Telkom recognises that responsible tax practices are fundamental to sustainable business operations and long-term value creation. Our tax strategy is designed to ensure compliance with applicable laws, safeguard our reputation, and contribute to the economies in which we operate.

Through our moderate-to-low tax risk appetite, we protect the Group's reputation and prevent unnecessary tax disputes. We achieve this by taking tax positions strictly in accordance with established legislation, court precedent, or specific interpretation notes and rulings.

Through direct and indirect tax payments, Telkom contributes to government revenues in South Africa and other jurisdictions where we operate. These revenues enable governments to invest in critical areas, such as healthcare and education.

We are committed to paying our fair share of taxes. In FY2026, the Group made the following tax payments:

- Income tax: R297 million (FY2025: R396 million)
- Employment tax: R1 844 million (FY2025: R1 730 million)
- Value-added tax: R2 004 million (FY2025: R2 156 million)

At this stage, the Group does not disclose estimated tax gaps or detailed exposure to low-tax jurisdictions. We continue to assess the maturity of our broader tax transparency disclosures.

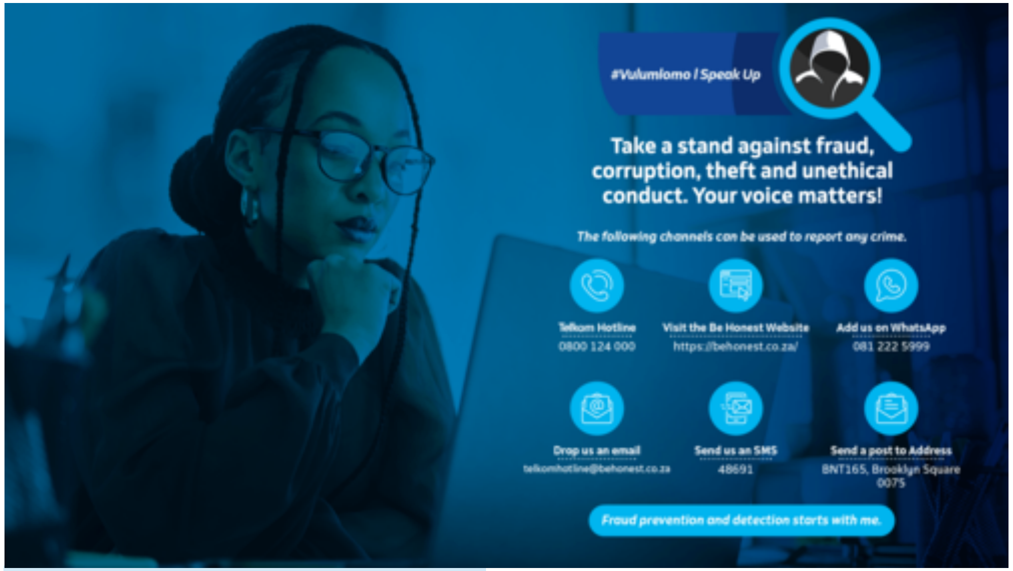
Whistle-blowing and grievances

Telkom offers a dedicated, confidential and anonymous whistle-blowing hotline (known as #Vulumlomo) to report fraud, corruption, theft and other irregular conduct. Other reporting mechanisms include direct reports to Telkom Group Forensics or the Ethics Office. All disclosures made through these facilities are confidential and protected in accordance with the requirements of the Protected Disclosures Act.

Disclosures and actions stemming from investigations are reported quarterly to the Social and Ethics Committee.

All Directors and employees have a responsibility to report any knowledge or suspicion of fraud, corruption or other unlawful conduct via an appropriate channel. Where appropriate, Telkom investigates reported and suspected acts of fraud and corruption and deals appropriately and consistently with all parties. If required, matters may be referred to the relevant law enforcement authorities for appropriate action, including the institution of criminal proceedings.

The Group Code of Ethics details the protocol to follow for reporting fraudulent, corrupt or irregular activities where a Board Member or Prescribed Officer may be involved.



Reporting fraud

Telkom Hotline:
0800 124 000

Be Honest Website:
https://behonest.co.za/

WhatsApp:
081 222 5999

Email:
telkomhotline@behonest.co.za

SMS:
48691

Postal address:
BNT165, Brooklyn Square, 0075

Incidents in FY2026

In FY2026, a total of 1 168 incidents were reported to Telkom's whistle-blowing hotline, an increase of 9.8% over FY2025. Reported matters were independently assessed and investigated, and outcomes were reported to various governance structures within the Group.

Reported cases are categorised as fraud, corruption, theft and irregularities (non-compliance with policies, procedures or established practices). Cases may be either internally or externally perpetrated.

- Externally perpetrated incidents included various types of scams and syndicate-driven incidents relating to subscription fraud, including application fraud, identity fraud and profile building. Other incidents included syndicate-driven economic crimes such as copper cable theft, battery theft and optic fibre damage
- Internally perpetrated incidents included various types of third-party misconduct, conflicts of interest, declaration of interest failures, and failure to comply with policies

Substantiated cases investigated by Telkom Group Forensics led to disciplinary actions against employees and third parties (including termination of contracts and various types of warnings), recovery of losses, opening of criminal cases and arrests of implicated parties, and internal blacklisting of implicated parties.

Most importantly, substantiated cases led to improvements in internal controls to enhance the Group's ethics and risk culture. We track the forensic recommendations, and most of the findings were implemented by management by year-end.

Looking ahead

In FY2027, we will continue to improve customer awareness. Specifically, we will introduce initiatives to combat emerging fraud trends, such as the increase in social engineering scams that manipulate or pressure people into parting with sensitive information. Such scams are becoming increasingly sophisticated as AI-related capabilities advance, posing a threat to traditional fraud controls.

We also aim to improve our fraud risk management practices. This will include conducting an ISO 37003 Fraud Control Management Systems gap analysis, and implementing a new system to track forensic recommendations and business intelligence tools.

Data security and privacy

Data security and privacy is one of our top sustainability risks, and cybersecurity is one of our material themes. Cyberattacks and data breaches pose significant risks for telecommunications companies. The expansion of digital services, cloud platforms and connected technologies increases exposure to sophisticated cyberthreats. Cyber incidents can disrupt services, compromise sensitive customer data and damage Telkom's reputation. As telecommunications networks form part of critical national infrastructure, maintaining robust cybersecurity capabilities is essential to protecting service continuity and stakeholder trust.

The Telkom cybersecurity strategy applies the principle of defence in depth by aligning with the five core cybersecurity functions of the National Institute of Standards and Technology (NIST), together with prominent industry standards such as the Center for Internet Security's Controls and Guidelines for ISO 27001 and the Information Security Forum's Standard of Good Practice for Information Security.

The NIST core functions enable us to implement multiple, overlapping layers of preventative, detective, corrective, response and recovery controls across the Group. By combining security risk and governance with layered technical, operational and resilience controls, we ensure we are able to withstand sophisticated cyberattacks in an evolving threat landscape. This approach provides the structure, confidence and controls necessary to enhance cybersecurity, address risk gaps, drive resilience, and ensure compliance with global standards.

We continue to strengthen our cybersecurity capabilities through enhanced monitoring, security architecture improvements, employee awareness initiatives and investment in information security technologies. We apply the “privacy by design” principle by building security protections into products, services, systems and culture from the onset. This approach, combined with the “security by design” principle, ensures that data protection is a business enabler rather than a cost factor.

The Telkom Board received training on cybersecurity and the evolving threat landscape in FY2026. Read more about cybersecurity risk management in the integrated report.

Telkom is committed to safeguarding the personal information of our customers, employees and service providers, supported by a strong governance and compliance framework.

We received two complaints from the Information Regulator and 22 customer complaints related to direct marketing in FY2026, and reported one incident of unauthorised access to information. We investigated all the matters, reported the outcomes, and implemented appropriate corrective actions to enhance the control environment.

Consumer data privacy and protection

Telkom ensures the privacy and security of consumer data through a structured framework. This outlines strict adherence to the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA) through formal POPIA and PAIA manuals.

As required by POPIA, the Group implements “appropriate, reasonable technical and organisational measures” to prevent any unauthorised or unlawful access to, or loss, damage or destruction of, personal information. This is supported by a regularly updated privacy statement and established procedures for notifying affected data subjects and regulators in the event of a suspected breach.

Governance of data privacy and security risks is treated as a top-level strategic priority. The Technology Committee is specifically mandated to oversee data protection and cybersecurity strategies. At the same time, the Risk Committee monitors data privacy as a component of the Group’s ERM framework.

Ensuring an ethical approach to digital and AI

Three frameworks guide employees and the Board on ethical behaviour in the digital space:

- The Telkom digital ethics framework ensures we maintain the integrity of our data, and maintain algorithmic processes and systems that guide outcomes and decisions on how we present products and services to users. We recognise the importance of collecting data in a transparent manner, and we make the user aware that this data could be used in future, including for machine learning or AI. We handle such data in a way that minimises the risk of any human bias
- Our privacy framework ensures that personal information collected, acquired, processed or stored by the Group or through a third party is treated as confidential and protected throughout the life cycle. The framework guides us on what is acceptable and ethical in how we identify, assess, monitor, use and dispose of information. It informs service design and delivery, information management, employee education and privacy breach management

- Telkom’s AI framework aims to unify, regulate and control the proliferation of AI across the business to ensure that its use is consistent, effective, economical, efficient, ethical, scalable and aligned with business goals. The framework helps to align AI initiatives with the OneTelkom approach. It also ensures that AI projects contribute meaningfully to business outcomes such as efficiency, innovation and customer satisfaction

Supply chain management

Suppliers play a critical role in our value chain and have a direct impact on equipment, material and other input costs. Telkom manages environmental impacts across our value chain through a structured governance framework anchored by our environmental and climate change policy statements.

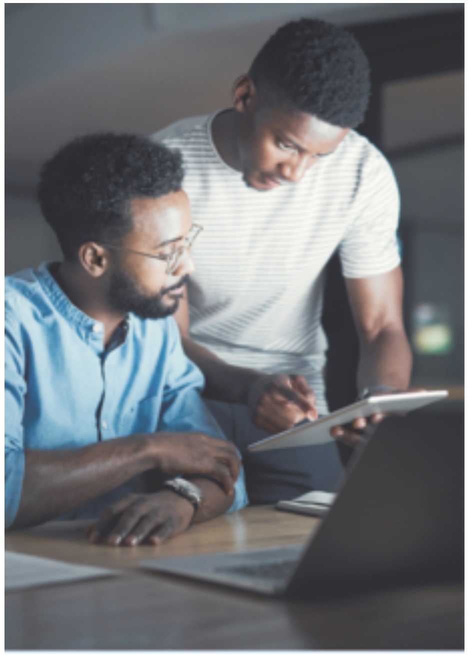
Telkom has identified its top 200 suppliers for focused engagement on the decarbonisation and sustainability clauses we have incorporated into new and renewed supplier contracts. We identified these suppliers through a comprehensive mapping of our supply chain.

Our contracts require suppliers to measure, monitor, report and progressively reduce their greenhouse gas emissions. We are working towards transitioning from spend-based to activity-specific and supplier-specific data for Scope 3 accounting. We conduct monthly and quarterly reviews with our suppliers to ensure alignment and strengthen partnerships.

Our structured supplier onboarding and external assessment process is designed to strengthen oversight across the supply chain. Suppliers are onboarded through the SAP Ariba platform, which incorporates compliance checks and requires adherence to our Supplier Code of Conduct.

As part of our supplier vetting process, we require disclosure on child labour, forced labour, and freedom of association risks through the sustainability assessment platform that we use. However, participation is currently limited, mainly because suppliers fund their own assessments through subscription fees, which has constrained uptake among smaller suppliers.

We are continually improving the process and investigating ways to strengthen the quality and consistency of suppliers' sustainability data. In the interim, we use our broader supplier risk vetting process to monitor for any adverse publicity related to human rights issues.



Forward-looking and sustainable procurement

Procurement is a critical enabler of Telkom's broader sustainability ambitions. It enables us to strengthen our performance, align with global best practices, and proactively respond to evolving business expectations.

In FY2026, we made progress towards finalising a forward-looking procurement strategy that will drive responsible sourcing, enhance supplier accountability, and unlock long-term value across our value chain.

In developing the strategy:

- We used a double materiality lens to identify the sustainability issues most relevant to Telkom's procurement activities
- We comprehensively assessed Telkom's procurement policies, Supplier Code of Conduct, contracts, and tendering processes against global best practices and peer benchmarks

- We made recommendations focused on quick, high-impact actions that are practical to implement
- We developed KPIs to track supplier performance, incorporated sustainability factors into our supplier evaluation criteria, and created an incentive and penalty framework to drive accountability
- We used Scope 3 emissions accounting to measure indirect emissions across the supply chain
- We defined best-practice roles and responsibilities to embed ownership within procurement and strengthen governance, and agreed on an implementation roadmap that will guide us over the medium term