



## OUR SUPPLY CHAIN

Improved supply chain management through responsible procurement practices and effective communication with suppliers

**Procurement as the strategic business enabler, technology driven towards intelligent procurement operations and support.**



### Responsible Procurement Practices

To support our Responsible Procurement Practices, Maxis has in place a robust set of policies and procedures to guide and govern the sourcing, selection, assessment and performance monitoring of our suppliers.

For example, Maxis always upholds ethical procurement practices with its suppliers, providing a level “playing field” which is guided by suppliers’ compliance to technical and commercial requirements which forms the basis of the evaluation and selection of suppliers. This includes our commitment to open and transparent competition based on suppliers’ capability and experience and not just on size and maturity, which helps drive inclusiveness and helps new businesses to flourish.

Potential suppliers are also required to go through our vendor onboarding process and due diligence check. Here, they are required to submit relevant business and financial documentation for assessment and to sign our Maxis Code of Business Practice (MCOBP) and Integrity Pledge (IP).

### Managing our Suppliers Effectively

The Maxis Code of Business Practice for Third Parties contains guidance to assist third parties in conforming to the ethical business standards observed by Maxis in all our business dealings with third parties. Third parties, who conduct business with the Group must formally declare that they have read and will adhere to the MCOBP upon commencing work with the Group. In addition, an annual Vendor Integrity Programme conducted by Maxis’ Integrity and Governance Unit raises bribery and corruption awareness to these external parties.

Maxis Vendor Management team also conducts periodic and ongoing assessments of identified key suppliers’ performance to identify improvements and correction actions. Existing suppliers are also required re-acknowledge the MCOBP annually. Maxis has also enhanced the policy on engaging consultants by providing clarity on what constitutes consulting services, in addition to requiring approval from top management for any appointments.

To ensure on-time delivery and sufficient supplies during the pandemic, we maintain constant dialogue with our critical suppliers, plan in advance and explore and secure alternative supplies as necessary. We have also optimised processes and technology tools in our Source to Contract framework, enabling online supplier collaboration throughout onboarding, tendering and contracting, for transparency and proper audit trails.

### Future Outlook

Looking ahead, our short-term goals are to further leverage technology, digitalisation and automation to provide the procurement team better insights and understanding regarding spend patterns and trends. We are also committed to developing an effective Supplier Relationship Management Framework to standardise the roles and responsibilities of our vendors. Maxis will also keep striving to improve efficiency, but without compromising on our controls and governance. In addition, we will continuously optimise our spending for low spend and low volume vendors.

Over the medium-term horizon, we aim to enable AI and predictive technology to free up our employees and drive greater productivity. We will also move towards more strategic partnerships with suppliers that will establish closer relationships and where performance, issues and value add activities can be discussed further. Finally, we believe that our function will evolve into Procurement as a Service, where we are a business value creator and enabler for Maxis.



**Our Priorities**

**Our priorities within 1 to 2 years:**

- Digitalisation & automation e.g., digital spend analytics, chatbots. Process simplification with technology enablement providing better understanding and insights through data and information.
- Develop an effective Supplier Relationship Management framework (including risk management), with clear roles and responsibilities. Standardising ways of managing strategic suppliers and contracts will reduce risk of contractual benefits leakage and opportunities.
- Continuous process improvement towards zero audit tolerance. Balancing the need for more efficient process that meets the current business needs while keeping control and governance in place.

- Review long tail vendors for spend and supplier optimisation. Though low value spend (purchases below RM5K) is a small percentage of Maxis total spend (<1%), a continuous review would facilitate better spend and supplier management.

**Our medium-term plan in the next 2 to 5 years:**

- Enable AI and predictive technology (extreme automation). This minimises administrative tasks which would allow staffs to focus on more strategic tasks.
- Move towards more strategic partnership with suppliers whereby channels are established to discuss performance, issues, value add activities including innovation and sustainability.

**OUR CYBERSECURITY**

Built a stronger cybersecurity culture and enhanced system resiliency

Ensuring robust cybersecurity of our systems and safeguarding data privacy is a critical and top priority for Maxis. The industry we operate in directly exposes us to numerous cyberthreats, especially when considering the large network that we operate and the millions of customers we support. As such, it is vital for us to invest in security infrastructure, create policies, processes, procedures and implement solutions that will strengthen our defense against the growing sophistication of would-be attackers, while ensuring that our business objectives can progress unimpeded.



Protect the Brand and Ensure Compliance



Embed Security in DNA



Strengthen Cyber Resilience and Support Digitalisation

"I am Maxis" embodies our commitment that all of us are responsible for cybersecurity. Our employees and partners are required to adhere to our cybersecurity policies and ensure that the necessary cybersecurity controls are implemented, monitored and reviewed. We also encourage active participation in our cybersecurity awareness programmes and provide updates on cybersecurity threats through our internal communication channels and through dedicated campaigns.

The Cybersecurity Management department is accountable for more than the cybersecurity posture of our networks and IT systems but also partner with the business to ensure that Maxis continues to remain resilient against cyber threats and protect our key assets. Cybersecurity as a whole is governed by members of

the Maxis Management Team and also provide periodic reports to the Audit & Risk Committee regarding posture, current and potential security threats as well as measures taken to manage the identified risks.

**Enhancing Cyber Resilience**

The potential for security threats increases indirectly as a result of digitalisation initiatives and thus prompts the need to review our strategies to enhance cybersecurity resilience. By definition, resilience means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, or compromises on systems.

Acknowledging that human error is a major factor in cyber security breaches, we continue to enhance cybersecurity resilience through our security awareness programme