

Marketplace and Customers

Ethical and Responsible Business Practices

The Singtel Group strives to reduce the negative impact of our products and services. Our responsibility encompasses governance and anti-corruption as well as safety, data privacy and fair communications for our stakeholders in the marketplace.

CUSTOMER HEALTH AND SAFETY

Today, the perceived health risks associated with the emission of Electromagnetic Energy (EME) from mobile devices, base stations and tower infrastructure remain a concern for our customers, the community and regulators. This is despite the absence of conclusive evidence on adverse health effects caused by mobile phone usage.

Please refer to our [website](#) for information on our efforts and measures to ensure compliance with both local and global standards for such emissions.

In Singapore, we continue to engage the National Environment Agency (NEA) during the year, which conducted eight radiation measurements at locations of concern island-wide. The results showed that our mobile base stations complied with the radio frequency radiation levels and safety guidelines set by International Commission on Non-Ionizing Radiation Protection (ICNIRP). The findings were shared with the stakeholders who raised the concern.

We also submit to IMDA a monthly report on newly commissioned base stations to ensure that their Effective Isotropic Radiated Power or transmission power is within its guideline.

In Australia, we conduct audits of base stations and undertake predictive EME modelling and testing to ensure compliance at our sites with the Australian standards. We publish the EME reports of all our sites at www.rfnsa.com.au.



CUSTOMER DATA PRIVACY AND PROTECTION

We conduct our business in compliance with data protection laws – the Personal Data Protection Act (PDPA) in Singapore and the Privacy Act and Telecommunications Act in Australia. These laws cover various rules governing the collection, use, disclosure and care of personal data. Singtel's Group Chief Information Officer is also our Data Protection Officer and reports to the Board Risk Committee to manage this important matter.

During the year, we conducted over 1,000 Privacy Impact Assessments in our Singapore and Australian operations to identify and assess personal data protection risks in our systems or processes that involve the handling of personal data, with recommendations addressing the risks.

We issued comprehensive guidelines on our staff portal Espresso to help our employees comply with the PDPA in Singapore. These guidelines cover the various aspects under three categories of collecting, disclosing and disposing of personal data. We also implemented a mandatory online privacy training for our

employees in Singapore and Australia. Our training programme was a finalist in the Australian Institute of Training and Development National Training Excellence Awards.

We recorded 21 minor incidents in Singapore and 48 cases in Australia of unintended data disclosure during the year, mainly due to human lapses and negligence, such as disclosing personal data to unintended recipients over the phone and sending documents containing personal data to the wrong email or postal addresses. Three of these cases were referred by the Personal Data Protection Commission of Singapore. We continue to work with our staff to reduce the recurrence of such lapses. From 22 February 2018, certain eligible data breaches are notifiable to the Office of the Australian Information Commissioner and Optus did not have such data breaches during the year.

To help enterprise customers protect their own data and their customer data, the Singtel Group offers a suite of cyber security solutions powered by our US-based subsidiary Trustwave and the Group's ten Advanced Security Operations Centres (ASOCs) across Asia

Marketplace and Customers

Pacific, Europe and US. Supported by about 2,000 cyber security professionals, we leverage our ASOCs' global threat intelligence, threat data analytics and advanced security automation capabilities to provide our enterprise customers with real-time monitoring, response and remediation against advanced and evolving cyber threats.

To meet the demand for cyber security talent, we have partnered government agencies, tertiary institutions and leading cyber security service providers to build a sustainable cyber security talent pool.

FAIR MARKETING COMMUNICATIONS

We recognise that fair marketing practices and being transparent in the way we communicate are critical to build trust and loyalty among our customers. Our marketing code sets out the requirements that Singtel organisations and representatives must follow to ensure that all marketing activities comply with various laws and guidelines such as the Singapore Code of Advertising Practice, IMDA Codes of Practice and Guidelines and PDPA.

There were no cases of non-compliance with regulations and voluntary codes concerning marketing communications at Singtel in Singapore during the year. However, we received three consumer complaints from the Advertising Standards Authority of Singapore, of which two were found to be invalid claims that our advertisements were misleading. The third involved a new mobile phone brand that claimed to have the "largest capacity found in any smartphone". We amended the advertisement copy which was provided by the mobile phone manufacturer.

On 11 December 2017, the Australian Competition and Consumer Commission (ACCC) accepted a court enforceable undertaking from Optus in relation to claims about speeds available to consumers on our fibre-to-the-node and fibre-to-the-building broadband plans offered over the National Broadband Network (NBN) that were likely to



Number of cases received in FY2018 via Whistleblower Hotlines

	Received	Substantiated	Not Substantiated	Under Investigation
Singtel	37	11	17	9
Optus	66	33	25	8
Singtel Group	103	44	42	17



Number of confirmed incidents in which employees were dismissed or disciplined for corruption

Singtel **2** Optus **0**



Number of confirmed incidents when contracts with business partners were terminated or not renewed due to violations related to corruption

Singtel **1** Optus **0**

contravene the Australian Consumer Law. On 22 May 2018, Optus was fined by the Federal Court A\$1.5 million for making misleading representations to customers about their transition from our network to the NBN.

ANTI-CORRUPTION

We continue to manage the Group's exposure to corruption risks by applying and emphasising good corporate governance, business ethics and transparency while applying robust internal controls in business processes as our core approach. Our efforts in this area have been recognised through the 2018 World's Most Ethical Companies ranking by Ethisphere Institute for the eighth consecutive year. Singtel is the only company in Singapore as well as in Asia's telecommunications industry to be honoured with this accolade.

We ensure that the Group's zero tolerance policy towards fraud, corruption and unethical actions is strictly adhered to. Our Group policies on Fraud Investigation and Whistleblower Programme underpin our fraud risk management framework and

processes. Please refer to our [website](#) for more information on this topic under Corporate Governance.

In August 2017, we published our [Singtel Group Anti-Bribery and Corruption Policy](#), which reinforces our longstanding zero tolerance approach to bribery and corruption of any form that is set out in our Code of Conduct. All Singtel Board of Directors, employees and third parties who represent us such as suppliers, contractors and business partners, must comply with this policy at all times. They must also comply with all relevant laws like the UK Bribery Act in countries where we conduct business.

We received a total of 103 cases via our whistleblower channels during the year. After investigation, 44 cases were substantiated and 42 cases were not, with the remaining 17 cases under investigation at the end of FY2018. Two of the substantiated cases took place outside Singapore and Australia. We closed 15 matters received in the prior year that were still under investigation as at 31 March 2017.

Highlights of the substantiated cases:

- 22 cases involved breach of policy and gaps in business processes by employees
- 10 cases of identity theft related issues in Australia that affected customers or members of the public
- 9 cases of employee misconduct and inappropriate behaviour involving unethical behaviour, conflict of interest, breach of code of conduct and corruption
- 2 cases involving harassment of fellow employees
- 1 case of vendor fraud involving forged documents

When these cases came to our attention, independent internal investigations were immediately conducted by our Internal Audit or investigation teams led by our subject matter experts. When an alleged corrupt or other criminal act by an employee is substantiated, the persons of interest were terminated and the matters reported to the relevant law enforcement authority.

During the year, we amended the public communications in Australia so that calls regarding customer identity theft were directly referred to our Optus' ID Theft Hotline. This resulted in a significant decrease in call volumes to our Whistleblower hotline in Australia.

SUSTAINABLE SUPPLY CHAIN MANAGEMENT

The Singtel Group has an extensive supply chain ranging from equipment and infrastructure suppliers to advertising agencies and content providers.

Given the complex nature and the widespread geographical presence of our supply chain, we believe that by collaborating with socially and environmentally conscious suppliers, we can mitigate a significant proportion of our sustainability risks and impacts. Results from our Life Cycle Assessment and Social Hotspot Analysis are further testimony to the need for responsible procurement practices in our business. Please refer to our [website](#) for more details.

MANAGING SUSTAINABILITY IN OUR SUPPLY CHAIN

In FY2018, we circulated our self-assessment questionnaire to gather inputs from our next set of top 50 suppliers. This questionnaire was developed last year and covered eight key ESG categories. All new suppliers were also assessed through the questionnaire as part of their on-boarding tender process.

The Singtel Group
contracted
6,534
suppliers worldwide
in FY2018



From the assessment, we are generally satisfied with the approach our larger suppliers have for the key ESG matters of importance to the Singtel Group.

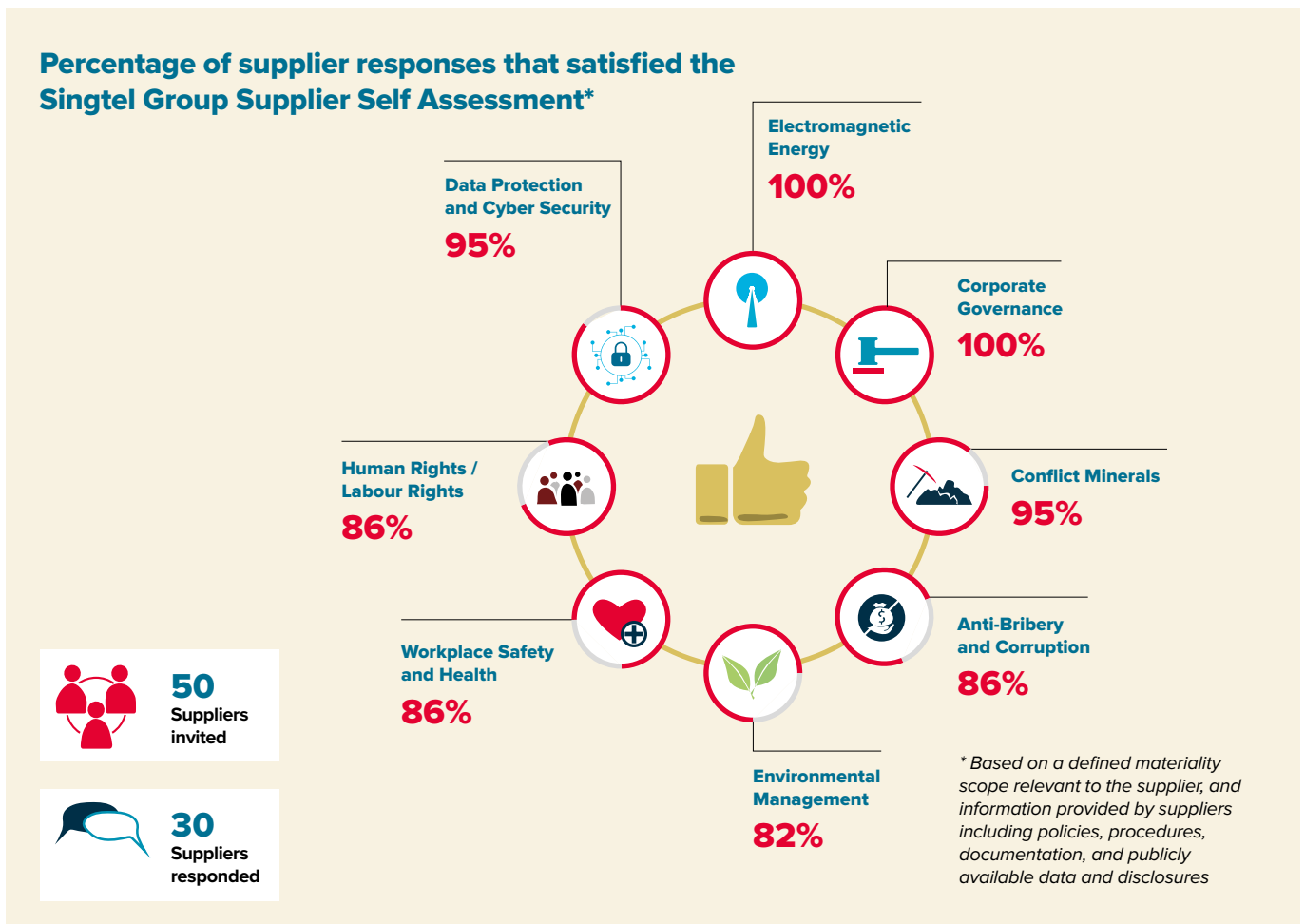
For suppliers who lack sufficient documentation to support their claims, we will request for more information regarding their areas of high sustainability risks. This will allow us to undertake a deeper dive into how our suppliers manage these key areas. If we are not satisfied that they have robust systems and methodologies governing the key ESG topics, we will request for further engagement and determine if there is a need to flag for third-party audits.

With the progress made with our Sustainable Supply Chain management programme, we are sharpening our focus on four key groups of suppliers who pose higher risks in our supply chain: Devices, Network equipment, IT hardware and Offshore call centres.

During the year, we also undertook a Security Compliance Assessment and visited 14 offshore secure locations to ensure that the facilities were set up according to the agreed regulatory security architecture and controls.

We are committed to inclusive procurement practices, which we believe will create long-term value for our partners and communities. Optus is a member of Supply Nation, a direct business-to-business purchasing link between corporate Australia, government agencies and Indigenous-owned businesses. As a Supply Nation member, we meet the requirements of the Australian Government's Indigenous Opportunity Policy and have access to an online database of Supply Nation-certified Indigenous business suppliers whom we seek to engage for services. We will proactively promote the services of Indigenous suppliers as part of our wider inclusion strategy.

Marketplace and Customers



SAFETY OF OUR CONTRACTORS

We continued with the Singtel Safe Contractor Accreditation (SCA) scheme, a set of Singtel's Workplace Safety and Health (WSH) standards that we piloted last year for contractors who perform high-risk technical or physical work in Singapore. We identified 120 contractors in the high risk category who require SCA accreditation and failure to do so will disqualify them from obtaining future contracts with Singtel. Our contractors have made good progress in this area with elevated WSH standards, with 105 achieving our SCA accreditation.

We increased efforts to identify lapses on-ground and help our contractors put in place programmes to address any unsafe work practice. We also produced a manhole safety video highlighting common risks and safe procedures to carry out work. The video is based on actual work scenes so that viewers can easily relate to.

We continued to issue 'show cause' notices for cases where serious safety violations were observed. During the year, we conducted more than 2,000 inspections. Contractors found to have infringements attended our Safety Time Out Programme (STOP) and implemented necessary precautions before resuming work with Singtel.



Enforcement Actions

