LIVING BY OUR PRINCIPLES AND PRACTICES

International SOS has been in business for 33 years. During this time, we have taken a long-term view of creating sustainable operations so that we are competitive and provide good livelihoods for our employees. We are guided by the business practices which contribute to our sustainability in the global marketplace.

INTERNATIONAL SOS
AMBULANCE
FIRST AID

BUSINESS CONTINUITY

The Board and Group Executive Committee of International SOS have developed and maintained a business continuity plan and disaster recovery plan designed to protect the safety and health of employees, ensure uninterrupted service to our clients and provide for the security of confidential information.

At International SOS we are uniquely structured in our ability to provide uninterrupted service operations for assistance callers. In the event of a business interruption at any of our Assistance Centres, International SOS has the capability to seamlessly divert all calls for daily business operations to another of its 26 Assistance Centres with no down time, and no compromise in language capability. All Assistance Centres utilise the same global proprietary software system for case management (NewCase), which ties into the Customer Relationship Management System (SFDC) and the Service Provider Information Network database (SPIN), as well as accounting processes and systems. Additionally, all Assistance Centres communicate through the same Information Technology (IT) network, follow a similar staffing structure and undergo standardised training, and have multilingual capabilities and operational procedures. This ensures complete business continuity and continued customer service for our clients.

Our software systems are integrated to ensure we are able to provide uninterrupted service operations for assistance callers. There follows a brief description of how our software systems interact:

- **Case Management –** International SOS utilises the NewCase proprietary case management software tool for automated tracking and monitoring patient status. The NewCase application allows the customisation of client, programme, case and incident level scripts to assist the Operations team in capturing the information required for a particular case.

  A case can be actioned by any Assistance Centre within NewCase depending on the location of the member, the relationship with the client and the needs of the particular case. This results in significant time savings. Communications at the Assistance Centres is centralised; this enables full audit ability and traceability on the progress of a case at any time.
- **SPIN —** has a service provider database of 81,000 medical and technical professionals.
- **Customer Relationship Management System –** International SOS utilises the SFDC centralised sales database to track all client programmes including any specialised operations procedures and all Authorised Persons. Authorised Persons are our first point of client contact during an emergency or overseas event that impacts their employees. This database provides an identification methodology of clients at the time of the first call. This database captures all client pertinent information for identification or verification purposes, however, the ethos within International SOS is to assist first and verify later.
- **Information Backup –** IT backups are completed daily. Backup tapes are stored offsite by a vendor in a secure location. All backup tapes are moved from the facility to the off-site vendor in locked boxes with tamper proof seals, to prevent unauthorised entry. Only authorised IT personnel can access the backup tapes. International SOS also runs in all major centres a process of real-time back up to parallel servers in local Disaster Recovery (DR) sites.

  The International SOS data backup process ensures that previously stored and backed up data will be available in the event of an inadvertent delete or overwrite, or the need to relocate to an alternative office environment from the immediate DR site. All systems have built in redundancy. International SOS has multiple uninterruptible power systems in all locations. These are backed up by diesel fuel generators, where building regulations allow, with a fuel supply equal to a minimum of three days' usage. The generators are tested each week and are covered under maintenance contracts.

  Based on internal audit processes, International SOS conducts crisis and disaster recovery testing at least twice a year in each location. This is then audited both internally and as part of our ISO 9001:2015 external accreditation process.
- **Pandemic Preparedness –** The Group Executive Committee considers pandemic preparedness planning to be of utmost importance to the company and its clients. International SOS has recognised that influenza pandemic could infect 30% of the workforce globally over a period of 12-15 months. The possible prolonged reduction of the company's labour force, together with a possible increased demand for its services in some areas, could significantly impact its operations. We have recognised these threats and established documentation designed to reduce the risk to our workforce and the company.

To support business continuity, we run a comprehensive corporate, regional and country level crisis management structure. This enables the coordination and management of client medical, security or internal employee or asset crisis response. This structure is owned by each General Manager of a location or function and a system is in place to train and support capabilities in this area.

The business continuity & crisis management plan comprises an executive summary, an introduction to the plan, an overview of its structure, various scenarios, a review of the crisis team makeup, how to activate the plan and all required testing, training, maintenance and auditing.

The crisis and business continuity planning covers seven primary risk areas. Each is supported by action sheets for all functions, guiding activity and supporting tools as follows:

- Infrastructure failure
- Single facility disaster
- City wide disaster
- Surge in demand
- Threat to reputation
- Individual employees in danger
- Influenza pandemic

DATA PRIVACY & PROTECTION AND CYBER SECURITY

In recent years the global movement towards the adoption of comprehensive and increasingly sophisticated legislation for privacy protection has gathered pace. The implementation of the EU's General Data Protection Regulation (GDPR) in May 2018 represents the most significant shake-up of data privacy law to date. Its detailed requirements and severe sanctions for breaches have impelled corporations to change the way they gather, store and process personal data.

At International SOS, we are committed to safeguarding the confidentiality, integrity, and availability of the information we collect from our clients, members and employees.

Our Group comprises companies in 90 countries. We ensure they each meet or exceed legislative and industry standards for Data Protection. This ensures that individuals' personal information is protected across borders while we provide support to clients around the globe. We are committed to protecting our clients' privacy and to being transparent in what information we collect, why we collect it, how we use and safeguard that information, and the choices they have regarding their data when using our services.

Data protection

The nature of the services we provide has meant that protection of personal and sensitive information has always been a high priority for us. We respect the right to privacy of all individuals who entrust us with their data and devote significant resources to ensure the security, confidentiality, integrity and availability of the data we process.

Our clients entrust us with sensitive personal data such as medical data. We recognise our reputation and ability to serve our customers is dependent on how we protect that data.

Our Data Protection and information security governance structure comprises our AEA Board of Directors, the Data Protection Committee and the Information Security Management Sub-Committee. This structure includes our Chairman and CEO, Group General Counsel and Chief Data Protection Officer, Group Chief Information Officer and Chief Security Officer.

In addition, employees in each region are tasked with the responsibilities of Data Protection Administrators, Data Protection Officers or Data Protection Experts. Their responsibilities span a specific country or group of locations and entail ensuring organisational compliance with the International SOS Data Protection Policy and all applicable national and state data protection regulations.

Our Data Protection Policy guides our approach to privacy and the protection of personal information. As the foundation for our approach to data protection around the globe it complies with:

- Laws in the countries where we do business
- The relevant provisions of the United States HIPAA regulations
- Binding corporate rules sanctioned by the European community's data protection authorities
- The General Data Protection Regulation

All employees receive initial training in the Data Protection Policy within 30 days of joining International SOS. This eLearning includes a comprehensive test of objectives that is applied on an annual basis. Job-specific training is provided to individuals working in roles that handle personal data. Periodic communiques are shared with all staff to maintain their awareness of cyber security risks, privacy developments and lessons learnt.

Contractual commitments to our clients include:

- Authority and accountability for data protection
- Reasons for collecting personal data
- Consent of data subjects
- Collection limitations and accuracy
- Limiting use, disclosure, retention and destruction
- Security
- Openness
- Individual access and correction
- Challenging compliance
- Transfers to a third-party and cross-border personal data flow

Security policy

International SOS has implemented an Information Security Management System in conformance with widely accepted and recognised standards. Our Information Security Policy, Standards and Procedures are aligned with ISO/IEC 27002 Information technology – Security techniques – Code of Practice for information security management.

Our Information Security Policy states our intent to maintain a secure information-processing environment and to protect information assets. It describes our approach to the security of information stored digitally, at any point on the network or within the organisation's boundaries of authority. The policy is approved by the AEA Board of Directors and is communicated to all International SOS employees. Compliance with our Information Security Policy is mandatory for all employees. It is reviewed and updated annually, and whenever there is any change in the information-processing environment which may have an impact on the information risk profile.

We recognise the importance of maintaining robust technical security measures to support the administrative controls we have developed. Our Group IT Security team continuously evaluates and improves our technical security controls in anticipation of evolving cyber security threats. Technical controls include, but are not limited to the following:

- Defense-in-depth
- Physical security & surveillance
- Web application firewall

Increase in robberies in Sao Paulo state underlines status of crime as main risk to travellers

Sunday January 25 2015 8:48 A.M.

Official statistics indicate that robberies in São Paulo state increased by 20.4% in 2014 compared to the previous year. The growth percentage is the highest in 14 years and represents a 41% increase when compared to 2001. Crime poses the main risk to travellers in Brazil and no area is immune, necessitating that members take basic security precautions at all times.

Travel Briefing

While violent crime mainly centres on favelas (shanty towns) and other impoverished urban areas, where the travel are rated as HIGH compared with the try's overall MEDIUM travel risk rating.

- Network firewalls & intrusion detection systems
- Logical segregation of networks
- VPN and two-factor authentication
- Vulnerability assessment & penetration testing
- End point security – antivirus and encryption
- Host based intrusion prevention systems
- Web content filter
- Spam protection & Transport Layer Security (TLS)
- Digital certificates and Secure Sockets Layer (SSL)
- Identification and authentication controls

Cyber Security

Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber security and physical security, including network security, application security, data security, identity management, and cloud security.

We have implemented physical, technical and administrative controls to protect client information against cyber threats and require third-party certification of these controls. This requires that internal resources and service providers are certified against ISO/IEC 27001, SOC2 Type ll and ISAE 3402 Assessments for the data centres we use.

We have also implemented technical security controls to ensure that our systems can withstand attacks and to allow our Security Operation Centre to detect and respond to threats in a timely fashion. We have contracted a third-party cyber-intelligence firm to monitor the dark web for any conversations that may involve our Group entities and clients. We have implemented web application firewalls, network firewalls, anti-virus systems and other monitoring and alerting tools to support awareness. We have instituted administrative security controls to ensure that our systems are protected against unauthorised physical access.

Assurance

International SOS has in place both internal and external audit programmes. Internal audits are performed annually by the Data Protection Team and findings are shared with each location's General Manager and specific asset owners and custodians. Locally nominated Privacy Experts then support and implement action plans to address any non-conformances identified, reporting back to the auditors and keeping the local General Manager informed. Auditors report compliance status to the Group General Counsel, a member of the Executive Committee.

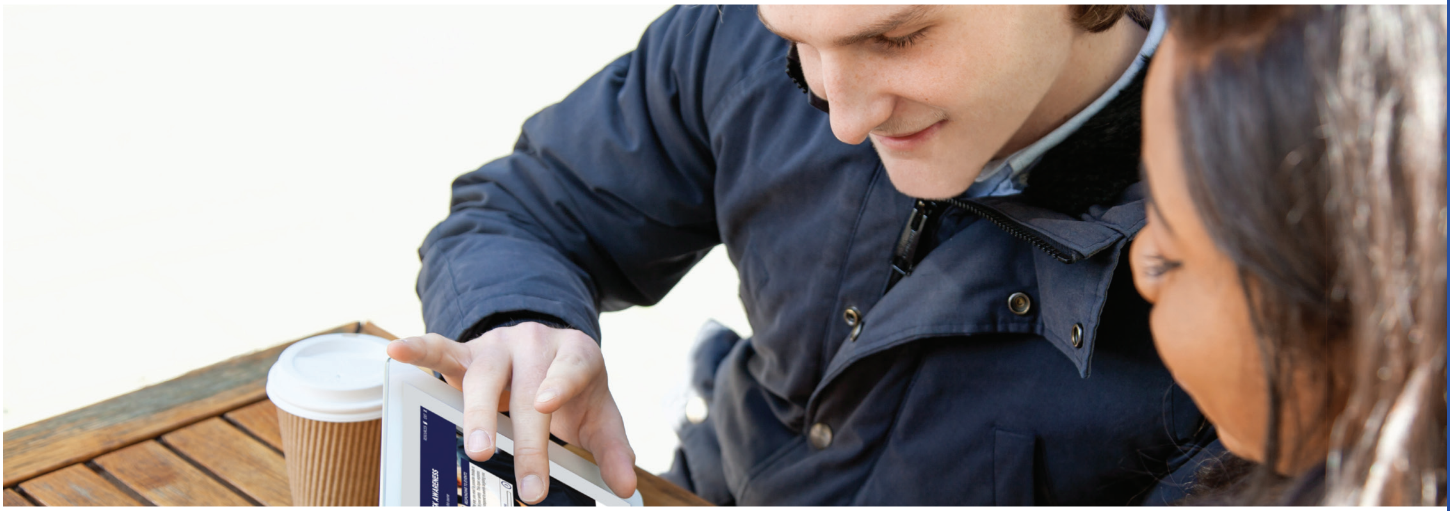
We engage qualified third-party auditors to perform examinations of our systems and services in accordance with the best practice recommendations of ISO/IEC 27002, for the purpose of auditing compliance with ISO/IEC 27001:2013 and the best practice recommendations of AT 101 Trust Services Principles, for the purpose of auditing compliance with SOC 2 Type II.

International SOS has recognised the implementation of the GDPR as an opportunity to evaluate and further enhance the effectiveness and resilience of our global information security framework, with a particular focus on the rights of data subjects.

The British Standards Institute (BSI), an independent standards body, had conducted an assessment of our business processes against the standards set by GDPR and affirmed that we operate our processes, systems and data gathering activities in alignment with the existing EU Data Protection Directive and are well positioned to fully comply with the General Data Protection Regulations.

To ensure sustainability in our business, we have made data privacy and protection a fundamental part of our product/service and process design framework. We have established Binding Corporate Rules (BCR) and other processes to ensure the safe transfer of personal data internationally within our corporate group. With this, our operations can support our clients 24/7, no matter where they are.

In FY1819, we have embarked on independent certification of our compliance with GDPR through Bureau Veritas. The first phase of this process involves auditing eight of our Assistance Centres.



BUSINESS INTEGRITY, TRANSPARENCY AND ETHICS

As a global organisation, employing people from over 90 countries, we respect and incorporate human rights into every aspect of our people agenda. All our offices seek to comply with local legislation and international standards, such as the UNGC principles, to offer a fair, safe and productive work environment and compensation for all employees. With an extensive Individual Rights Policy in place and in-depth awareness training, we constantly reinforce our stand against modern slavery, child labour, forced labour and any similar exploitative practices. We also work with business partners, suppliers, vendors and contractors to ensure they are aware of our employment standards, including our prohibition on forced labour and child labour. We recognise the right of our employees to group in accordance with local laws and are supportive of the freedom of association and the right to collective bargaining.

Our employees follow the International SOS Code of Conduct and Ethics (the “Code”), a set of principles by which we seek to operate a safe, honest, and responsible business. Our commitment to the Code is an important part of our brand and the reassurance we aim to give – demonstrating how we put the interests of our clients and members first to make a real difference in people’s lives. Our ethics and values give us pride in our work and our organisation and help us sustain our standing as a socially responsible organisation and a good corporate citizen.

Our policy also provides rules on handling personal gifts or hospitality that creates a conflict of interest.

International SOS attaches great importance to the honest and ethical conduct of our employees, our customers and our providers. Where permitted under local regulations, we conduct background checks on prospective employees, including criminal records and credit reference checks for those roles with exposure to finance.

All International SOS employees are required to complete annual training on the Code. This reinforces the value the company places on ethical business, and reminds them of the risks they and the business face if they do not live up to the Code. The annual training covers practical examples of situations that an employee might encounter and provides guidance to help clarify how the Code should be applied in such situations.

The management conducts regular training (e.g. annual refreshers) and orientation for new hires and experienced employees. This aligns the tone at the top of the organisation to the behaviour and actions in the middle and on the front line. It engages, educates, and raises awareness among employees about our culture of integrity. Network, Medical Supplies and IT providers are pre-qualified to ensure that they operate with the highest integrity and are free of the use of forced, bonded or child labour.

The General Affairs Policies and Procedures (the “GAPP”) governs how International SOS Senior Management is accountable for the management of business operations. The GAPP ensures that all expenditure, whether operating or capital in nature, is spent justifiably, within budgets and with appropriate levels of approval and authorisation.

We are committed to eliminating fraud and corruption in relation to our activities through the development, implementation and regular review of fraud and corruption prevention, detection and control strategies. Our Fraud and Corruption Control Policy is designed to allocate group responsibilities for oversight and implementation of the Fraud and Corruption Control Plan. Additionally, we communicate our policies on the prevention, detection and response to acts of fraud or corruption to our network of third party providers. We also require all employees to undertake yearly Global Compliance eLearning courses and refreshers. As at FY1718, we do not have any reported incidents of corruption relating to our business.

The Whistleblower Policy is one of many policies that promote a culture of integrity, honesty and ethical behaviour within International SOS. All employees are expected to promptly and fully report and breaches of the Code via the compliance hotline, safe in the knowledge that they will be protected against retaliatory action. Employees are encouraged to ask questions concerning ethical issues and report ethical violations or breaches of company policy without fear of retribution.

ENVIRONMENTAL IMPACTS OF OUR OPERATIONS

We are committed to meeting international environmental best practices for employees, customers and providers that are consistent with, and appropriate to, our business activities and operations worldwide. We have set in place an environmental policy to govern our environmental standards at all facilities. We also have environmental practices to reduce paper usage, encourage recycling and minimise electricity consumption. Our environmental practices vary by facility, but we strive to reduce waste, paper and electricity consumption and recycle where possible.

Medical waste

Chemicals and pharmaceuticals are being detected in the environment. There is genuine concern that these compounds, even in the small concentrations at which they are found, could impact human health or aquatic organisms.

To address this, we have always promoted and provided our clients with, safe options for medication disposal, using appropriate licensed disposal methods and contractors. Medical waste is disposed of with trusted third party providers via incineration. Similarly, for medical needles, they are discarded in labelled containers and sent for destruction by way of incineration. In countries where our standards are more stringent than the local regulations, we strive to adhere to our standards.

Guidelines followed by our MedSupply International fulfilment centres/ warehouses

MedSupply International has fulfilment centres across the world and each centre has its own unique procedure with respect to the destruction/disposal of medications in line with local regulations.

A disposal service is also offered to our clients for out of date products returned for destruction. The client must have prior authorisation before returning any items. On receipt, expired pharmaceuticals and consumables are segregated and placed in separate colour coded bags to ensure they are disposed of appropriately.

We have set in place an environmental policy to govern our environmental standards at all facilities.

Guidelines followed by medical services sites and clinics

Our Group Pharmacy Procedure outlines the pharmaceutical practices within the pharmacy services of our medical services sites and International SOS clinics globally. The procedure guides the storage, handling, dispensing and destruction of medication. It combines our corporate minimum standards for pharmacy management, with those local laws and regulations designed to prevent and reduce risks and errors.

Medications that have expired should be removed from the shelves during the end-of-month stock take. The medication should be destroyed as medical waste, according to the local regulations, with the support of an authorised and licensed pharmaceutical waste contractor. There are strict regulations regarding destruction of expired or damaged controlled medications in different jurisdictions; the regulations must be known and followed at all times.

Qualification of waste contractors

Each fulfilment centre has a different process but in general, as a part of ISO 14001, we have a Service Level Agreement with our waste contractor which is reviewed annually. We are expected to keep records and ensure that the contractor is licensed to perform the duties as required. The licenses are reviewed annually. For example, one of the centres in the United Kingdom has a ten-page supplier questionnaire that needs to be completed by the waste contractor and documented during every renewal.
No additional audit is conducted.

Annual quality and safety plan

The Quality and Safety Plan defines the annual objectives for the establishment, sustainability and/or improvement of quality, compliance and workplace safety within all MedSupply International fulfilment centres, and is subject to continuous review and updating.

Having raised awareness, we can see that change is happening and the enthusiasm and commitment among our employees is growing.

Go Green — Project Kijani

In line with our global commitment to continually embed sustainability practices into our business, we have formed Project Kijani to promote a cleaner, greener environment. 'Kijani' is Swahili for green.

We began in October 2017 by establishing our objectives and the project's phases. Our first step was to raise awareness among employees. The initiative was launched on Earth Day on 28 April 2018, with a short video and poster campaign encouraging people to 'Consume less' and 'Recycle more'.

The next phase, continuing throughout 2018, is to collate information on green initiatives in all our offices. Measuring what we are currently doing is an important starting point.

Case study: our Dubai office

Over the last 12 months:

- As an office, we have generated more than three tonnes of non-recyclable waste
- Our paper use consumed more than 50 trees
- Our total spend on consumables and paper was approximately US$18,200.

Our action points:

- **We aim to consume less by:**
  - Removal of consumable items and introduce 'Bring your own utensils'
  - Introducing central bins and bin-less desks
- **We encourage our employees to recycle more through:**
  - Increasing the number of recycle bins in the office
  - More effective use of current recycle bins
  - Printing less
  - Increased awareness

Phase 3, planned for 2019, will focus even further on the individual by asking the question: **What are you doing?**

We are drawing attention to the everyday opportunities to reduce water, gas and electricity consumption, save paper, and find alternatives to plastic water bottles. Those who bring in their own lunch are asked to supply their own utensils rather than single-use plastics. Instead of having waste bins at every desk, recycle bins are located at key points in the office.

We are encouraging employees to walk or cycle to work. Providing facilities, such as showers and lockers to support this, is part of our thinking when upgrading or moving offices.

Kijani team members have monthly calls to swap ideas and update each other. We are sharing progress and encouraging action through newsletter articles, infographics and other communications.

Having raised awareness, we can see that change is happening and the enthusiasm and commitment among our employees is growing.

Disposable kitchen items (per year)

Item	Pieces
Big plates	11,400
Cups	58,800
Bowls	7,200
Spoons	15,600
Forks	13,800
Knifes	6,000
Tea spoon	18,600
Small plates	8,400
Total	139,800

Waste bins

Item	Number of bins
Desk bins	194
General waste bins	10
Recycling bins	1
Big bins	56
Total	261

Paper usage

Item	kg per year
Shredded	2,460kg
General waste bins	4,100kg
Total	6,560kg

Case study: greener London headquarters

We selected Chiswick Park as the location of our London headquarters, in part because of the facility's strong green credentials. The building features:

- Recycling 90% of waste
- Capture of grey water, washroom taps to reduce water consumption and waterless urinals
- Automatic light shutoff and monitoring light/heat usage to identify waste
- Roof-mounted solar water heating
- Bike to work schemes
- Chemical reduction in cleaning, gardening and engineering activities

Case study: the KUDOS! Award

The KUDOS! Award is a London initiative where our people recognise a colleague 'on the spot' for doing something remarkable, particularly where it involves working collaboratively with other teams or functions.

Beginning in April 2018, we have honoured our KUDOS! awarded colleagues with a donation to Trees for Cities, the only charity working on an international scale to create greener cities. Since 1993, they have engaged over 70,000 people to plant over 770,000 urban trees in parks, streets, schools and housing estates across the UK, as well as internationally, revitalising these areas and improving the lives of the people who live in them.