INTERNATIONAL SOS

Information Security Policy

Version 2.00

POLICY

Document Owner: **LCIS Division**

Document Manager: **Group General Counsel**

Effective: ***August 2009***

Updated: ***April 2018***

WORLDWIDE REACH.
HUMAN TOUCH.

© 2018 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.

The only controlled copy of this document is maintained electronically. If this document is printed, the printed version is an uncontrolled copy.

Group	INTERNATIONAL SOS Information Security Policy	Policy

		DOCUMENT OWNER:	**LCIS Division**
EFFECTIVE DATE:	August 2009	**DOCUMENT MANAGER**:	Group General Counsel

Revision History

Revision	Rev. Date	Description	Prepared by	Reviewed by	Date	Approved by	Date
1.00	August 2009	**Original Document**	Group Information Security Manager	Group General Counsel	August 2009	Group Managing Director	August 2009
1.01	October 2012	Minor updates to para 2.1, 2.5 and 2.7	Chief Security Officer	Group GM Legal	December 2012	Group General Counsel	December 2012
1.02	February 2015	Transfer contents to new Policy template with new Intl.SOS logo	Group Manager Compliance	Group General Counsel	February 2015	Group General Counsel	February 2015
1.03	February 2016	Annual review of Policy according to Documents Policy	Group Manager Compliance	Group General Counsel	March 2016	Group General Counsel	March 2016
1.04	June 2016	Minor Update to para 2.8.1 - Removal of Safe Harbor reference.	Project Director, Legal	Group General Counsel	July 2016	Group General Counsel	July 2016
2.0	October 2017	Annual review	Group Manager Compliance	Group Deputy Director, Quality and Compliance Chief Security Officer Chief Data Privacy Officer Group Information Security Director	February 2018	Group General Counsel	April 2018

Responsibilities

All employees are required to comply with the policies in this document.

© 2018 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.

TABLE OF CONTENTS

1. INTRODUCTION

1.1.1. Information Security is a priority at International SOS. We devote significant resources to ensure the confidentiality, integrity and availability of our data. International SOS is committed to continuously evaluating and improving our Policies, standards, processes and information systems in supporting business and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements.

1.1.2. As a modern, forward-looking business, International SOS recognises the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, employees and other stakeholders.

1.1.3. In order to provide such a level of continuous operation, International SOS has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

1.1.4. This information security policy forms a key part of our set of controls to ensure that our information is protected effectively and that we can meet our obligations to our customers, employees, and other stakeholders.

2. THE POLICY

To achieve these information security objectives, we adopt industry standards and best practices in each of the following control domains:

2.1. Information Security Policy

2.1.1. This information security policy states our intent to maintain a secure information-processing environment and to protect information assets. This policy has been approved by the AEA Board of Directors and must be communicated to International SOS employees. It will be reviewed and updated annually. The policy will also be updated as and when there is any change in the information-processing environment, which may have an impact on the information risk profile.

2.2. Security Organisation

2.2.1. An Information security governance structure and information security management system has been established within the organisation to facilitate the strategic direction on information security and implementation of security controls across the organisation.

2.3. Asset Management

2.3.1. The inventory and asset ownership must be defined and mandated using standard requirements. Respective information owner and custodians must maintain an inventory of information assets to ensure that these assets are effectively protected. An annual review of inventory of information assets must be performed by respective asset owners and custodians. Standard requirements must define the security configuration management of key IT assets.

2.3.2. Information assets must be classified and handled as per the data classification standards or restricted data handling standards. An acceptable use standard has been documented to define the rules for protection and proper use of information assets including but not limited to electronic media (such as the internet, and company-provided email), and supporting systems such as desktops and laptops.

2.4. Human Resource Security

2.4.1. Security roles and responsibilities of employees, contractors and third party users are to be documented and communicated to all employees, contractors and third party users.

2.4.2. All International SOS employment contracts must include employees' responsibilities for information security such as provisions regarding non-disclosure of confidential information, information security, compliance with applicable policies, laws, copyrights and our code of conduct.

2.4.3. All employees must go through the approved background verification checks to ensure the authenticity of the person and to reduce the likelihood of insider threats to critical information assets. The background verification must include verification of employment history, academic and professional qualifications, and reference checks of prospective employees. Criminal records checks, litigation and insolvency checks must be carried out based on their applicability under local laws, client requirements, and respective job profiles.

2.4.4. International SOS employees and third party personnel working for International SOS must complete training on International SOS's policies, which includes the completion of e-learning modules on information security and data protection within 60 days of joining the organisation. This e-learning should be tested or refreshed annually and non-compliance should be reported to respective managers, business unit heads and the Information Security Management Committee.

2.4.5. To ensure that employees are kept up-to-date on information security policies, standards and procedures, periodic information security awareness e-mails must be sent to all employees, contractors and third party users. Also, managers should ensure that employees, contractors and third party users are briefed to apply security principles in accordance with established policies, standards and procedures.

2.4.6. Although each country may have specific disciplinary and employment termination policies (to comply with local legal requirements) the information security policy requirements must be documented in all such policies, approved and communicated to ensure the correct and fair treatment for employees who are suspected of committing breaches of security. The policies shall provide a framework for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business.

2.4.7. The process for termination of contracts of employment must be documented, approved and communicated to respective HR partner/ representative together with supervising manager of the person leaving. Respective HR partner/ representative must ensure that employees are not provided with experience letters or service letters unless the employee/ contractor's access is revoked by information technology service desk. To ensure this, an exit checklist must be exercised documenting the revocation of system permissions, access rights, and the return of company assets.

2.4.8. In case of and based on an internal transfer, the respective Human Resources team must inform the responsible managers. Respective managers must ensure that access rights on information assets and information processing facilities are adjusted in accordance to the access control policy and 'need to have' principle.

2.5. Physical Security

2.5.1. International SOS Information processing facilities (server room, data centre, communications room, etc) must be protected against unauthorized access and damage.

2.5.2. All International SOS facilities must have an up-to-date Site Security Plan which describes the local risk profile and protection approach for that location.

2.5.3. Physical access to Server Rooms must be controlled in accordance with the Server Room Physical Access Procedure. Access control to these sensitive areas must include a two-factor authentication system. All International SOS employees must display their photo ID badge at all times whilst on the premises. Coloured lanyards should be used to indicate the person's identity as a permanent employee, contractor, or visitor.

2.5.4. Visitor access must be controlled through a manned security point or reception area. Visitors should be issued with serially-numbered visitor badges and should sign an acknowledgement of our confidentiality and safety standards. Visitors should be escorted by an International SOS employee and the visitor access should be reviewed on a monthly basis. These visitor logs should be retained for 90 days.

2.5.5. Closed Circuit Television (CCTV) surveillance systems should be installed in all International SOS Assistance Centres, Clinics and in all facilities that house server rooms or data centres.

2.5.6. These systems must support continuous recording and these recordings are to be retained for a minimum period of 90 days (subject to local legal requirements).

2.5.7. Environmental conditions such as temperature and humidity should be continuously monitored and controlled in data centres and server rooms.

2.5.8. An emergency response plan must be in place and periodic staff training on firefighting and simulated fire evacuation drills must be conducted at regular intervals.

2.5.9. Facility keys should be maintained and secured by the administration team. The keys should only be provided for a business purpose to authorised individuals only.

2.5.10. International SOS facilities must prohibit, smoking, unauthorised photographic, unauthorised video/ audio recording.

2.5.11. Information assets such as documents, printed outputs, correspondence, computer media (IT personnel), must be kept in locked drawers and/or cabinets when not in use. Monthly internal audits must be performed and records should be maintained regionally. The non-compliance must be reported.

2.6. Operations Security

2.6.1. Secure log-on controls such as log-on banner, two-factor authentication, account lockout features, and logging of log-on attempts must be implemented to prevent unauthorized access to information systems.

2.6.2. Mobile devices must be configured with mobile device security settings such as encryption, complex password etc.

2.6.3. Business Wi-Fi must be secured with secure wi-fi configuration settings and protocols such as WPA2 Enterprise, AES, RADIUS, etc. It must not use the weak security controls such as WEP, WPA-PSK, LEAP, TKIP etc.

2.6.4. Servers, databases and web servers must be configured as per internal security configuration standards. An annual compliance review must be performed to validate the technical configuration compliance.

2.6.5. All changes must be controlled and managed as per the change management procedure. This procedure provides details on Normal and Emergency change requests.

2.6.6. Only authorized and approved hardware and applications may be installed in the International SOS environment. All new applications and systems must go through a security assessment before release to production.

2.6.7. Anti-Virus software must be used for prevention of virus, worms and Trojan outbreaks. It should be configured to receive virus definition update on a daily basis. It should also be configured to scan the servers on a weekly basis and laptop/ desktops on a daily basis.

2.6.8. All laptops must be installed with disk encryption software with AES 256 as the encryption protocol.

2.6.9. All emails should be protected via email content filter and all internet traffic should be protected via web content filter.

2.6.10. A patch management policy has been documented and communicated to relevant stakeholders. The security patches, packages, and hotfixes must be applied as per the criticality of patches on applications, servers, backup systems, storage systems and network devices, as applicable.

2.6.11. An acceptable use standard has been documented and communicated to all employees. It states the rules for protection and proper use of group assets including but not limited to electronic media (such as the internet, and company-provided email), and supporting systems such as desktops and laptops.

2.6.12. A computer protection standard has been documented and communicated to all relevant stakeholders. It mandates the use of antivirus, disk-based encryption software, cable lock, remote VPN software, and standard requirements for screen lock and password protection.

2.6.13. A data retention, archiving and destruction policy has been documented and communicated to relevant stakeholders. It defines the requirements for data retention and archival. It also mandates the secure disposal of information.

2.6.14. Information system backups must be maintained and tested regularly for the purpose of data recovery in case of events such as system crash, virus attack or accidental deletion of information.

2.6.15. Backup procedures must define the data backup frequency, storage of backup media, labelling convention for backup media, retention of, and restoration from, backup media and movement of tapes to an offsite location for backup management.

2.6.16. A Firewall Management Standard has been documented and communicated to relevant stakeholders. It defines the requirements for firewalling between International SOS Network and any non-International SOS network to segregate trusted and un-trusted networks and limit access between such networks.

2.6.17. A Remote Access and VPN Standard has been documented and communicated to relevant stakeholders. It outlines requirements for employees, business partners and personnel affiliated with contracted third parties on secure connection with the International SOS network and safeguard International SOS information against unauthorized access.

2.6.18. A Security Log Management Standard has been implemented for logging and collection of system security logs, database logs, firewall logs, IDS and HIPS logs and web server logs. It should also define the high risk activities across these technologies to be reviewed in Security Information and Event Management (SIEM) system.

2.6.19. A Vulnerability Management Standard has been documented and communicated to relevant stakeholders. International SOS Group Information Security must perform the vulnerability assessment and penetration testing of IT infrastructure and applications as per the following schedule:

- Internal Patch Scan – Monthly
- Internal Vulnerability Assessment – Quarterly
- Internal Configuration Assessment - Quarterly
- External Vulnerability Scan and Pen Testing – Annual

2.6.20. The business function owner is accountable and the assigned asset custodian is responsible for remediation of identified findings.

2.6.21. All unauthorised scans must be blocked by the respective network team as directed by security operations. International SOS doesn't allow customers/clients initiated vulnerability assessment and penetration tests on IT infrastructure and applications due to shared nature of applications and infrastructure systems behind our firewalls.

2.6.22. A Data Loss Prevention Standard has been documented and communicated to relevant stakeholders. It defines the requirements for data loss prevention (a.k.a. DLP) within International SOS.

2.6.23. An Internet Access Policy and Social Media Policy has been documented and communicated to relevant stakeholders. It defines the rules for internet access and use of social media.

2.6.24. Email Policy has been documented and communicated to relevant stakeholders. It defines the rules for email access and use.

2.7. Systems Development and Maintenance Cycle

2.7.1. A Product Development Standard has been documented and communicated to relevant stakeholders. It defines the ownership of products and product security within respective business function. A product must not be shipped to market unless the information security risk management has been performed and signed-off by business function owner.

2.7.2. A High-Risk Application Security Standard has been documented and communicated to relevant stakeholders. It states the mandatory steps for secure application development and infrastructure build such as documentation of security requirements, secure coding practices, code reviews, vulnerability assessment, penetration testing and remediation. It also mandates infrastructure security requirements such as network firewall, zone segmentation, intrusion detection, web application firewall, patch management, and antivirus.

2.8. Access Management

2.8.1. An Access Control Policy has been documented and communicated to relevant stakeholders. It describes the rules and refers to procedures related to access management, unique identification, privilege access, annual reviews and removal of access rights.

2.8.2. An Account and Password Management Standard must be documented and communicated to relevant stakeholders. It should outline the requirements for creation, protection, length, complexity, history of passwords.

2.9. Encryption Management

2.9.1. An Encryption Management Standard has been documented and communicated to relevant stakeholders. It defines the requirements for the encryption of information in transit and at rest. It also defines the requirements for digital certificate management.

2.10. Supplier Management

2.10.1. An External Vendor Security Management Standard must be documented and communicated to relevant stakeholders. It must define the requirements related to supplier risk assessment and criteria for on-boarding and on-going security assessments of external vendors/ suppliers.

2.10.2. All contracts with suppliers must have security requirements defined with respect to the type of services provided by supplier and the associated impact on information security posture of International SOS. External vendors must confirm in writing that they adhere fully to the requirements of the European Union General Data Protection Regulation (GDPR), and the internal assessment of such vendors must corroborate this and be approved by the ISMC.

2.11. Business Continuity Management

2.11.1. Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) have been developed and documented for each material facility and business line. These plans establish the roles and responsibilities of our teams for business continuity and recovery processes.

2.11.2. Each Business Continuity Plan and Disaster Recovery Plan must be updated and tested on an annual basis at a minimum.

2.12. Information Security Incident Management

2.12.1. An Information Security Management Procedure has been documented and communicated to relevant stakeholders. Information Security Incidents must be effectively monitored, reported, and investigated to ensure that corrective actions are taken to control and remediate security incidents in a timely manner.

2.12.2. Information security incidents that require breach notification requirements to clients, regulatory bodies, and media should be managed as per the Data Breach Contingency Plan. International SOS must report to customers in writing and as soon as reasonably practicable after we become aware of any material breach of security of their data, in accordance with our Data Protection Policy and applicable laws.

2.13. Compliance

2.13.1. A Legal and Regulatory Requirements Procedure has been documented and shall be maintained by the Legal, Compliance, Insurance and Security (LCIS) function. It provides the guidelines to identify the statutory, regulatory, and contractual requirements and our approach to meet these requirements for each facility and information system.

2.13.2. International SOS must comply with the requirements of European Union General Data Protection Regulation (GDPR) and legislation in key jurisdictions such as France, Singapore, Germany, United Kingdom, Australia and United States. At a minimum, International SOS shall maintain the following:

- Registration of International SOS legal entities as required under GDPR
- Binding Corporate Rules sanctioned by the European Community's data protection authorities, approved by the French Data Protection Authority (CNIL); and
- Contractual commitments with our customers and vendors.

3. RESPONSIBILITY

3.1. All employees and contractors are required to read, understand and abide by International SOS's data protection and information security requirements. Employees are required to sign an Information Security Policy statement and a confidentiality agreement. Standard form agreements with contractors contain obligations with regard to data protection and confidentiality.

4. ENFORCEMENTOF THIS POLICY

4.1. Breaches of this Policy may have serious legal and reputation repercussions and could cause serious damage to International SOS.

4.2. If any employee is found to have breached this policy, they will be subject to disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

4.3. If you do not understand the implications of this policy or how it may apply to you, seek advice in the first instance from your immediate manager.

© 2018 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.