INTERNATIONAL SOS

Information Security Policy

Version 1.04

POLICY

Document Owner: **LCIS Division**

Document Manager: **Group General Counsel**

Effective: ***August 2009***

Updated: ***July 2016***

WORLDWIDE REACH.
HUMAN TOUCH.

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

Responsibilities

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

TABLE OF CONTENTS

1. INTRODUCTION

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.

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. We have adopted an Information Security Policy and Standards that are aligned with ISO/IEC 27002. These are constantly being reviewed and updated by the Information Security Management Sub-Committee (ISMC). The ISMC is responsible for developing the information security framework and enforcing the Information Security Policy across the International SOS Group. The International SOS Data Protection Steering Committee provides business input into the development of the information assurance strategy, and oversees the work of the ISMC.

2.2. Organizational Security

2.2.1. The protection of information assets is the responsibility of every employee at International SOS. To ensure that the information security objectives are achievable and the Information Security Policy is complied with, we have created an Organizational Security structure with the mission to plan, manage and implement effective information protection controls.

2.3. Human Resource Security

2.3.1. Our Human Resource Security controls also include background checks and security clearances that are required for specific positions, to ensure that staff who have access to sensitive information have been appropriately vetted.

2.4. Systems Development and Maintenance Cycle

2.4.1. Information systems changes follow a stringent change and release control process that includes user testing and acceptance and quality acceptance, prior to implementation. Controls such as risk assessments, development checklists and secure coding are incorporated in the Systems Development and Maintenance Cycle to ensure that security is properly addressed in the information systems that we develop.

2.5. Access Control

2.5.1. Sensitive information is restricted on a least-privilege basis, with access controlled based on the business requirements. This approach aims to reduce the risks associated with misuse, including: alteration, destruction and unauthorized dissemination of information.

2.6. Business Continuity Management

2.6.1. Our Business Continuity Management involves the assessment of a variety of risks to organizational processes and the creation of standards, procedures and processes and plans to minimize the impact those risks might have on the organization and our customers if they occur.

2.7. Information Security Incident Reporting

2.7.1. We have put in place an Information Security Incident Reporting process that tracks and monitors incidents. The information security team investigates and leads the follow up actions within twenty-four hours of all Priority 1 incidents. All material incidents are also reported and reviewed by the Information Security Management Committee on a monthly basis.

2.8. Compliance

2.8.1. Our employees are bound by laws and regulations to protect personal data in the countries in which we do business and in which we gather, store and transfer personal data. We have implemented an enforcement plan to assure the effectiveness of our Data Protection Policy. We strive to ensure Compliance with the law and with industry standards such as the Data Protection Binding Corporate Rules regime in the European Union. The Data Protection Policy can be found at http://www.internationalsos.com/en/files/Policy_DataProtection.pdf.

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 Intl.SOS. Consequently, breaches can potentially lead to disciplinary action.