INTERNATIONAL SOS

INTERNATIONAL SOS

Data Retention, Archiving and Destruction Policy

Version 1.10

POLICY

Document Owner: **LCIS Division**

Document Manager: **Group General Counsel**

Effective: ***January 2009***

Updated: ***March 2017***

WORLDWIDE REACH.
HUMAN TOUCH.

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** **Data Retention, Archiving and Destruction Policy**	**Policy**

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

Revision History

Revision	Rev. Date	Description	Prepared by	Reviewed by	Date	Approved by	Date
1.00	January 2009	**Original Document**	Group GM Compliance	Group General Counsel	January 2009	Group Managing Director	January 2009
1.01	May 2009	Format to Documents Policy compliant	Group GM Compliance	Group General Counsel	May 2009	Group General Counsel	May 2009
1.02	December 2009	Amended Document Classification from “Intl.SOS Internal” to “Public” and placed the Policy on www.internationalsos.com website for client tender purposes	Group Manager Compliance	Group General Counsel	December 2009	Group General Counsel	December 2009
1.03	March 2013	Standard review and update of at least once every 3 years according to Documents policy	Group GM Legal	Group General Counsel	March 2013	Group General Counsel	March 2013
1.04	July 2013	Amended Document Classification from “Public” to “Intl.SOS Internal” and removed the Policy from www.internationalsos.com website	Group Manager Compliance	Group General Counsel	July 2013	Group General Counsel	July 2013
1.05	July 2014	• Changed Document Classification from “Intl.SOS Internal” to Public” • Amended Retention Policy, Archiving Policy, Destruction Policy • Included exceptions to the retention period • Amended Annex 1 and 2	Group GM Legal	ISMC	July 2014	Group General Counsel	August 2014
1.06	January 2015	Minor tweak to paragraph 2.3	Group Manager Compliance	Group GM Legal	January 2015	Group General Counsel	January 2015
1.07	February 2015	Transfer contents to new Policy template with new Intl.SOS logo	Group Manager Compliance	Group GM Legal	February 2015	Group General Counsel	February 2015
1.08	February 2016	Annual review of Policy according to Documents Policy	Group Manager Compliance	Group General Counsel	March 2016	Group General Counsel	March 2016
1.09	September 2016	Update to requirements for retention of Aspire Lifestyles Concierge Centres	Chief Security Officer	Group GM Aspire Lifestyles Operations, Group Senior Manager, Concierge Operations Group Information Security Director	September 2016	Group General Counsel	September 2016
1.10	March 2017	Minor typo error in Annex 1 Definition of “Active Use”	Group Manager Compliance	Group GM Legal	March 2017	Group General Counsel	March 2017

Responsibilities

All employees are responsible to comply with the policies and procedures in the Data Retention, Archiving and Destruction Policy.

TABLE OF CONTENTS

1. INTRODUCTION....4
1.1. Introduction....4
1.2. Objectives....4
2. RETENTION POLICY....5
3. ARCHIVING POLICY....6
4. DESTRUCTION POLICY....7
5. EXCEPTIONS TO THE RETENTION PERIOD....7
6. RESPONSIBILITIES....7
7. ENFORCEMENT AND REPORTING BREACHES....8
Appendix 1: RETENTION PERIODS....9
Appendix 2: EXCEPTION REQUEST / LITIGATION HOLD FORM....10

1. INTRODUCTION

1.1. Introduction

1.1.1. This Data Retention, Archiving and Destruction Policy (the "Policy") has been adopted by International SOS in order to set out the principles for retaining, reviewing and destroying data. This Policy covers all employees (whether full time or not) and all directors and officers of the International SOS group, where ever they may be located or working. We also expect our consultants and goods and services providers to introduce and follow appropriate data retention practices.

1.1.2. This Policy covers all data retained or in International SOS’s custody or control in whatever medium such data is contained in. This Policy is not therefore restricted to information contained in paper documents but includes data contained in an electronically readable format. For the purposes of convenience, in this Policy, the medium which holds data is called: “a Document”.

1.1.3. This Policy should be read in conjunction with other policies that have as their objectives the protection and security of data such as the Data Protection Policy and the Information Security Policy.

1.2. Objectives

1.2.1. International SOS is bound by various obligations with regard to the data that we retain or that is in our custody or under our control. These obligations include how long we may retain data and when and how we can destroy it. The obligations may arise from local laws or regulations or from contracts and promises that we have made to our employees, customers, goods and service providers and our partners.

1.2.2. Further, International SOS may be involved in unpredicted events such as litigation or business disaster recoveries that require us to have access to the original Documents in order to protect International SOS’s interests or those of our employees, customers, goods and service providers and our partners.

1.2.3. As a result, Documents may need to be archived and stored for longer than the data may be needed for day to day operations and business processes. A contract may, for example, expire after two years but other Documents may, by law, need to be retained for a longer period.

1.2.4. Broadly, when the Document Retention Period is over and we no longer need the Document, we ought to destroy it in a proper manner.

2. RETENTION POLICY

2.1. Retention is defined as the maintenance of documents in a production or live environment which can be accessed by an authorized user in the ordinary course of business. For the avoidance of doubt, Documents used in staging, development, and testing or draft versions of Documents shall not be retained beyond their active use period nor copied into production or live environments.

2.2. The retention period of a Document shall be an active use period of two years unless an exception has been obtained permitting a longer or shorter active use period by the business unit or division ("Function") responsible for creating, using, processing, disclosing storing and destroying the document.

2.3. After active use has expired and according to appropriate exceptions, Documents shall be archived in accordance with section 3 until the Documents are destroyed in accordance with section 4.

2.4. For the purposes of enforcing retention in accordance with this policy each function is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list of document types across International SOS by function is attached as Annex 1. This list shall be maintained by each Function.

2.5. Each Head of Function shall be responsible for enforcing the retention, archiving and destruction of Documents, and communicating these periods to the relevant employees.

2.6. Each Head of Function shall be responsible for submitting exception requests to the process, including consulting and receiving legal advice if necessary to justify making an exception request under section 5.

2.7. The Legal Department may issue a litigation hold request to the Head of Function which requires that documents relating to potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be retained in accordance with instructions from the Legal Department.

2.8. Each employee shall be responsible for returning Documents in their possession or control to Intl.SOS upon separation or retirement. Final disposition of such Documents shall be determined by the immediate supervisor in accordance with this policy.

3. ARCHIVING POLICY

3.1. Archiving is defined as secured storage of Documents such that Documents are rendered inaccessible by authorized users in the ordinary course of business but which can be retrieved by an administrator designated by the head of function for the Documents in question.

3.1.1. Paper records shall be archived in secured storage onsite or secured offsite location, clearly labelled in archive boxes naming the Head of Function, department or division and date to be destroyed.

3.1.2. Electronic records shall be archived in accordance with International SOS Information Security Standards for access controls and in a format which is appropriate to secure the confidentiality, integrity and accessibility of the Documents.

3.2. The archiving period of a document shall be seven (7) years unless an exception has been obtained permitting a longer or shorter active use period by the Head of Function responsible for creating, using, processing, disclosing storing and destroying the Document.

3.2.1. An archiving period of more than seven (7) years may be granted by exception for Documents with a vital historical purpose such as corporate records, contracts, technical knowhow. The Head of Function will request an exception in accordance with section 5 to archive Documents. Such exception request shall specify the administrative, organizational and technical measures to be undertaken to ensure the confidentiality, integrity and availability of such Documents.

3.2.2. An archiving period of less than seven (7) years may be granted by exception for documents with a limited business purpose such as emails, OCS messages, travel itineraries, pre-trip advisories, or to comply with client or industry requirements (for example PCI).

3.3. After the archival period has expired, Documents shall be destroyed in accordance with section 4.

3.4. For the purposes of enforcing archiving in accordance with this policy each function is responsible for the Documents it creates, uses, stores, processes and destroys. A sample list of Document types across International SOS by function is attached as Annex 1. This list shall be maintained by each Head of Function.

3.5. The Legal Department may issue a litigation hold request to the Head of Function which requires that documents relating to potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be archived in accordance with instructions from the Legal Department.

3.6. Each Head of Function shall be responsible for enforcing the retention, archiving and destruction of Documents, and communicating these periods to the relevant employees.

4. DESTRUCTION POLICY

4.1. Destruction is defined as physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

4.2. Intl.SOS Corporate IT and Regional IT shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files. Paper Documents shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by security screened personnel for disposal.

5. EXCEPTIONS TO THE RETENTION PERIOD

5.1. Exceptions may be requested under the following circumstances:

5.1.1. The Head of Function shall review and submit to the Intl.SOS Information Security Management Committee an exception request to archive data for a different period as prescribed in Annex 1. The reasons may be a client requirement, business requirement, legal requirement or vital historical purpose.

5.1.2. The Exception Request Form shall be reviewed and approved by the Intl.SOS Information Security Management Committee and routed to the Head of Location and Corporate or Regional IT to enforce as shown in Annex 2.

5.2. Documents which consist of Designated Medical Records as defined in Annex 2 shall be archived for 30 years in accordance with regulations requiring the retention of Medical Records.

5.3. Documents for which the Legal Department has issued a Litigation Hold Order shall be archived retained and destroyed as specified by the Legal Department.

6. RESPONSIBILITIES

6.1. Heads of Functions shall be responsible for implementing this Policy and ensuring that employees understand this Policy and that they perform the processes and procedures to execute this Policy.

6.2. The Compliance Department shall be responsible for auditing compliance with this Policy and providing an audit report with recommendations to be reviewed by the Group General Counsel, in the capacity of Chairman of the Information Security Committee and by the relevant senior management.

7. ENFORCEMENT AND REPORTING BREACHES

7.1. Breaches of this Policy may have serious legal and reputation repercussions and could cause material damage to International SOS. Consequently, breaches can potentially lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.

7.2. All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor or the Group General Counsel. Reports made in good faith by someone who has not breached this Policy will not reflect badly on that person or their career at Intl.SOS. Reports may be made using the following e-mail address: Compliance@internationalsos.com.

Appendix 1: RETENTION PERIODS

Division or Function			Retention Period	Archival Period
Human Resources			2 years	7 years
Finance			2 years	7 years
Legal			2 years	7 years
IT			2 years	7 years
ITG			2 years	7 years
Sales & Marketing			2 years	7 years
Medical Services			2 years	7 years
Operations			2 years	7 years
Security Services			2 years	7 years
Concierge Services	Aspire Lifestyles Services	ePC – CVV2	72 hours	not applicable
		ePC – Inactive card data	90 days	not applicable
		ePC – inactive case records (no PAN or CVV2)	2 years	7 years
		Call Recordings	1 year (standard) or 90 days to 1 year based on contractual requirements	not applicable
		Audit logs	3 months online	1 year minimum
	Aspire Lifestyles Membership		2 years	7 years

Term	Definition
"Active Use" / "Hot Data"	Active use shall be two years unless an exception is submitted and approved by the Head of Function.
"Medical Records"	Medical Records shall be destroyed 30 years after active use or upon decommissioning, whichever is earlier. Medical Records are those records created, stored, used and disclosed by Intl.SOS Abermed, Topside Response Centers, Global Response Centers, Clinics, MedAire, Medfit, Medlink, Medsite, records created during medical transport or related services which contain the evaluations, opinions and/or conclusions of licensed medical professionals employed by or operating at the control and direction of Intl.SOS. For the avoidance of doubt, case records created in the normal course of rendering assistance by Intl.SOS Assistance Centres or by third-party medical providers and provided to Intl.SOS in the normal course of rendering assistance shall be destroyed in accordance with business records destruction period above.
"Assistance Centre Records"	Minors records will be kept in line with the records defined as "Medical Records".
"Litigation Hold"	LCIS may issue a 'hold order' to IT and any relevant division to preserve all information relative to threatened or pending litigation, regulatory action or government order. Such hold order shall appoint a custodian of records and specify a location for storage and review of documentation.
"Vital Historical Records"	Vital Historical Records shall be archived for 50 years after active use. Vital Historical Records shall include Occupational Health clinic records, Norway clinic records, Occupational health check records, MedSite records, Health surveillance, preemployment / predeployment health checks, contracts, corporate secretarial records.

Exceptions Process	Rationale and Process
Requests to destroy records in advance of schedule	Provide rationale to ISMC for approval, ISMC to then send approval to IT to destroy.
Requests to retain records and archive rather than destroy	Provide rationale to ISMC For approval, ISMC to then send approval to IT to archive.

Appendix 2: EXCEPTION REQUEST / LITIGATION HOLD FORM

Information Security Exception Request Form (ISERF)

Instructions:
The Information Security Exception Request Form below is required whenever a business unit or organization within Intl.SOS would like to deviate from the Intl.SOS Data Retention, Archiving and Destruction Policy ("Policy") and the Information Security Standards. The instructions below are designed for use by Heads of Functions when requesting an exception to the standard retention schedule of active use + 7 years as outlined in Annex 1 of the Policy.

The type of exception request you can submit is:
To obtain approval to archive data for less than seven years and destroy it.
To obtain approval to archive data for more than seven years and stop its destruction.

Submit this form to the Head of Function for review before submission to the ISMC for final approval (or rejection).

Item	Item Description	Explanation
1.	Policy Name or Standard Name in Reference:	The Intl.SOS Data Retention, Archiving and Destruction Policy requires that data be archived for seven years after active use and then destroyed. The I Policy implements this mandate by requiring that all systems prompt the owner of a particular dataset to approve archival seven years from the last date stamp of the record in question.
2.	Reference Number/ Control ID/ Clause Number in Reference:	The policies you are requesting an exception from are listed here. The form is pre-populated for your convenience. Do not change or amend this section.
3.	Location Scope: Region (or Site) and Scope Storage) for which this Exception Request Form applies to:	Insert your Region (or Site) and the Client Name for which you are requesting this exception.
4.	Technology Scope: Name of Application / System / Database / Storage / Network Equipment for this Exception Request Form applies to:	Insert the name of the application, system, database, storage medium or network equipment for which you propose to modify the retention schedule.
5.	Organisation Scope: (Infrastructure Projects / Business Applications / Internet Technologies / IT Operations / Others (please specify)) for which this Exception Request Form applies to:	Insert the name of your organization or business unit here.
6.	Description and Reason for the Non-Compliance:	Describe your request in detail by answering the following questions: 1. What is the business justification for the request? 2. Who will be responsible for answering queries related to this request? 3. What assurances exist that this request is in keeping with contractual requirements and local laws?
7.	Benefits to Business or Services if the exception is 'Approved':	Explain what the commercial benefit to Intl.SOS is of approving this request.
8.	Impact on Business or Services (i.e. Cost, Schedule, Efforts) if the exception is 'Denied':	Explain what the commercial impact to Intl.SOS if this request is NOT approved.
9.	Description of Risk associated with Non-Compliance:	Please describe the risks associated with your proposal to either shorten the archival period or hold records for a longer period.
10.	Proposed Plan for Managing the Risk associated with Non-Compliance (Complementary Security Controls):	Specify how the risk of incomplete deletion or excessive deletion will be managed? 1. If you wish to destroy information earlier before the 7 year period has elapsed, how will you ensure that the information you wish to destroy is rendered technically irretrievable? 2. If you wish to retain data for longer than seven years, how will you ensure that the information you wish to archive is stored in a format that is technically retrievable?
11.	Anticipated Duration for the Exception:	Please specify whether this is a one-time request or a standing order.
12.	Ownership to Accept the Risk:	Please insert the approval of WHAT LEVEL here after their review.
13.	Ownership to Enforce Compliance after Exception Expiry:	Please indicate the person who is responsible for ensuring that your approved request is submitted to IT or other data administrator for execution.

14.	Additional Information from Requester (If required):	Any additional information you would like to provide should be stated here.

Important Note

This exception request form should be used only if there is a clear legal or business need to either retain or destroy the data in question.

Requester's Information (To be filled by the Requester)

Name:	Designation:	Phone #:	E-Mail:	Location (Region / Site):

Deviation Details (To be filled by the Requester)

#	Details	Requester's Response (Click to fill)
1.	Policy Name or Standard Name in Reference:	International SOS Data Retention, Archiving and Destruction Policy
2.	Reference Number/ Control ID/ Clause Number in Reference:	International SOS Data Retention, Archiving and Destruction Policy
3.	Location Scope: Region (or Site) and Scope Storage) for which this Exception Request Form applies to:	
4.	Technology Scope: Name of Application/ System/ Database/ Storage/ Network Equipment for this Exception Request Form applies to:	
5.	Organisation Scope: (Infrastructure Projects/ Business Applications/ Internet Technologies/ IT Operations/ Others (please specify)) for which this Exception Request Form applies to:	
6.	Description and Reason for the Non-Compliance:	
7.	Benefits to Business or Services if the exception is 'Approved':	
8.	Impact on Business or Services (i.e. Cost, Schedule, Efforts) if the exception is 'Denied':	
9.	Description of Risk associated with Non-Compliance:	Intl.SOS is committed to ensuring adequate information security which includes retaining, reviewing and destroying information when such information no longer serves a business purpose. Absent such controls, Intl.SOS is at risk of contravening its obligations under our Data Protection Policy, Binding Corporate Rules, Documents Policy and applicable data privacy laws for which monetary fines, contractual penalties and reputational harm can result.
10.	Proposed Plan for Managing the Risk associated with Non-Compliance (Complementary Security Controls):	
11.	Anticipated Duration for the Exception:	
12.	Ownership to Accept the Risk:	
13.	Ownership to Enforce Compliance after Exception Expiry:	
14.	Additional Information from Requester (If required):	

ISMC Decision (Approval/ Denial), For ISMC Use Only

Decision on Exception request	☐ Approved	☐ Denied	☐ More Info Needed

#1 Name:	Sign/ Attach Approval Email	Date:
#1 Name:	Sign/ Attach Approval Email	Date: