INTERNATIONAL SOS

Data Retention, Archiving and Destruction Policy

Version 2.03

POLICY

Document Owner: **Legal**

Document Manager: **Group General Counsel**

Effective: ***January 2009***

Updated: ***February 2021***

WORLDWIDE REACH.
HUMAN TOUCH.

Group	INTERNATIONAL SOS Data Retention, Archiving and Destruction Policy	Policy

		DOCUMENT OWNER:	**Legal**
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
2.00	December 2017	Extensive revisions introducing Data Asset and local data inventories, update to retention periods, distinction between Personal Data, Account Data and other Data, distinction between Documents and Records, addition of Appendix 2: Document and Record Types	Data Protection Officer Europe	Chief Security Officer Chief Data Privacy Officer	August 2018	Group General Counsel	August 2018
2.01	August 2019	• Adds and clarifies definition "Data Processing" (1.2.8) • Definitions and diagram to clarify Data Processing, back-up and archival (1.3.) • Replacement of departmental record requirements with Data Inventories (2.0) • Clarify retention periods (3.1)	Data Protection Officer Europe	Chief Security Officer Chief Data Privacy Officer	August 2019	Group General Counsel	August 2019

Group	INTERNATIONAL SOS Data Retention, Archiving and Destruction Policy	Policy

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

Revision History

Revision	Rev. Date	Description	Prepared by	Reviewed by	Date	Approved by	Date
2.02	December 2020	Update retention period for call recordings (3.1)	Group Deputy Director Assistance Operations; Head, Group Business Applications	Chief Security Officer	January 2021	Group General Counsel & ISMC	February 2021
2.03	February 2021	Update retention period for call recordings (3.1)	Group Deputy Director Assistance Operations; Head, Group Business Applications	Chief Security Officer	February 2021	Group General Counsel	February 2021

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

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 and destroying specified categories of data.

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

1.2. Definitions

1.2.1. "**Account Data**" consists of cardholder data and/or sensitive authentication data.

1.2.2. "**Anonymisation**" is the process of turning data into a form which does not identify individuals. It is a type of information sanitization whose intent is privacy protection.

1.2.3. "**Archiving**" is the process of moving data that is no longer actively used to a separate storage device or location for retention.

1.2.4. "**Asset Owner**" is the Functional or Business Line Head who is responsible for the Data Asset (or within whose function or business line the Data Asset resides or is used).

1.2.5. "**Case Records**" are records maintained in New Case or other database systems which relate to the membership services offered and delivered to customers and their employees.

1.2.6. "**Data**" is Record and Document.

1.2.7. "**Data Asset**" is any item or entity that comprises data. For example, databases are data asset that comprise records. A data asset may be a system or application output file, database, document, or webpage. A data asset may also include a means to access data from an application.

1.2.8. "**Data Processing**" is the collection and manipulation of data to produce meaningful information. Processing includes transformation, accessing, updating, transferring, destruction and any other manipulation of data.

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

1.2.10. "**Document**" as used in this Policy, is any medium which holds Information used to support an effective and efficient organizational operation. Examples of Documents include:

(a) Policies

(b) Quality Criteria

(c) Procedures

(d) Tools and Templates

1.2.11. "**Financial Records**" is pieces or sets of information related to the financial health of a business. The pieces of data are used by internal management to analyze business performance and determine whether tactics and strategies must be altered

1.2.12. "**Litigation Hold Order**" Legal 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.

1.2.13. "**Personal Data**" (also "Personally Identifiable Information") is any information relating to an identified or identifiable natural person (the "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2.14. "**PCI DSS**" The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. It was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually.

1.2.15. "**Record**" as used in this Policy, is any medium which holds information or evidence about a past event. Examples of Records include:

(a) Case records

(b) Reports

(c) Minutes

(d) Video and audio recordings

(e) Data generated by physical access control systems

1.3. Definitions in Context of Data Processing

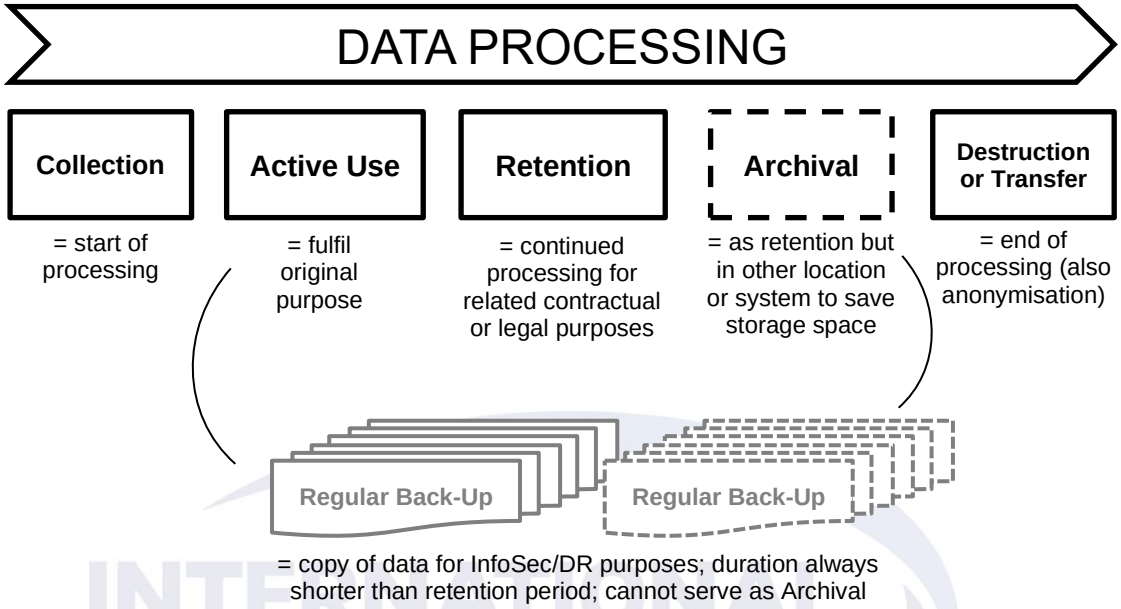
1.3.1. The collection, transformation, accessing, updating, transferring, destruction and any other manipulation of data is termed "**Data Processing**".

1.3.2. "**Retention**" is the continued processing of data, after the initial "Active Use" has achieved the purpose for which the data was originally collected.

1.3.3. Data Retention is usually required to meet applicable legal or contractual obligations or meet business objectives (see 1.5). **Retention Periods** are determined accordingly. For Personal Data they must be no longer than necessary to protect the rights and freedoms of individual data subjects in accordance with International SOS Data Protection Policy and applicable Data Protection regulation.

1.3.4. In some cases, retention may be in the form of "Archival", to preserve storage space or bandwidth on the system or container originally employed for Active Use processing.

1.3.5. Throughout the data processing, for Information Security and Disaster Recovery/Business Continuity purposes, regular back-ups or copies may be created of the data. Retention periods of such back-ups should be only as long as required to fulfil this purpose. Back-up tapes should not serve as a replacement for data retention.



1.4. Scope

1.4.1. This Policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to Data. It is the responsibility of all the above to familiarise themselves with this Policy and ensure adequate compliance with it.

1.4.2. This Policy covers all data processed or in International SOS's custody or control in whatever medium such data is contained in.

1.5. Obligations and General Principles of Data Retention

1.5.1. International SOS is bound by various obligations with regard to the data that we process or control. These obligations include how long we may retain Data and when and how we can destroy it. The obligations may arise from industry standards, local laws or regulations or from contracts and promises that we make to our employees, customers, goods and service providers and our partners.

1.5.2. 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 Data in order to protect International SOS's interests or those of our employees, customers, goods and service providers and our partners.

1.5.3. As a result, Data may need to be archived beyond its active use. A contract may, for example, expire after two years but other Data may, by law, need to be retained for a longer period.

1.5.4. Broadly, when the Document Retention Period for a particular type of data is over, we ought to destroy that data in a secure manner unless a documented exception is agreed by the International SOS Information Security Management Committee.

1.6. Obligations and Principles specific to Personal Data

1.6.1. To effectively protect data subjects' right to privacy and comply with regulatory requirements, it is important to apply certain principles when processing Personal Data. This will determine retention periods for data that falls into this category.

1.6.2. Personal Data should only be retained as long as is necessary for each specific purpose for which it was collected.

1.6.3. Personal Data should be kept up-to-date and accurate. Ensuring that records containing Personal Data are disposed of when no longer needed will reduce the risk that such data will become inaccurate, out of date or irrelevant and that it may be used in error.

1.6.4. Accurate and up-to-date records of Personal Data Processing Activities must be maintained.

1.7. Obligations and Principles specific to Account Data

1.7.1. PCI DSS applies whenever Account Data is stored, processed or transmitted. Account Data that are no longer needed must be discarded.

2. DATA INVENTORIES

2.1. Data Asset Inventory

2.1.1. Documents and Records should be organised into Data Assets such as SharePoint sites, databases or electronic information systems (examples would be a payroll and benefits system) to allow systematic, standardised management.

2.1.2. Data Management outside of such systems must be reduced to a minimum.

2.1.3. It is the responsibility of the respective Functional or Business Line Head to ensure that each International SOS Data Asset is registered on the Inventory by the nominated Asset Owner.

2.1.4. Each Data Asset is subject to a specific retention period for the data, reflecting the legitimate basis justifying the need for and use of the Data. Retention periods for different types of Data will depend on the nature of such Data.

2.1.5. Asset Owners are to ensure that their Data Asset Inventory entries are reviewed, and if necessary updated, at least annually and every time significant changes are made to a process involving a Data Asset assigned to them.

2.2. Personal Data Processing Inventory

2.2.1. It is the responsibility of the respective Functional or Business Line Head to ensure that all Personal Data Processing are recorded on the Data Processing Inventory.

2.2.2. For each Processing Activity, the following should be recorded:

(a) Purpose of Processing

(b) Data Subject Type

(c) Data Type

(d) Location / Data Asset

(e) Lawful basis of Processing

(f) Condition met for Sensitive Personal Data (if applicable)

(g) Start of Retention, Retention Periods and Archival (if applicable)

(h) Vendor processing the data (“Data Processor”) (if applicable)

2.2.3. Respective Functional or Business Line Head are to ensure that their Inventory entries are reviewed, and if necessary updated, at least annually and every time significant changes are made to a process.

3. DATA RETENTION AND ARCHIVING

3.1. Retention and Archiving Period

3.1.1. For the purposes of enforcing Retention in accordance with this Policy, each function is responsible for the Records and Documents it creates, uses, stores, processes and destroys. A sample list of Record and Document types across International SOS by function is attached in Appendix 2: Record Types. These lists of Record and Document types shall be maintained by each Function under guidance from the Compliance Department.

3.1.2. The standard Retention periods are:

	Category	Retention Period	
		In-System*	Total Retention (including Archival)
1	Medical Record	3 years	30 years or based on applicable regulations
2	Occupational Health Assessment Record	3 years	30 years or based on applicable regulations
3	Human Resources Record	Duration of employment	Based on applicable regulations
4	Medical and Security Assistance Case Record	2 years	3 years
5	Concierge Services Case Record	As below or as per relevant contractual commitments	
	(a) CVV2	72 hours	72 hours
	(b) Inactive card data	90 days	90 days
	(c) Inactive case record (No PAN or CVV2)	2 years	3 years
6	Call Recordings	As below	
	(a) **Standard** call recordings for All Assistance Centres except the below	1 year	NA
	(b) HCM Assistance Centre**	7 years	NA
	(c) JNB Assistance Centre**	3 years	NA
	(d) KUL Assistance Centre**	5 years	NA
	(e) MDC MedAire Phoenix**	3 years	NA
	(f) SYD Assistance Centre**	No destruction	NA
	(g) TPE Assistance Centre**	2 years	NA
7	Audit Logs	3 months	1 year
8	Corporate Secretariat Record	Life of the entity	Life of the entity plus 50 years
9	Accounting and Financial Record	2 years	7 years or based on applicable regulations

	Category	Retention Period	
		In-System*	Total Retention (including Archival)
10	Procurement and Contract Record	Contract duration	Contract duration plus 7 years or based on applicable regulations
11	Tracker Record	2 years or based on contractual commitments	3 years or based on contractual commitments
12	Other Records	2 years or based on applicable regulations	2 years or based on applicable regulations
*In-System = retention in same application / location that served for original Active Use (i.e. not Archive)			

**** HCM Assistance Centre** – National regulatory requirement / technical capabilities
**** JNB Assistance Centre** – Consistent with MDC / litigation requirements
**** KUL Assistance Centre** – Other obligations
**** MDC MedAire Phoenix** – Litigation requirements
**** SYD Assistance Centre** – Other obligations
**** TPE Assistance Centre** – Other obligations

3.2. Safeguarding of Data during Archiving

3.2.1. All archived data must be encrypted or locked and continuously safeguarded to avoid data breaches.

3.2.2. 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.

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

3.2.4. If archival is outsourced, the vendor must first be assessed to ensure they comply with our Data Protection and Information Security Standards and appropriate contracts with Data Protection and Information Security clauses must be implemented.

3.2.5. The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to regional or country IT Manager or equivalent in charge of the storage function.

3.3. Retention and Archiving Exception

3.3.1. An archiving period more or less than the period stated in the summary table may be granted by exception. The Head of Function will request an exception in accordance with section 5 to archive such Records. Such exception request shall specify the administrative, organizational and technical measures to be undertaken to ensure the confidentiality, integrity and availability of such Records.

3.3.2. An archiving period lesser than the period stated in the summary table should relate to records with a limited business purpose such as emails, OCS messages, travel itineraries, pre-trip advisories, or to comply with client or industry requirements.

4. DATA DESTRUCTION

4.1. Regular Review

4.1.1. All Data, whether held electronically, on individual employees' devices or on paper, should be reviewed on a regular basis to decide whether to destroy or delete any Data in accordance with the designated retention period.

4.1.2. Responsibility for the destruction of data included in the Data Asset Inventory falls to each Functional or Business Line Heads.

4.1.3. Responsibility for the destruction of data included in local departmental document and record inventories falls to each Departmental Head.

4.2. Safe Destruction and Disposal

4.2.1. Personal Data or confidential or restricted information must be disposed of as confidential waste and be subject to secure electronic deletion or Anonymisation.

4.2.2. Some expired or superseded contracts may only warrant in-house shredding.

4.2.3. 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.

4.2.4. International 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.

4.2.5. International SOS Corporate IT and Regional IT shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

4.2.6. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that International SOS Corporate IT or Regional IT subcontracts for this purpose. All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements, and all data disposal is subject to applicable provisions under relevant data protection laws and the International SOS Data Protection Policy and Information Security Policy.

4.3. Accidental Loss

4.3.1. Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the International SOS Data Protection Policy and Information Security Policy.

5. EXCEPTIONS

5.1. Exception Requests

5.1.1. The reasons may be a client requirement, business requirement, legal requirement or vital historical purpose:

(a) The Head of Function shall review and submit to the International SOS Information Security Management Committee an exception request to archive data for a different period as detailed in Section 3.1.2.

(b) The Exception Request Form shall be reviewed and approved by the International SOS Information Security Management Committee and routed to the Head of Location and Corporate or Regional IT to enforce.

5.2. Litigation Holds

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

5.2.2. A Litigation Hold Order shall appoint a custodian of records and specify a location for storage and review of documentation.

6. RESPONSIBILITIES

6.1. Functional or Business Line Heads

6.1.1. Each Head of Function is responsible for the data it creates, uses, stores, processes and destroys.

6.1.2. Each Head of Function is responsible to nominate an Owner for each Data Asset and Personal Data Processing Activity.

6.1.3. Respective Functional or Business Line Heads must ensure that each Data Asset and Personal Data Processing Activity is registered on the Data Asset and Personal Data Processing inventories by the nominated Owner.

6.1.4. Functional or Business Line Heads are responsible to maintain their respective inventories.

6.1.5. Each Functional or Business Line Head shall be responsible for implementing procedures for the retention, archiving and destruction of data, communicating these periods to the relevant employees and enforcing compliance.

6.1.6. 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.

6.2. Local Functional Heads

6.2.1. Each local functional or business line team is responsible for the Data it creates, uses, stores, processes and destroys.

6.2.2. Functional or Business Line Heads in each location are to ensure that Data Asset and Data Processing inventories are compiled, regularly reviewed, and if necessary updated, at least annually.

6.2.3. These staff are also responsible for the destruction of Data in accordance with the retention periods defined in departmental Data Processing inventories.

6.3. Compliance Department

6.3.1. The Compliance Department may audit compliance with this Policy from time to time and provide recommendations to be reviewed by the Group General Counsel, in the capacity of Chairman of the International SOS Information Security Management Committee and by the relevant senior management.

6.3.2. The Compliance Department shall provide guidance with regard to this Policy.

6.3.3. The Compliance Department shall administrate and oversee the use of Data Asset and Personal Data Processing Inventory systems.

6.4. All Employees

6.4.1. Each employee shall be responsible for returning Records and Documents in their possession or control to International SOS upon separation or retirement.

6.4.2. Final disposition of such Records and Documents shall be determined by the immediate supervisor in accordance with this policy and the respective country employee exit process.

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.

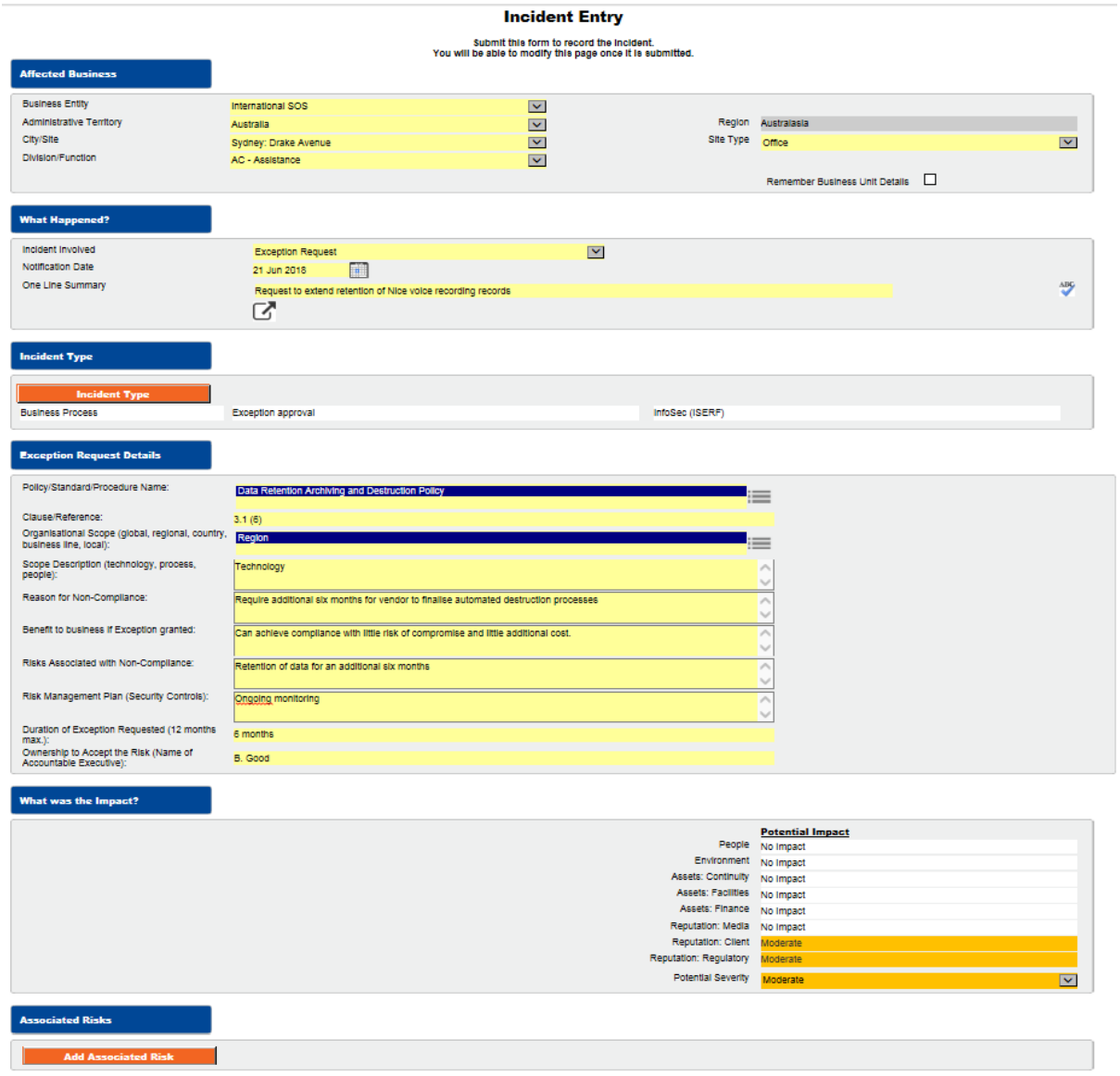
7.2. All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor or the Group General Counsel. Reports made in good faith by someone who has not breached this Policy will not reflect badly on that person or their career at International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

8. APPENDIX 1: EXCEPTION REQUEST / LITIGATION HOLD FORM

Information Security Exception Request Form (ISERF)

Instructions

1. The Information Security Exception Request Form below is required whenever a business unit or organization within International SOS would like to deviate from the International SOS Data Retention, Archiving and Destruction Policy ("Policy") and the Information Security Standards.
2. This form is embedded in the Hydra Incident system and appears when Incident Involved = Exception Request.
3. The form is used when Asset Owners need to request an exception to the defined retention schedules as outlined in Section 3.1.2 of the Policy.
4. The type of exception request you can submit is:
   (a) To obtain approval to reduce the period of retention.
   (b) To obtain approval to increase the period of retention.
5. Submit this form to the Head of Function for review before submission to the International SOS Information Security Management Committee for final approval (or rejection).



Incident Entry

Submit this form to record the incident.
You will be able to modify this page once it is submitted.

Affected Business

Business Entity	International SOS		
Administrative Territory	Australia	Region	Australasia
City/Site	Sydney: Drake Avenue	Site Type	Office
Division/Function	AC - Assistance		
		Remember Business Unit Details	☐

What Happened?

Incident Involved	Exception Request
Notification Date	21 Jun 2018
One Line Summary	Request to extend retention of Nice voice recording records

Incident Type

Incident Type

Business Process	Exception approval	InfoSec (ISERF)

Exception Request Details

Policy/Standard/Procedure Name:	Data Retention Archiving and Destruction Policy
Clause/Reference:	3.1 (6)
Organisational Scope (global, regional, country, business line, local):	Region
Scope Description (technology, process, people):	Technology
Reason for Non-Compliance:	Require additional six months for vendor to finalise automated destruction processes
Benefit to business if Exception granted:	Can achieve compliance with little risk of compromise and little additional cost.
Risks Associated with Non-Compliance:	Retention of data for an additional six months
Risk Management Plan (Security Controls):	Ongoing monitoring
Duration of Exception Requested (12 months max.):	6 months
Ownership to Accept the Risk (Name of Accountable Executive):	B. Good

What was the Impact?

	Potential Impact
People	No Impact
Environment	No Impact
Assets: Continuity	No Impact
Assets: Facilities	No Impact
Assets: Finance	No Impact
Reputation: Media	No Impact
Reputation: Client	Moderate
Reputation: Regulatory	Moderate
Potential Severity	Moderate

Associated Risks

Add Associated Risk

9. APPENDIX 2: RECORD TYPES

9.1. Medical Record

9.1.1. Original Records, regardless of format, which a physician or licensed health care or medical professional has prepared (across time within a particular health care provider's jurisdiction) with respect to, and which include medical information about, such physician's or professional's patient, pursuant to a physician-patient relationship.

9.1.2. Medical Records within the International SOS environment are those which have been created by physicians or licensed medical professionals employed by or operating at the control and direction of International SOS in a clinical environment.

9.1.3. Medical Records prepared by 3rd party medical service providers, who have their own obligation to maintain medical records relative to their patients, are not considered to be Medical Records for the purpose of this Policy.

9.1.4. For the avoidance of doubt, Case Records created in the normal course of rendering assistance by International SOS Assistance Centres (including copies of any third-party prepared Medical Records provided to International SOS in the normal course of rendering assistance) are classified as Case Records, not Medical Records.

9.2. Occupational Health Assessment Record

9.2.1. Original Records, regardless of format, that hold a medical health assessment or review and recommendations relative to an individual travelling on behalf of, or being employed by, a customer.

9.2.2. Occupational Health Assessment Records are prepared by a physician or licensed medical professional employed by or operating at the control and direction of International SOS, and submitted to the customers authorized person. For the avoidance of doubt, "Health Passports" and other summarizations of Medical Records or Occupational Health Assessment Records, and travel or work related recommendations created in the normal course of rendering medical fitness reports are generally not considered to be Medical Records (since the original Medical Records upon which the assessment is based or records of a 3rd party, but are to be retained as Occupational Health Assessment Records.

9.2.3. In many instances, Occupational Health Assessment Records and underlying copies of Medical Records related thereto should be transferred to the customer, who is the 'owner' of such records, in which event copies retained by International SOS, if any, will be classified as Case Records.

9.3. Human Resources Record

9.3.1. Information about an employee's eligibility for employment, promotion, compensation, transfer, termination, disciplinary or other adverse action (such as, evaluations or reports related to the employee's character, credit, and work habits).

9.3.2. The contents of this record may be maintained in paper or electronic format and the following are examples:

(a) Pre-employment records (employment application, resume, offer/acceptance letter);
(b) Hiring records (confidentiality agreement, conflict of interest questionnaire, arbitration agreement, sign-on bonus agreement);
(c) Attendance records (attendance management reports, leave notifications);
(d) Compensation statements (salary increases, bonuses, long-term incentives);
(e) Disciplinary process documents (performance, behaviour, warnings);
(f) Flexible work agreements and related information;
(g) Performance appraisals;
(h) Development plans;
(i) Training, development, and education courses (certificates of completion);
(j) Notes of commendation or discipline;
(k) Termination documents (resignation letter);
(l) Exit interviews.

9.4. Medical and Security Assistance Case Record

9.4.1. Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed as part of the case management.

9.5. Concierge Services Case Record

9.5.1. Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed as part of the case management.

9.5.2. Credit card information is permitted to be stored only if there is an approved and documented business need.

9.5.3. All data must be protected as described in all sections of the PCI DSS.

9.5.4. The following card holder data is permitted to be stored with conditions:

(a) Primary Account Number (PAN)
(b) Cardholder name (must be protected if stored in conjunction with the PAN)
(c) Service Code (must be protected if stored in conjunction with the PAN)
(d) Expiration Date (must be protected if stored in conjunction with the PAN)

9.5.5. The following card holder data is not permitted to be stored after completion of authorization:

(a) Full Magnetic Stripe (Track 1 or 2 data)
(b) CVV2, CVC2, CID, CAV2
(c) PIN / PIN Block

9.5.6. System and audit logs showing access to stored data must be retained for at least 1-year. Logs must be kept online and available for 90 days.

9.6. Call Recordings

9.6.1. All call recordings that are made for any calls that are received by or made by the Assistance centres or Concierge centres.

9.7. Audit Logs

9.7.1. Audit logs are records that document an event in an information (IT) technology system. In addition to documenting what resources were accessed, audit log entries usually include destination and source addresses, a timestamp and user login information.

9.8. Corporate Secretariat Record

9.8.1. Records which relate to the establishment, operation, control, ownership and management of legal entities which are within the Group.

9.8.2. All documents, regardless of format, which include but not limited to the following:

(a) Statutory Registers
(b) Minutes and resolutions of Board of Directors and Shareholder
(c) Company Seal
(d) Corporate Filing
(e) Documentation related to restructuring, acquisitions and disposals

9.9. Accounting and Financial Record

9.9.1. Accounting records are key sources of information and evidence used to prepare, verify and/or audit the financial statements. They also include documentation to prove asset ownership for creation of liabilities and proof of monetary and non monetary transactions.

9.10. Procurement and Contract Record

9.10.1. Procurement and contract records are the evidence of all actions taken to award contracts, and of the results of the monitoring and oversight of contract implementation.

9.10.2. Procurement and contract records are the basis for internal and external audits, and are needed to determine compliance with the procurement legal and institutional framework.

9.11. Tracker Record

9.11.1. Tracker Records include information of a person's travel, emergency contact details as well as location data.

9.11.2. Location data is any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to:

(a) the latitude, longitude or altitude of the terminal equipment;
(b) the direction of travel of the user; or
(c) the time the location information was recorded.

9.12. Other Records

9.12.1. All Records that do not fall into any of the Records defined in this section.