Sunass — El regulador del agua potable	**SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)**

Update: 11/04/2022

1. **SCOPE OF THE MANAGEMENT SYSTEM**

The Sunass has defined the scope of the Information Security Management System - ISMS for the process:

Process	Process owner
Management of appeals resolution	Administrative Tribunal President of Users' Claim Solution of Sanitation Services

The aim of the process is to resolve in a second and final administrative authority, the claims among service suppliers and users. Besides, to solve complaints filed due to faults in the claims process among service suppliers, respecting legal framework and assisting the society.

2. **PHYSICAL LOCATION**

The scope of the application of the ISMS covers the process and activities developed

Office	Address
Main Office	Calle Bernardo Monteagudo 210-216 Magdalena del Mar

3. **APLICABILITY**

The ISMS control applications are detailed in the document: "Statement of Applicability"

4. **INFORMATION SYSTEMS**

The main information systems impacted or that provide support o ISMS are the following:

- Document Control System (SISTRAM, for its Spanish acronym)
- Institutional E-mail
- Office 365 (Microsoft Office, TEAMS, among others).
- Document Repository

5. **INTERFACES AND DEPENDENCIES**

5.1 INTERNAL INTERFACES AND DEPENDENCIES

The internal interfaces that interact with the scope defined in the ISMS are:

Department	Interfaces
Information Technology Office	- *Integrated Management System Policy.* - *Directive "Specific Guidelines for Information Security".* - *Internal documents (directives, procedures, instructions, among others) that document technical support, development and system maintenance processes, as well as those necessary for the operation of the ISMS* - *lectronic Document Management System (SIGED), email and information system.*
Legal Advisory Office	- *Integrated Management System Policy.* - *Directive "Specific Guidelines for Information Security".*

Department	Interfaces
	- *Internal documents (directives, procedures, instructions, among others) that document the processes of the organizational unit, as well as those necessary for the operation of the ISMS.* - *Legal alerts* - *SIGED, email and information system.*
Human Resources Unit	- *Integrated Management System Policy.* - *Directive "Specific Guidelines for Information Security".* - *Internal documents (directives, procedures, instructions, among others) that document document management processes, as well as those necessary for the operation of the ISMS.* - *SIGED, email and information system.*
Supply Unit	- *Integrated Management System Policy.* - *Directive "Specific Guidelines for Information Security".* - *Internal documents (directives, procedures, instructions, among others) that document the procurement processes of goods and services, as well as those necessary for the operation of the ISMS.* - *SIGED, email, and information systems.*
Document Management Unit	- *Integrated Management System Policy.* - *Directive "Specific Guidelines for Information Security".* - *Internal documents (directives, procedures, instructions, among others) that document the document management processes, as well as those necessary for the operation of the ISMS.* - *SIGED, email, and information system.*

5.2 EXTERNAL INTERFACES AND DEPENDENCIES

The external interfaces that interact with the scope defined in the ISMS are:

Entity	Interfaces
Governing government entities	*Legal regulations, SIGED, Service Desk, email, PIDE services, Institutional Portal (GOB.PE)*
Providers	*Directive "Specific Guidelines for Information Security", process documentation, contracts, service orders, email, Service Desk, information systems, service deliverables, Institutional Portal (GOB.PE)*
Drinking water and sanitation service providers	*General Regulation for Users' Claims of Sanitation Services and related regulations, Service Desk, information systems, Institutional Portal (GOB.PE)*
Users of drinking water and sanitation services	*Service Desk, Institutional Portal (GOB.PE)*

6. EXCLUSIONS

- *Systems, applications, and information resources whose mandatory use is regulated by governing entities of the public sector.*
- *The home network of the server in teleworking mode.*

CHANGE RECORD		
N°	**Ítems**	**Description of the change**
1	4. INFORMATION SYSTEMS	The systems "Imaging Soft" and "SIGA" were removed because they are not critical-level assets for the ISMS.
2	5. INTERFACES AND DEPENDENCIES	- This section was modified to specify internal and external interfaces and dependencies. - The "Legal Advisory Office" was added as an internal interface. - The external interface "Oversight Entities" was replaced with "Governing government entities".
3	6. EXCLUSIONS	Added in section 6.

The indicated changes are with respect to the latest update.

Updated by:	Reviewed by:	Approved by:
Jenny Castañeda Zubiaur Digital Security Officer	Kelly Elizabeth Paz Orellana Coordinator / ISM Manager	Manuel Fernando Muñoz Quiroz Senior Management of IMS