AVRAMAR

Information Management Policy

Version	1
Issue Date	November 2020
Effective Date	November 2020
Next Review	November 2023
Classification	Public
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically reviewing and updating this Policy so as to reflect regulatory, best practice and business developments.
Approver	

Policy Summary

Effective Information management requires understanding and management of Information throughout its life-cycle. This Policy provides the framework to manage Group Information by defining the minimum requirements for each stage of the Information life-cycle to enable the Group to understand, manage, and protect its Information at all stages. This Policy is to be used in conjunction with the Group Code of Conduct and any other relevant Group or local policies.

Policy Implementation

Role	Responsibility
Asset CEO (or equivalent)	▪ Designate an Information Management Owner (IMO)
Information Management Owner (IMO)	▪ Work with stakeholders to develop and deploy appropriate procedures to satisfy the requirements of this Policy ▪ Provide training on this Policy and procedures ▪ Monitor implementation, compliance, and effectiveness of Information management ▪ Support the IMO throughout the implementation Comply with this Policy and internal procedures

Information Life-Cycle Responsibilities

Stage	Information Management Owner	Information Owner	Information User
Identification	▪ Compile and maintain the Information Register ▪ Work with stakeholders to identify Vital Information listed in the Information Register	▪ Create a list of owned information and provide it to the IMO ▪ Keep the list of owned Information up-to-date	▪ Support the IMO & the information Owner
Creation, Receipt, Categorizatio n& Marking	▪ Work with stakeholders to define Information creation, categorization, and marking principles ▪ Work with stakeholders to develop and maintain an Information Category Matrix ▪ Develop Information marking requirements	▪ Provide the IMO and Information Users with unique Information creation, categorization, marking, and receipt requirements ▪ Identify the appropriate Information Category for Information ▪ Categorize and mark Information as required	▪ Follow Information creation, receipt, categorization, and marking principles ▪ Know the Information Category ▪ When creating Information, categorize and mark it as required ▪ Seek advice from the Information Owner when receiving

			unmarked Information
Storage & Security	Specify storage and security requirements for each Information Category	Provide IMO with unique storage and security requirements	Store and protect Information in accordance with the requirements of its Information Category and any unique requirements
Access & Sharing	Specify acceptable access and sharing methods for each Information Category	Specify who may have access to share and receive Information and communicate this to Information Users	Access and share Information in accordance with the requirements of its Information Category and unique requirements
Retention	Work with stakeholders to define the Retention Period for Information on the Information Register	Maintain Information in accordance with its Retention Period or Legal Hold Notice requirements	▪ Retain Information for its appropriate Retention Period or in accordance with a Legal Hold Notice ▪ Return original Information to the Information Owner when no longer needed ▪ Properly hand over Information upon departure from a role
Disposal	Specify disposal methods and requirements for each Information Category	▪ Inform IMO of unique disposal requirements ▪ Dispose of Information in accordance with the requirements of its Information Category and unique requirements	▪ Dispose of duplicate copies of Information in accordance with the requirements of its Information Category and any unique requirements ▪ Support disposal of Information at the end of its Retention Period or lifting of Legal Hold Notice

Applicability & Consequences

This Policy applies to the Group and to Group Personnel. Group Personnel agree to uphold the Group's commitment to do what is right and to follow this Policy and the Group Code of Conduct. Group Personnel who fail to uphold this commitment put themselves, their colleagues, and the Group at risk of fines, penalties, reputational damage and personally may be subject to disciplinary action, up to and including, loss of employment. The Group reserves the right, at its sole discretion, to disclose information about violations of law to relevant authorities. Any Group Personnel who have violated applicable laws may be personally liable for penalties or fines or may be subject to imprisonment.

A Group Asset may establish standards that are stricter than this Policy. Any exceptions to or deviations from this Policy must be submitted to the Ethics & Compliance Office.

Your Responsibilities:

- Follow applicable laws and regulations
- Understand and comply with the requirements of this Policy, the Group Code of Conduct, other Group Policies, and any Division/Sector or Asset policies or procedures in relation to this Policy
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Complete assigned training related to this Policy
- Uphold our commitment to always do what is right
- Leadership will provide appropriate resources and support to ensure the successful implementation of this Policy

Questions & Reporting Violations:

Refer in good faith any questions, concerns, or any known or suspected violations of this Policy to your line manager or other internal management or to the Ethics & Compliance Office.

Retaliation for good-faith reporting is not tolerated. Group Personnel who engage in retaliatory conduct are subject to disciplinary action.

Policy Requirements

1. Policy Implementation

To satisfy the Information management requirements throughout the life-cycle of Information, and each Asset must designate an Information Management Owner to:

- Ensure that the requirements of this Policy are established and implemented
- Develop and deploy appropriate procedures and processes to ensure that the requirements of this Policy are met
- Provide training on this Policy and all related internal policies and procedures to Group Personnel
- Monitor implementation, compliance, and effectiveness of Information management in the Asset
- Information Owners and Information Users are required to support the Information Management Owner

2. Information Lifecycle

Information management within the Group requires different stakeholders to comply with requirements based on their roles. Those requirements follow the Information lifecycle below:

- Identification of Information residing in /Asset: The first step is to understand what Information resides in /Asset, which is done by creating an Information Register. This Information Register must be kept up-to-date and is a key reference document in the Information management program
- Creation/Receipt of Information: This is the beginning of the Information lifecycle and occurs when Information is either created internally or received from outside / Asset. Creation or receipt brings Information under the Group's custody and/or control
- Categorization and Marking of Information: To define and communicate the handling requirements applicable to Information based on its level of sensitivity, Information must be assigned an appropriate Information Category, and Information must be appropriately marked with its Category
- Storage and Security: Each Information Category identifies specific storage, security practices, and requirements that apply to the Information
- Sharing: To protect Information from unauthorized disclosure, each Category defines specific access and sharing rules. Access to Information should only be granted according to its Category and instructions defined by the Information Owner
- Retention: Regulatory, legal, contractual, and operational requirements define for how long Information must be kept. A Retention Period is defined and is listed in the Information Register for each Information type. The Retention Period may also be published in a Retention Schedule
- Legal Hold: In cases where /Asset is subject to a potential or ongoing claim, investigation, or audit, Information may need to be retained regardless of its Retention Period. Information subject to a Legal Hold will be identified by /Asset's Legal Counsel in a Legal Hold Notice. Only Legal Counsel may issue AND remove a Legal Hold Notice

- Information handover: When Group Personnel leave a role for any reason (e.g., changing roles, changing departments, leaving the company), Information must be handed over appropriately
- Disposal: When the Information's lifecycle reaches an end, and only after satisfying specific conditions, it must be destroyed in the manner that is specified by its Information Category

3. Information Management Owner (IMO) requirements

The IMO plays a key role in the implementation of this Policy and the ongoing management of /Asset's Information management program throughout the Information lifecycle.

a. Identification of Information residing in /Asset

The IMO must work with Information Owners to compile and maintain an Information Register. The Information Register must include details related to Information, such as type, owner, storage medium, Category, Retention Period, and whether it is Vital Information.

The Information Register must be detailed enough for Information Users and Information Owners to carry out day-to-day Information management practices.
The IMO must work with Information Owners to identify Vital Information on the Information Register and ensure that appropriate stakeholders are aware of the list of Vital Information.

b. Creation/Receipt of Information

The IMO must work with internal stakeholders (such as Communications) to define and communicate Information creation guidelines within /Asset. The IMO must also specify guidelines on proper receipt of Information, which requires the Information User to obtain, where possible, the Category and the Retention Period of the Information being received.

c. Categorization and Marking of Information

The IMO must develop an Information Category Matrix, working closely with relevant stakeholders – especially appropriate Legal Counsel – to ensure that relevant regulatory, legal, contractual, national security, and business needs are taken into consideration. The Information Category Matrix not only must be practical but also reflect the sensitivity of Information and the degree of damage that would result from unauthorized disclosure. The IMO must also develop appropriate marking requirements for Information, regardless of its medium.

d. Storage and Security

The IMO must specify storage and security methods and requirements for each Information Category on /Asset's Information Category Matrix. The requirements must take into consideration applicable regulatory, legal, contractual, national security, and business requirements.

The IMO must ensure that unique storage and security requirements for Information are listed in the Information Register. The IMO must also coordinate with relevant stakeholders to provide adequate means to store and protect Information.

e. Access and Sharing

The IMO must specify access and sharing methods and requirements for each Information Category. The requirements must take into consideration applicable regulatory, legal, contractual, national security, and business requirements.

The IMO must ensure that unique access and sharing requirements for a specific type of Information are listed on the Information Register. The IMO must also coordinate with the relevant stakeholders to provide resources to satisfy access and sharing requirements.

f. Retention

The IMO must work with /Asset's Legal Counsel, Information Owners, and other relevant stakeholders to define Retention Periods. The IMO should review Retention Periods annually to align with changes in legal, regulatory, contractual, and business requirements.

g. Handover

Human Capital in /Asset will require an appropriate handover of Information when Group Personnel leave a role, which will include certification by the direct supervisor that an appropriate handover occurred. Human Capital also will request written authorization from Group Personnel to access secured business-related data that may be needed after the person's departure.

h. Disposal

The IMO must specify disposal methods and requirements for each Information Category on /Asset's Information Category Matrix. Disposal requirements must take into consideration applicable regulatory, legal, contractual, national security, and business requirements.

The IMO must ensure that unique disposal requirements for a specific type of Information are listed next to that Information on the Information Register. The IMO must coordinate with the relevant stakeholders to provide resources to satisfy disposal requirements.

4. Information Owner requirements

Information Owners are responsible for how Information is managed as follows:

a. Identification of Information residing in /Asset

The IMO must work with Information Owners to compile and maintain an Information Register. The Information Register must include details related to Information, such as type, owner, storage medium, Category, Retention Period, and whether it is Vital Information.

The Information Register must be detailed enough for Information Users and Information Owners to carry out day-to-day Information management practices.
The IMO must work with Information Owners to identify Vital Information on the Information Register and ensure that appropriate stakeholders are aware of the list of Vital Information.

5. Information User requirements

Information Users handle Information in /Assets on a daily basis and must understand and comply with the following requirements:

a. Creation/Receipt of Information

The Information User must understand and follow Information creation guidelines. The Information User must obtain the Information Category for Information received.

b. H Categorization and Marking of Information

The Information User must know the Information Category. The Information User must mark Information as per the Information Category assigned by the Information Owner and listed on the Information Register. The Information User must seek guidance from the Information Owner when in doubt.

c. Storage and Security

The Information User must store and protect Information according to the requirements of its Category and any unique requirements assigned for specific Information.

d. Access and Sharing

The Information User must access or share Information according to the requirements of its Information Category and only share with those authorized to receive it. The Information User must seek guidance from the Information Owner when in doubt.

e. Retention

The Information User must ensure that original Information is returned to the Information Owner, when no longer needed. The Information User must not keep unnecessary copies of Information.

The Information User must preserve Information subject to a Legal Hold in the manner specified in the Legal Hold Notice. The Information User leaving his/her role is responsible for ensuring that Information is handed over appropriately.

f. Disposal

The Information User is responsible for disposing of Information according to the requirements of its Information Category and any unique requirements assigned for specific Information.

Definitions

Throughout this Policy, defined terms are capitalized and have the following meanings:

Term	Definition
Asset	Any company or business within the Group
Division/Sector	A business or corporate function
Ethics & Compliance Office	The Ethics & Compliance Office or relevant Asset ethics & compliance function
Group Policy(ies)	Any policy that applies to the Group. Group Policies do not include policies that only apply to a limited set of Group Personnel, for example, a policy that only applies to a specific Division/Sector or Asset within the Group
Information	Data, documents, or records in any format (e.g., electronic, physical), created by or in the possession or control of the Group or Group Personnel, including third party Information created or stored on behalf of the Group
Information Category(ies)	A classification of Information that indicates its level of confidentiality or sensitivity
Information Category Matrix	A table that specifies Information Categories. and each Asset will have its own Matrix
Information Management Owner (IMO)	Individual(s) responsible for establishing and managing the Information management program in or the Asset
Information Owner	The head of the respective function that created the Information or first received Information from a third party; this role may be delegated to an appropriate individual(s)
Information Register	A table that lists Information and associated characteristics such as the Information Owner, its storage medium, and its Information Category
Information Users	Group Personnel who create, access, use, or handle Information to perform their assigned duties. For example, Information Users may be employees, contingent workers, contractors or third parties such as business partners, consultants, customers or suppliers specifically authorized to access Group Information or systems
Leadership	The Chief Executive Officer of the Group, a Functional Head or, in each case, a nominated representative
Legal Hold Notice	An instruction issued by Legal Counsel to relevant Information Owners and Information Users requiring the retention of specified Information that may be required to respond to existing or foreseeable litigation, investigation, or audit. Only Legal Counsel may remove a Legal Hold
Group	Avramar ; any entity, operation, or investment controlled by ; and/or any entity, operation, or investment that adopts the Group Code of Conduct
Group Personnel	All individuals who work directly for or represent the Group, including directors, employees, consultants, and long-term contractors of the Group
Retention Period	The period of time during which Information must be kept to comply with applicable laws, regulations, contracts, and business requirements.
Retention Schedule(s)	A list of Retention Periods for Information

Vital Information	Asset Information that is critical for business continuity and requires specific handling measures, which include storage in locations that provide the ability to restore Vital Information if a crisis occurs

Ethics & Compliance Contact Information

Telephone Number (Spain): +34 607 907 477

Facsimile: + 34 964 586 321

E-mail: ethics@avramar.eu