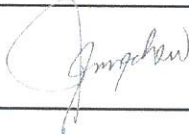
	Manual Title:		
	LEGAL AND COMPLIANCE MANUAL		
	Policy Number:	Effectivity Date:	Page Number:
	SPAVI-LCM-01.2024 Rev 00	January 30, 2024	Page 1 of 15
	Policy Title:	Supersedes Policy Number:	
	DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL	N/A	

Document History:

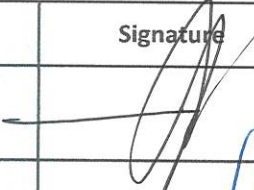



- Revision Number 00 always means Official Release
- For Revision Number 01 onwards, Description of Change must indicate which Section Numbers have been revised.


Revision Number	Description of Change	Author	Signature	Issued Date
00	Official Release			

Reviewed by:

Department	Name	Designation	Signature	Date
Legal	Atty. James Earl R. Chew	DPO / Legal Counsel		

Approved by:

Designation	Name	Signature	Date
President and Chief Executive Officer	Vicente L. Gregorio		
Vice President and Chief Financial Officer	Manuel T. Del Barrio		
Chief Operating Officer	Jorge Ma. Q. Concepcion		5/20
Chief Human Resource Officer	Ma. Elma C. Santos		5/20

	Manual Title:		
	LEGAL AND COMPLIANCE MANUAL		
	Policy Number:	Effectivity Date:	Page Number:
	SPAVI-LCM-01.2024 Rev 00	January 30, 2024	Page 2 of 15
	Policy Title:	Supersedes Policy Number:	
	DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL	N/A	

1.0 OBJECTIVES


- 1.1. To specify and implement a document management policy with data classification, management and retention and disposal standards that will help the SPAVI Group (Group, for brevity) secure its documents and information from risks such as unauthorized disclosure, sharing and access.
- 1.2. To provide guidelines for handling records, documents, and data throughout the Group, and how the Group retains and disposes of records necessary for ongoing business operations, legal, audit and regulatory compliance, whilst promoting orderly and efficient records management
- 1.3. To establish guidelines for the consistent and orderly maintenance and retention of adequate, unaltered, and accurate company records for the appropriate periods of time in compliance with the relevant statutory, contractual, legal, regulatory, financial, operational and research requirements

2.0 SCOPE/COVERAGE

- 2.1 This policy applies to all SPAVI employees, employees of subsidiaries and joint ventures in which Shakey's Pizza Asia Ventures, Inc. (SPAVI) has a controlling interest, as well as contractors and third parties with access to SPAVI information, records, or systems or who maintain information on behalf of the Group and the individuals responsible for complying with this policy. All levels of management are responsible for ensuring that all staff under their supervision comply with this Policy.
- 2.2 This Policy covers all company records whether housed or stored on company premises. Data classification categories shall be applied to all information in both digital and hard copy format and shall be mandatory for all SPAVI business units and subsidiaries. SPAVI is required to ensure that complete and accurate records are identified, retained, stored, protected and subsequently destroyed or archived within their area of assigned responsibility and in accordance with this Policy.

3.0 DEFINITIONS

- 3.1 Data Protection Laws – refers to the Data Privacy Act of 2012, its Implementing Rules and Regulations, issuances and of the National Privacy Commission and other applicable data protection laws and regulations.
- 3.2 Document - A written agreement, proposal, or other formal instrument regarding a course of action, the expenditure of company funds, or other contractual obligation - which is intended to be binding upon SPAVI, its subsidiaries or affiliates. Documents obligate SPAVI or its subsidiaries and affiliates, to act, engage, consent, perform, or pay. Typically, at least one party to the transaction is external to SPAVI. Documents may be in the form of contracts, proposals, agreements, statements, notices, resolutions, letters, memorandums, licenses, indentures, etc., but such documents may go by other names as well. Documents may refer to physical or hard copy documents or Electronic Documents.
- 3.3 Document Owner or User – means the individual who has the responsibility for issuing and maintaining a Document.
- 3.4 Employee – means any employee of the Group, employees of subsidiaries and joint ventures in which the Group has a controlling interest, as well as contractors and third parties with access to SPAVI information.
- 3.5 Hold Instruction – an instruction from Group Legal to preserve documents in relation to a Proceeding.
- 3.6 Legal – refers to the Legal and Compliance Department
- 3.7 Personal Data – as defined in the Data Protection Manual.
- 3.8 Proceeding – any legal, official, governmental, or other proceeding or investigation.
- 3.9 Records – all documents and other data (including Personal Data) that are created, received, used, or distributed by the Group in the course of its business, regardless of medium and includes without limitation hard copy, soft copy, Word, Excel or PowerPoint files, emails (inbox, outbox, drafts, folders and trash files), servers, cloud storage, instant messages, intranet and other media.

	Manual Title: LEGAL AND COMPLIANCE MANUAL		
	Policy Number: SPAVI-LCM-01.2024 Rev 00	Effectivity Date: January 30, 2024	Page Number: Page 3 of 15
	Policy Title: DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		Supersedes Policy Number: N/A

*Note: For purposes of this policy, Documents and Records as defined above shall be collectively referred to as "Documents".

4.0 POLICIES

4.1 General Policies

- 4.1.1 Documents that are created or received and maintained by SPAVI employees, third parties and those working for SPAVI as contractors, in the course of their duties and business activities for the company, are deemed company records and information assets belonging to SPAVI.
- 4.1.2 All Documents shall be maintained and handled in accordance with this policy unless there is reason to believe that:
 - a. A proceeding is pending or reasonably anticipated, in which case Legal shall be consulted for further guidance before destroying, altering, moving, or rearranging any Document; or
 - b. Legal has ordered or issued a Hold Instruction.

4.2 Document Classification

- 4.2.1 Documents shall be classified as Critical or Ultra-Critical according to their contents, intended use and impact on SPAVI. Document Classifications shall dictate the treatment and protection levels for each record or document.
- 4.2.2 Document Classifications shall be applied to different Information Categories used as a standard to classify company information.

Classification	Information Category	Description	Examples
Non-critical	Unclassified Public	Information is not confidential and can be made public without any negative impact on the Group. These are data or information whose disclosure does not expose the Group to financial loss, damage reputation, or violate privacy rights of the Group's data subject/s. These are data or information that are intended to be publicly available or provided to the public. The Group's only responsibility in processing such data is to ensure that the source of such data is reputable. Integrity is important but not vital.	<ul style="list-style-type: none"> Literature on Product information/ brochures that is widely distributed Information available on public domains/ company websites Reports as required by regulatory authorities that are made available to the public Newsletters, notices or other public communication for general consumption
Critical	Client Confidential	Information received from clients in any form excluding Personal and Sensitive Personal information for processing. The original copy and/or details of such information must not be changed in any way without written permission or consent from the client. The highest level of integrity, confidentiality and restricted availability are vital as its compromise or loss would have a substantial negative	<ul style="list-style-type: none"> Media devices provided by guests Electronic submissions by customers e.g. electronic feedback forms from Company websites Hard copy feedback forms, letters, answered brochures, raffle tickets,



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 4 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

Classification	Information Category	Description	Examples
		impact upon the Group and affected clients.	etc. that was submitted by customers
Critical	Proprietary and Company Confidential	<ul style="list-style-type: none">• Information collected and used by the Group in and for the conduct of its business, to log and fulfill client orders, and to manage all aspects of corporate finance.• Information integrity is vital as unauthorized access can affect the Group's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.• This information should not be freely distributed or shared as its loss or compromise would have a negative impact on the Company.• Access to this information is restricted within the Company. The highest level of integrity, confidentiality and restricted availability are vital.	<ul style="list-style-type: none">• Marketing information• Business/Corporate plans• Non-disclosure agreements entered by the company• Standard operating procedures used in all parts of the Company's business.• All company developed software codes, food formulas, reports and research documents.
Ultra-Critical	Legal and Regulatory, Financial Records, IT Security	<ul style="list-style-type: none">• Information collected and used by the Group in relation to its obligations under applicable laws and government regulations or in relation to or legal and adjudicatory proceedings. This information should not be freely distributed or shared as its loss or compromise would have a negative impact on the Company. Should be restricted to management approved internal access.• The highest level of integrity, confidentiality and restricted availability are vital.	<ul style="list-style-type: none">• Certificates and licenses issued by government agencies and regulators.• Notices, issuances by courts and legal and regulatory agencies.• Case files and related documents including copies of emails used in legal or administrative proceedings.• Stock certificates, property titles• Other confidential business data and contracts• Stock Certificates• Project Documents (APA, MOA, Deed of assignment of TMs• DOAS of other assets (acquisition of land, buildings)• Financial Documents including submissions to government agencies



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 5 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

Classification	Information Category	Description	Examples
			<ul style="list-style-type: none">• Login credentials and information on corporate security procedures
Ultra- Critical	Personal Information and Sensitive Personal Information	<p>Any information, whether recorded in material form or not, that would allow an individual to be identified, or when put together with other information would directly and certainly identify the individual. While unauthorized processing does not necessarily constitute personal data breach, it could still cause damage to the Group and its data subjects.</p> <p>Sensitive Personal Information refers to:</p> <ul style="list-style-type: none">• race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;• health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;• Data issued by government agencies peculiar to an individual which includes social security numbers, health records, licenses or its denials, suspensions, and revocations, and tax returns; and• Data specifically established by an executive order or an act of Congress to be kept classified. <p>These are documents or files containing data that could cause the most serious harm to data subjects or the Group.</p>	<ul style="list-style-type: none">• HR Documents• Employee 201 Files• Government IDs or licenses• Records of Administrative Proceedings• Documents and records from health care providers, including results of annual physical exams

- 4.2.2.1 To mitigate and manage risks, all Documents maintained by SPAVI shall be designated "Critical" as the default classification regardless of content, unless or until a higher or lower protection level is assigned.
- 4.2.2.2 If multiple classifications are combined or applicable to the information within a Document, the highest level of classification should be assigned to the record or document.
- 4.2.2.3 The Document Classification shall apply from the time the data is created, collected or received and until it is disposed, unless the Document owner decides that the classification should be modified according to the data classification categories. In such a case, the changes should be reflected in the levels and applicable document inventory.
- 4.2.2.4 Document Classification coverage shall be periodically reviewed and updated.



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 6 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

4.3 Categorization and Naming Conventions

4.3.1 All company documents shall observe the standard naming convention and information and Document Classifications in this Policy.

4.3.2 Documents that are routinely produced, submitted and/or created by the Department shall follow a dedicated naming convention that corresponds to the needs of each department and shall be created by the designated Department personnel.

4.3.2.1 Related or supporting documents, annexes and attachments shall be classified and marked in accordance with the classification of the main Document.

4.3.2.2 Hard copies of Documents classified as Ultra-Critical shall be stamped or marked with its Data Classification in a manner that is clearly visible and must be placed in an enclosing folder that is also clearly marked with the Data Classification. Marking of the Document Classification shall be mandatory only for documents classified as Ultra-Critical and folder containing Ultra-Critical Documents.

4.3.1.1 Naming Conventions provided by the Department Managers shall comply with any regulation or requirement under applicable regulatory requirements or certifications (e.g., ISO certifications) but must include the following minimum information:

- i. Version number
- ii. Month-date-year (mm-dd-yyyy)
- iii. Business Unit
- iv. Department
- v. Title of document
- vi. Document category

4.3.3 **Markings.** Documents classified as public and intended for public dissemination must bear the legal, business markings, and legends necessary to communicate SPAVI's ownership, rights, management controls, and information integrity.

4.3.3.1 Legal and business markings include:

- i. Copyright notice shall be placed at the bottom of each page.
- ii. "TM" or "R" symbols for trademarks shall be indicated for word marks, logo marks and image duly registered with the appropriate intellectual property office.
- iii. "Confidential" or "Proprietary" notice or markings
- iv. Signature or name of the SPAVI business unit

4.3.3.2 Electronic mail or e-mails at the point of creation shall contain a disclaimer on appropriate use of information as standard template that will read as follows:

"This email (and any attachment/s) is confidential and for viewing only by the intended recipient/s. If you received this in error, please notify the sending party immediately and delete all copies. Any unauthorized access to, review, reproduce, disseminate or other use of the information contained herein is strictly prohibited. Opinions, conclusions and statements in this email are opinions, conclusions and statements of the sender and are not necessarily given, endorsed, espoused or expressed by SPAVI. The use of email for any unlawful purpose or for any purpose other than what is permitted by SPAVI is also prohibited."

4.4 Document Management

4.4.1 **Safekeeping.** Original or duplicate physical copies of all finalized or signed contracts and Documents shall be submitted for recording and safekeeping purposes in accordance with clause 4.4.5 of this policy.



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 7 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

- 4.4.2 **Uploading of electronic copies.** To preserve important information in a usable format which enables access commensurate with frequency of use, electronic corporate documents or digital copies of original or hard copies of documents shall be created and uploaded to SPAVI's document management platform in accordance with clause 4.4.5 of this policy.
- 4.4.3 **Attachments and Annexes.** Where Documents contain attachments, annexes or schedules, such attachments shall be treated as an integral part of the main Document and stored accordingly.
- 4.4.4 **Consent.** Documents containing Personal Information collected by SPAVI should have or be accompanied by the proper consent or authorization from the data subject. Unless explicitly exempted, consent should be obtained prior to or as soon as practicable after collection, in accordance with SPAVI's Data Privacy Manual.
- 4.4.5 **Storage and Security.** Documents shall be securely stored in reasonable and appropriate facilities based on the classification of the information. Storage arrangements, including methods of storage for physical and electronic records, should ensure that Documents will remain complete, unaltered, and accessible throughout the retention period.
- 4.4.5.1 Physical Documents that require digital preservation/ digitalization and Electronic Documents that is required to be kept for a minimum period of time in compliance with existing laws and regulations shall be kept in a secure facility in accordance with SPAVI's policy on retention of documents.
- 4.4.5.2 SPAVI shall define access rights privileges for Critical and Ultra-Critical Documents.
- 4.4.5.3 Digital or electronic copies of Critical and Ultra-critical Documents are subject to restricted access in accordance with SPAVI's policy on access controls. Access Control Profiles must provide for detailed access controls such as read, editing, downloading, etc. for its specific users.
- 4.4.5.4 Storage requirements for physical and electronic Documents shall be based on the Document Classifications:

Classification	Document Type	Storage requirements
Non-Critical	Physical and/or electronic documents and copies	<ul style="list-style-type: none">• Store in safe and secure physical and/or electronic storage facilities in accordance with the capacity and requirements of the relevant department or Business Unit of the author or user.• Where necessary, copies shall be submitted for archival purposes.
Critical	Physical documents and hard copies	<ul style="list-style-type: none">• Store in a safe and secure physical storage facility in accordance with the capacity and requirements of the relevant department or Business Unit.• Secure in appropriate file cabinets with lock and key for securing specific types of documents.• In case appropriate physical and electronic security assets are not yet in place, Department Heads shall submit the appropriate requests for the provision thereof.
Ultra-critical	Physical documents and hard copies	<ul style="list-style-type: none">• Endorse and store in designated vaults and locked file cabinets in the care of the duly assigned custodian or document owner.• Only officers and employees with the strictest access control profiles shall be allowed to use and handle Ultra-Critical Documents.



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 8 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

Classification	Document Type	Storage requirements
Critical and Ultra-critical	Electronic copies	<ul style="list-style-type: none">• Critical and Ultra-critical Documents should be reported and endorsed to the IT Security manager for enrollment in the appropriate data loss prevention system.• Apply the appropriate Access Control Matrix /Information Rights management system• Apply the appropriate retention periods and schedules to ensure ease of retrieval

4.5 Retention of Records and Documents

4.5.1 **Retention Policy.** Documents shall be kept only for as long as it is required or in accordance with the Records Retention Schedule under Annex A.

4.5.1.1 Documents that contain Personal Information are protected under the Data Privacy Act of 2012 and shall be retained in a form which permits identification of individuals only for as long as is necessary to fulfill the purpose for which it is collected and processed.

4.5.1.2 Documents that have been identified by government agencies (e.g. BIR, National Privacy Commission, Securities and Exchange Commission, Board of Investments, etc.) as stated in the relevant law's implementing rules and regulations must be kept at least for the minimum period as prescribed under the relevant law or regulation.

4.5.2 **Records Retention Schedule.** The retention periods for specific Documents shall be set by the individual Department or Business Unit or Document owners and users.


4.5.2.1 Retention periods may be expressed as a range including the starting point plus the number of additional years to be kept, although a permanent retention period/date may be advised or necessary for some records.

4.5.2.2 In setting retention periods, the following considerations shall be taken into account:

- i. The relevant legal or regulatory requirements for the market concerned.
- ii. Expert advice from appropriate members of SPAVI's Legal, Tax, Internal Audit and Risk departments and/or external counsel.
- iii. The operational and commercial value of data and documents, or the need for evidence of business processes, the probability of future use and the consequences if the information were not available. The value of the information and reference rate usually decline over time so a decision should be made as to the point the records are likely no longer to be required.

4.5.2.3 The Records Retention Schedule shall include the following information:

- i. Record description – The type of record or document, applying to all formats of record.
- ii. Retention period – The recommended length of time for which the records should be kept by the Company.
- iii. Justification for the retention period – The legal/statutory or regulatory basis or other operational or business justification for the retention period should be indicated.
- iv. Action at end of retention period – There are three potential disposal outcomes for a record at the end of its retention period:
 - a) Reappraisal of the document's continued retention
 - b) Long-term preservation / Sending to Company archives


	Manual Title:		
	LEGAL AND COMPLIANCE MANUAL		
	Policy Number:	Effectivity Date:	Page Number:
	SPAVI-LCM-01.2024 Rev 00	January 30, 2024	Page 9 of 15
	Policy Title:		Supersedes Policy Number:
	DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		N/A

c) Destruction

- 4.5.3 **Retention of Records in different mediums.** Retention periods should be the same for the same type of recorded information regardless of media (i.e. information retained in digital format should be retained for the same period as it would be kept in paper form), unless records need to be retained in one format for archival purposes.
- 4.5.4 **Retention of duplicate copies.** It shall not be necessary to retain duplicate copies of the same Document, nor to retain both paper and electronic versions, for the same period, unless a duplicate copy of the Document needs to be retained for archival purposes or is specifically required under a legal or regulatory requirement, or pursuant to a legitimate operational or business justification.
- 4.5.5 **Archiving.** Documents deemed to be of permanent legal or historical significance to SPAVI will be preserved in SPAVI's historical archives [facilities] in a medium or format that will ensure that they will remain complete, unaltered and accessible, in accordance with SPAVI's policy on retention of records. Such records and documents shall be marked "For Archival Purposes."
- 4.5.6 **Retention Review.**
- 4.5.6.1 Documents that that are kept, stored and/or archived must undergo an annual retention review by the Document owner or designated custodian to determine whether there is a need for disposal of extension of the retention period.
- 4.5.6.2 The Records Retention Schedule including assigned retention periods shall be periodically reviewed and updated in accordance with changes in the applicable legal or regulatory requirements and changes in SPAVI's business and legal needs.
- 4.5.7 **Minimizing Retention of Personal Data.**
- 4.5.7.1 Subject to limited exceptions, the collection and retention of Personal Information shall be limited only to "what is necessary" in relation to the purpose of processing.
- 4.5.7.2 Data processing operations shall be periodically reviewed to consider whether any Personal Information that are not strictly necessary in relation to the relevant purposes are being processed.

4.6 **Disposal and Destruction of Documents**

- 4.6.1 **Disposal and Destruction.** The following Documents shall be tagged and processed for disposal or destruction:
- Documents that have passed their stated retention periods or are found to be no longer relevant or needed, whether in digital or hard copy format, unless a legal or regulatory justification is specified, or a Hold Instruction has been issued in relation to the relevant Record; and
 - Personal Information that is inaccurate or out of date must be destroyed/erased if not or is unable to be rectified.
 - Personal Information that is no longer needed for a specific purpose must be deleted (if in electronic format) and/or destroyed (if in hard copy), unless the Document owner or user has determined a legitimate purpose for its retention.
- 4.6.2 **Method of Disposal or Destruction.** Documents shall be destroyed and disposed of in a manner that will prevent unauthorized disclosure during any disposal process in accordance with the document format or medium.
- 4.6.2.1 Physical or hard copies of Documents must be shredded and/or redacted before they are disposed.

	Manual Title: LEGAL AND COMPLIANCE MANUAL		
	Policy Number: SPAVI-LCM-01.2024 Rev 00	Effectivity Date: January 30, 2024	Page Number: Page 10 of 15
	Policy Title: DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		Supersedes Policy Number: N/A

- 4.6.2.2 Softcopies or electronic copies must be thoroughly scrubbed from any disk/digital storage to ensure that there is no opportunity for data recovery by conventional (file restore) and unconventional means (I/O level restore).
- 4.6.2.3 Documents that contain Personal Information shall be destroyed or disposed of in a manner that will ensure anonymization or de-identification and prevent the identification of data subjects.
- 4.6.2.4 Destruction and disposal of Documents classified as Ultra-Critical shall be recommended by the Document Owner, and approved by the Department Head, IT Department Head, CIO and CFO of shall be issued a Certificate of Destruction and Disposal to be signed by approvers.
- 4.6.3 **When Disposal or Destruction shall be permitted.** Documents may only be destroyed or disposed of when all the following conditions are met:
- There is no improper motive for the destruction of the Documents;
 - There is no legal or regulatory reason or requirement to maintain the Documents;
 - The destruction is in accordance with mandated retention periods as set out in Annex A;
 - Destruction or disposal has been approved by the Document Owner or designated custodian; and
 - There is no Hold Instruction in place.
- 4.6.4 **When Disposal or Destruction is a contractual obligation.** The disposal of or destruction of certain Documents or proprietary information provided or shared by in connection with a contract or agreement with a third party, including data outsourcing or sharing arrangements, may be required as a contractual obligation.
- 4.6.4.1 Where SPAVI is contractually required to dispose of or destroy Documents, an official tally or list of the Documents to be disposed of or destroyed shall be prepared and required to be received and signed by the designated recipient of the third-party contractor.
- 4.6.4.2 Where SPAVI contractually requires a third-party contractor to dispose of or destroy Documents, it shall require an official tally or list of the Documents to be disposed of or destroyed, as well as a Certificate of Destruction in case the destruction shall be carried out by the third party contractor.
- 4.6.5 **Hold Instruction.** The Head of Legal or other members of the Tax or Corporate Accounting departments, or the CIO, may, on occasion, notify employees that the routine disposal of certain Documents relating to certain activities must be suspended, usually because of pending or actual litigation or investigation (i.e., on "Legal Hold").
- 4.6.5.1 A Hold Instruction will require that all Documents potentially relevant to the pending or actual litigation or investigation be preserved. If a potentially relevant Document is subject to a Hold Instruction, the original copy of that Document must be retained if possible, and the regular disposal of the same must not be resumed until the Hold Instruction is removed by Legal.
- 4.6.5.2 If an employee believes that he or she may have material or Documents related to a proceeding or that should be subject to a Hold Instruction, but requires advice and assistance, the employee should promptly consult Legal. If there is doubt on whether a Document is relevant to a Hold Instruction, such Document must be preserved and submitted it to Legal for review.
- 4.7 Return of Records and Documents**
- 4.7.1 **Return by Employees.** Employees must return or destroy, at SPAVI's option, all Documents in their possession and control upon the end of their service with SPAVI. This includes, without limitation, physical Document located anywhere including the SPAVI's premises, the personal homes of Employees, authorized storage facilities, and electronic Records.



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 11 of 15

Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

4.7.1.1 The Group reserves the right to audit any SPAVI-issued device or SPAVI-supported personal device upon separation to ensure that it does not contain any SPAVI Documents or Information subject to applicable law and contractual agreements.

4.7.2 **Return by SPAVI.** SPAVI may be required to return certain Documents or proprietary information to third-party contracting parties under certain contractual arrangements. The return of Personal Information or Documents containing Personal Information will usually be required in Data Sharing Agreements.

4.7.2.1 Where SPAVI is contractually required to return Documents, an official tally or list of the Documents to be returned shall be prepared and required to be received and signed by the designated recipient of the third-party contracting party.

4.8 Document Management Framework

This framework shall outline the areas of responsibility in Document Management and the parties responsible.

Areas	Key Responsibilities	Party Responsible
Categorization and Naming	<ul style="list-style-type: none"> Create and maintain the standard naming convention of all Documents that the Department produces, submits and/or creates. Ensure that all naming conventions are submitted to the IT Information Security Manager for inputting and processing by the data loss prevention system of SPAVI. Cascade the Naming Convention and upload the same to DMS. 	<ul style="list-style-type: none"> Department/BU Head Plant Manager /Comptroller
Record and Safekeeping	<ul style="list-style-type: none"> Mark Ultra-Critical Documents received by its Document Classification. Mark Documents with the appropriate legal, business markings, and legends (e.g., "Copyright" notice, "TM" or "R" symbol, "Confidential" or "Proprietary" notice). Stamp or mark the original or duplicate copies of all finalized or signed contracts and Documents and hard copies of Documents with the appropriate data classification 	<ul style="list-style-type: none"> Addressee Document Owner or designated custodian Author Document Owners
Record and Safekeeping	<ul style="list-style-type: none"> Keep original or duplicate copies of all finalized or signed contracts and Documents in a safe and secure physical storage facility Keep and maintain original and electronic copies of Legal and Regulatory Documents including government-issued Certificates and Licenses, notices, issuances and orders issued by courts and legal and regulatory agencies, case files and related documents. Create and upload digital or electronic copies of Documents or SPAVI's document management platform. Ensure all Documents containing personal data collected by SPAVI are accompanied by the proper consent or authorization from relevant data subjects. 	<ul style="list-style-type: none"> Author Document Owners Designated custodian Legal (for Ultra-Critical Documents) Designated Owner or designated custodian Legal Document owners and/or designated custodians Document owners



Manual Title:

LEGAL AND COMPLIANCE MANUAL

Policy Number:

SPAVI-LCM-01.2024 Rev 00

Effectivity Date:

January 30, 2024

Page Number:

Page 12 of 15


Policy Title:

DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL

Supersedes Policy Number:

N/A

Storage and Security	<ul style="list-style-type: none"> • Ensure that the appropriate physical and electronic security assets are used in safeguarding Documents. 	<ul style="list-style-type: none"> • Document owners and custodians • Department /Business Unit Heads
	<ul style="list-style-type: none"> • Determine and apply appropriate storage arrangements for physical and electronic Documents. • Utilize and request for appropriate physical facilities and electronic security assets. 	<ul style="list-style-type: none"> • Department/Business Unit Head
	<ul style="list-style-type: none"> • Keep and maintain original and electronic copies of 	<ul style="list-style-type: none"> •
	<ul style="list-style-type: none"> • Keep all original and digital copies of all stock certificates, formulations and property titles. 	<ul style="list-style-type: none"> • Cathy Uy
	<ul style="list-style-type: none"> • Keep and maintain Business unit/ Plant based contracts or Documents, with copies furnished to the Corporate Comptroller and Business Unit Heads. 	<ul style="list-style-type: none"> • Company/Plant Comptroller and Business Unit Heads.
	<ul style="list-style-type: none"> • Report Critical and Ultra-critical Documents to the IT Security manager for enrollment in the data loss prevention system. 	<ul style="list-style-type: none"> • Author • Document owners and custodians
	<ul style="list-style-type: none"> • Define access rights privileges for officers and employees 	<ul style="list-style-type: none"> • Management
	<ul style="list-style-type: none"> • Create Access control profiles for officers and employees based on access rights privileges 	<ul style="list-style-type: none"> • IT Department
Retention of Records and Documents	<ul style="list-style-type: none"> • Set or assign retention periods for specific Documents 	<ul style="list-style-type: none"> • Document Owner • Department/Business Unit Head
	<ul style="list-style-type: none"> • Prepare and maintain an inventory of Documents kept and maintained by the Business Unit/Department. • Include references to the legal and regulatory requirements on which retention periods are based in the records inventory of each Business Unit • Regularly review legal and regulatory requirements to ensure continued compliance. • Conduct annual review of Documents kept, stored and/or archived to determine whether there is a need for disposal of extension of the retention period. • Periodically review data processing operations for any Personal Information that are not strictly necessary in relation to the relevant purposes are being processed. 	<ul style="list-style-type: none"> • Individual Business Units • Document owner or designated custodian
	<ul style="list-style-type: none"> • Periodically review and update the Records Retention Schedule in accordance with changes in the applicable legal or regulatory requirements and changes in SPAVI's business and legal needs. 	<ul style="list-style-type: none"> • Individual Business Units • Corporate Tax • Corporate Accounting • Legal and Compliance
	<ul style="list-style-type: none"> • Preserve and maintain Documents deemed to be of permanent legal or historical significance to SPAVI in SPAVI's historical archives [facilities] 	<ul style="list-style-type: none"> •

	Manual Title:		
	LEGAL AND COMPLIANCE MANUAL		
	Policy Number:	Effectivity Date:	Page Number:
	SPAVI-LCM-01.2024 Rev 00	January 30, 2024	Page 13 of 15
	Policy Title:		Supersedes Policy Number:
	DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		N/A

Disposal and Destruction	<ul style="list-style-type: none"> Review and tag Documents for disposal or destruction 	<ul style="list-style-type: none"> Document owner/custodian Department/Business Head
	<ul style="list-style-type: none"> Review and approve Documents for disposal or destruction 	<ul style="list-style-type: none"> Department/Business Head
	<ul style="list-style-type: none"> Shred physical or hard copies of Documents before they are disposed. 	<ul style="list-style-type: none"> Document owner/custodian
	<ul style="list-style-type: none"> Scrub softcopies or electronic copies from any disk/digital storage to ensure that there is no opportunity for data recovery by conventional (file restore) and unconventional means (I/O level restore) 	<ul style="list-style-type: none"> Document owner/custodian IT Department
	<ul style="list-style-type: none"> Issue Hold Instructions for Documents subject of or to be used in pending or actual litigation or investigation 	<ul style="list-style-type: none"> Head of Legal Designated officers from the Tax or Corporate Accounting departments CIO
	<ul style="list-style-type: none"> Report and consult Legal on any material related to a proceeding or that should be subject to a Hold Instruction. 	<ul style="list-style-type: none"> All employees
Return of Records and Documents	<ul style="list-style-type: none"> Prepare an official tally or list of the Documents to be disposed of or destroyed by SPAVI under contract 	<ul style="list-style-type: none"> Document owner
	<ul style="list-style-type: none"> Receive the official tally or list of the Documents to be disposed of or destroyed and Certificate of Destruction in case the destruction shall be carried out by the third-party contractor 	<ul style="list-style-type: none"> Document owner

4.9 Non-Compliance and Penalty


- 4.9.1 All employees are required to consistently follow this Policy to ensure compliance with all applicable legal, regulatory and business-related recordkeeping requirements.
- 4.9.2 All employees shall be responsible for observing and upholding the guidelines and restrictions for classified company Documents. All employees shall be responsible for preventing unauthorized access to review, reproduce, disseminate or any other use of the information contained in the subject classified Document. If an employee receives a classified Document in error, said employee must notify the sender and/or Document owner of the Document's mishandling and immediately delete and/or destroy all copies of the document.
- 4.9.3 Any and all violations to this policy are subject to appropriate penalties as provided for in the employee handbook where company rules and regulations are not followed or observed.



Manual Title: LEGAL AND COMPLIANCE MANUAL		
Policy Number: SPAVI-LCM-01.2024 Rev 00	Effectivity Date: January 30, 2024	Page Number: Page 14 of 15
Policy Title: DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		Supersedes Policy Number: N/A

Annex A
Record Retention Periods

Records Category	Retention Period	Specific Basis for Retention	Action upon expiration of retention period
Constitutional/Corporate Records			
Statutory registers	Life of company		*Archive
Constitutional documents including: Certificates of incorporation/name change; memorandum and articles of association; resolutions Shareholder agreements Directors' service contracts Contract for purchase of own shares	Life of Company Life of Company 6 years after Expiry 10 years from purchase		
Share issuance documents	Later of 6 years and date on which shares are fully paid		*Archive
Share transfers and related documents, including: Share and stock transfer forms Letters of indemnity for lost certificates Cancelled share/stock certificates	[10 years if on or after 6 April 2008; 20 years if before that date] Life of company 1 year after registration of transfer		
Property Titles			
Legal and Compliance Records			
Contracts and Related/Supporting Documents	26 months after expiration		Re-appraise
Special Project files			
Case files			
IP registration certificates	1 year after expiration		Archive electronic copy
Finance and Accounting Records			
Procurement contracts for the purchase of: Capital goods (Domestic and International) Inventory (Domestic and International) Marketing Materials,	5 years from expiration		
Contracts for: Related Party Purchases, Services, Rentals, Freight, Warehouse Rentals and Fees, Brokerage fees, Advertising, Manpower Services, Utilities, Accommodations, Consultancy Services,	5 years		
Documents relating to Government Remittances: BIR, SSS, PhilHealth, HDMF,	5 years		

	Manual Title: LEGAL AND COMPLIANCE MANUAL		
	Policy Number: SPAVI-LCM-01.2024 Rev 00	Effectivity Date: January 30, 2024	Page Number: Page 15 of 15
	Policy Title: DOCUMENT MANAGEMENT, RETENTION AND DISPOSAL		Supersedes Policy Number: N/A

Records Category	Retention Period	Specific Basis for Retention	Action upon expiration of retention period
Documents relating to Payroll, and Employee Compensation and Benefits (loans, commissions and incentives, reimbursements)	5 years		
Documents relating to sales (processing of payment and collections, return of goods, deductions, zero-rated sales, etc.)	5 years		
Treasury Documents			
BIR Filings and Tax Assessments			
Financial Statements	5 years		
HR Records			
Employee 201 Files (including PIS, Government IDs and records, Employee Information, Performance Management, Employee Movement, Employee Discipline, Confidentiality/Non-Disclosure/Non-Compete/Proprietary Information Agreement Form, APE Records, etc.)	5 Years from Separation of Employee		
Employee Relations and Labor Relations (Administrative Proceedings, Labor Cases,)	5 Years from Separation		
Service Agreements, Consultancy Contracts	5 Years from Separation		
Organization Health and Safety Documents, DOLE Documents and Permits	5 Years from Separation		
Documents relating to talent acquisition (Talent Assessments and Profiles)			
Customer Information and Records			
