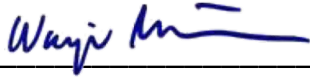


Subject :	Information Safeguarding Guideline
------------------	------------------------------------

Downloaded from <http://ajphaphysocpharm.sagepub.com/> at 10:06 10 May 2015

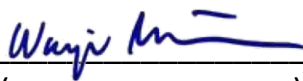
[illegible]



Unit / Division Owner :	RISK MANAGEMENT & INTERNAL CONTROL		
	Document Type : Guideline		
	Document Number :		Revision : 1 Jan 2021
	Effective Date :	1 January 2019	Page No.: 2 / 6
	Approved by  _____ (Wannipa Bhakdibutr) President		

Subject : Information Safeguarding Guideline



	Unit / Division Owner : RISK MANAGEMENT & INTERNAL CONTROL		
	Document Type : Guideline		
	Document Number :		Revision : 1 Jan 2021
	Effective Date :	1 January 2019	Page No.: 3 / 6
	Approved by  (Wannipa Bhakdibutr) President		

Subject : Information Safeguarding Guideline

Information Safeguarding Guideline

1. Introduction

The objective of the Information Safeguarding Guideline (IS Guideline) is to provide guidance for complying with Company Asset Policy Statement requirements for safeguarding information as stated in Osotspa's Code of Conduct. Specifically this guideline addresses the protection of Company Information. Company Information is defined as nonpublic information that is created by, created for or otherwise by Osotspa.

Company Information used by employees and contractors in the course of Osotspa business activities is a valuable asset that should be appropriately safeguarded against unauthorized disclosure, modification, or loss.

Appropriate cost-effective protective measures relevant to the associated risk should be implemented based on sensitivities and value of the information to the company and to others. In addition, good judgement and application of common sense are integral tools in protecting information.

2. Scope

All Company Information is subject to this guideline. The Guideline is applicable to Osotspa Public Company Limited and its affiliated companies in Thailand and in other countries.

3. Roles and Responsibilities

Information safeguarding is a responsibility of all employees. This includes roles in exercising appropriate controls, protecting, storing and communicating the company information.

- **Internal Control** : own and maintain the IS Guideline. They coordinate with relevant functions to provide guidance and training regarding the protection of information.
- **Business Unit / Function Management** : is responsible for its functional or business unit compliance with the IS Guideline.
- **Employees** : are responsible for properly handling information and making appropriate arrangements for safeguarding information. All employees who share Osotspa information with third parties are responsible for following business controls for the appropriate protection of information including the release of information outside the company and should ensure that third parties are aware of their responsibility to protect Osotspa information as agreed in the business arrangement.

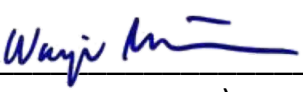
4. Information Protection and Classification Principles

Information security vulnerabilities exist both within and outside the Company. This has potential for significant financial, reputation and competitive advantage damage to the Company and should be guarded against through the application of information security principles in this Guideline.

All Company Information should be safeguarded and considered for classification and labeling by its owner and protected by its handlers (e.g., authors, owners, recipients).

The classification level is based on the value of the information to the Company and the consequence of inappropriate disclosure, modification or loss.



Unit / Division Owner :	RISK MANAGEMENT & INTERNAL CONTROL		
	Document Type : Guideline		
	Document Number :		Revision : 1 Jan 2021
	Effective Date :	1 January 2019	Page No.: 4 / 6
	Approved by  (Wannipa Bhakdibutr) President		

Subject : Information Safeguarding Guideline

The three classification levels for Company Information – i) Company Use Only; ii) Proprietary or Private; and iii) Restricted Distribution – are defined in *Section 7.1*.

Access to Information, particularly classified information, should be reasonably limited to that which is needed as part of a job / business role. Also note that certain information access may be restricted by Data Privacy Laws or other agreements or obligations (e.g., non-disclosure agreements), regardless of classification.

Release of Company Information, regardless of its classification, may only be released to third parties, including joint ventures, through an appropriate and approved release process including non – disclosure agreements. The existence of non – disclosure agreement alone does not preclude use of this process.

5. Labeling

Unclassified information requires label as Company Use Only. All classified information should be labeled according to its classification of Proprietary, Private or Restricted Distribution. All pages of a document containing classified information should be labeled based on the highest classification on information contained within it. Regardless of classification, the information may not be disclosed or used outside the Company without following appropriate release processes.

Additional designations, which may also be required on some information, are beyond the scope of this IS Guideline. These additional designations include:

- **Privileged and Confidential** – Used at the direction of Legal and Tax Departments
- **Confidential** – May be used to establish Osotspa intellectual property rights for information shared with third parties


6. Control Points and Handling

Protection of information incorporates barriers, or control points, commensurate with the classification level. A control point limits access to electronic or physical information. Currently our security measures ensure that at least one physical control point exists at the majority of the Company facilities, generally at the controlled entrance. Each additional physical control point further restricts access to the information. Electronic and physical control points should not be used in combination with each other to satisfy the number of necessary control points. Physical control points can only be used to protect physical information, and electronic control points can only be used to protect electronic information.

Because of the inherent single control point at most Osotspa facilities, unclassified information does not require any additional control points. Information classified as Proprietary or Private requires two control points. Restricted Distribution information requires three control points. Refer to section 7 for further classification considerations (*Section 7.1*) and guidance on control points (*Section 7.2*).

If a recipient of information perceives that the information is incorrectly classified, the information should be protected as labeled or perceived classification (whichever is higher) until the issue is resolved between the recipient and the information's owner. Do consult the owner before further sharing of **Restricted Distribution** information.



Unit / Division Owner :	RISK MANAGEMENT & INTERNAL CONTROL		
Document Type :	Guideline		
Document Number :		Revision :	1 Jan 2021
Effective Date :	1 January 2019	Page No.:	5 / 6
Approved by	 (Wannipa Bhakdibutr) President		


Subject : Information Safeguarding Guideline

7. Classification and Control Points Considerations

7.1 Classification Levels

Types of Company Information		Examples	Labelling	# Control Points
Unclassified Information	Information that is not subject to classification as described below. If inappropriately disclosed or disseminated, would not have significant effect on the company or others.	<ul style="list-style-type: none"> Majority of Company Information that is for internal/business uses should fall under this category. 	Company Use Only	1
Classified Information	Sensitive Company Information regarding individual employees such as performance ranking and appraisal, medical or illness data obtained during employment, pre-employment background screening reports and salary information, etc. This information should be handled in compliance with HCOE Guidelines.	<ul style="list-style-type: none"> Personal Information and Salary Performance ranking data and appraisals Individuals employment, information Medical or illness records 	Private	2
	Information that is of specific value to business and its access is limited. If inappropriately disclosed, could influence operational effectiveness, or could have significant effect on company, e.g., earnings, reputation or competitive advantage, etc.	<ul style="list-style-type: none"> Financial and Operating Performances reports and related Analysis Business plans or targets Company's know-how used to process and operate business Internal Audit reports 	Proprietary	
	Information that, if inappropriately disclosed or disseminated, could have severe damaging consequences / penalties for the company	<ul style="list-style-type: none"> Key business strategic / investment / divestment plans not yet announced Trade secrets / formulas New product launch plan Earnings not yet disclosed to SET/public 	Restricted Distribution	3



	Unit / Division Owner : RISK MANAGEMENT & INTERNAL CONTROL		
	Document Type : Guideline		
	Document Number :	Revision :	1 Jan 2021
	Effective Date :	1 January 2019	Page No.: 6 / 6
	Approved by  (Wannipa Bhakdibutr) President		

Subject : Information Safeguarding Guideline

7.2 Control Points (Examples)

	Unclassified Information	Classified Information	
Classification & Labeling	Company Use Only	Private / Proprietary	Restricted Distribution
# Control Points Protection	1	2	3
Control Points			
Physical Information <u>Examples:</u> printouts, reports, files, folders, etc.	<ul style="list-style-type: none"> Employee badge – getting through office building entrance 	<ul style="list-style-type: none"> Employee badge Locked drawer or cabinet 	<ul style="list-style-type: none"> Employee badge (1) Locked drawer or cabinet (2) Restricted office/ area, individual locked office (3)
Electronic Information <u>Examples:</u> data, files, folders stored in computing system or other electronic medias.	<ul style="list-style-type: none"> Log on or User ID & Password – getting into Company's computing system or network 	<ul style="list-style-type: none"> Log on User ID & Password Folders in shared drive accessible by authorized users 	<ul style="list-style-type: none"> Log on / User ID & Password (1) Folders in shared drive (2) Files/folders with encryption, password-protected (3)

Consideration: Electronic and physical control points should not be used in combination with each other to satisfy the number of necessary control points. Physical control points can only be used to protect physical information, and electronic control points can only be used to protect electronic information.

8. Release of Company Information

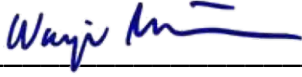
Company Information is valuable asset, which is owned by the company and should be safeguarded according the the above guidance. Generally, employees should not release Company Information outside the company.

Release of Information outside the company, regardless of its classification, may only be released to public, third parties, including joint ventures, through an appropriate and approved release process including non-disclosure agreements. The existence of non-disclosure agreement alone does not preclude use of this process.

Release of Information should receive prior review/approval by management and endorsement by functions relevant to the nature of information, e.g. Finance & Accounting, Investor Relations, Legal, Corporate Communication. Exception is for that of recurring reports as required by laws and regulations with established management review/approval and internal control process in place.

Osotspa has designated authorized channels or appointed persons for handling the release of Company Information or communicating business updates or company news with third parties. Employees should exercise extreme care and be mindful not to release Company Information without prior appropriate review/approval process, e.g., through social medias, in public areas or at social events, etc.



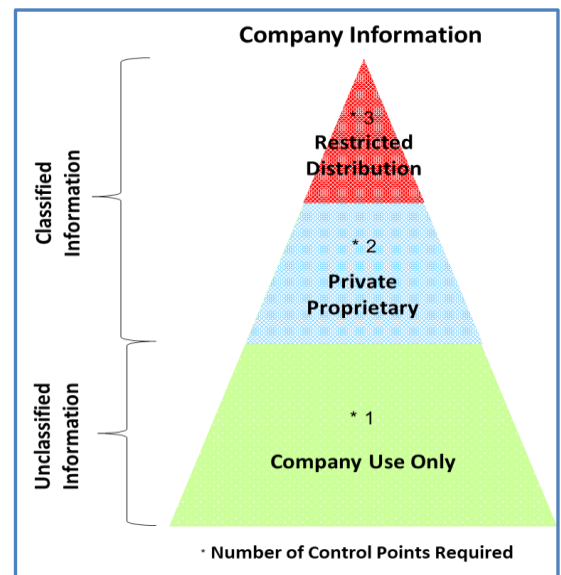
Unit / Division Owner :	RISK MANAGEMENT & INTERNAL CONTROL		
Document Type :	Guideline		
Document Number :		Revision :	1 Jan 2021
Effective Date :	1 January 2019	Page No.:	7 / 6
Approved by	 (Wannipa Bhakdibutr) President		

Subject : Information Safeguarding Guideline

Information Safeguarding (IS) Guideline – Quick Reference Card

Information Protection Steps

1. **Classify** Information – Use the IS Guideline to determine if/how information should be classified.
2. **Label** Information – If the information is classified, put classification label in a prominent location such as the document header or footer. All pages of a document containing classified information should be labeled based on the highest classification of information contained within it.
3. **Protect** Information according to its classification through use of control points.
4. Exercise care and good judgment in the handling of all information – Protecting information throughout its lifecycle is the responsibility of all employees.



Types of Company Information		Labeling Required	Classification Level	# Control Points
Unclassified Information	Information that is not subject to classification as described below. If inappropriately disclosed or disseminated, would not have significant effect on the company or others.	Yes	Company Use Only	1
Classified Information	Sensitive Company Information regarding individual employees such as performance ranking and appraisal, medical or illness data obtained during employment, pre-employment background screening reports and salary information, etc. This information should be handled in compliance with HCOE Guidelines.	Yes	Private	2
	Information that is of specific value to business and its access is limited. If inappropriately disclosed, could influence operational effectiveness, or could have significant effect on company, e.g., earnings, reputation or competitive advantage, etc.	Yes	Proprietary	
	Information that, if inappropriately disclosed or disseminated, could have severe damaging consequences / penalties for the company	Yes	Restricted Distribution	3