1.0 Overview

Information being the primary asset, all the employees should understand appropriate data access and handling procedure of information assets at MSP. This is to protect the assets from being inadvertently compromised by unauthorized personnel using unsecured media.

2.0 Purpose

This procedure will help employees in understanding the information available on different media types, information sensitivity through confidentiality rating and the correct procedure to handle such Information.

3.0 Scope

This is applicable to all the business related information of MSP. The scope of access extends to employees of MSP, who have access to such information.

4.0 Policy and Procedure

4.1 General

The guidelines given, provides the classification of different types of information, media types in which the information is stored, handling and storage of the same.

This applies to:

1. Information in hard copy
2. Information in electronic form
3. Equipment or Software handling classified information

Source	Description	Identification
PC/ Server / Laptop / Portable hard disk drive	Information shall be stored onto respective folder on the hard disk drive.	Identification of organization property will be by the sticker or product label. Password protection mechanisms should be adopted during booting or for the drives, as applicable.
CD ROM/ DVD/Floppy/ USB	Shall be used to backup/transfer limited information	Identification of organization property will be by the sticker or product label. It is recommended that the cover/item should be labeled indicating the confidentiality rating for restricted items.
Paper	Information can be available on Paper media such as signed agreements, contracts, ownership documents, company letters,	The organization logo or Company Name in the header will identify an official document. Confidential documents has the confidential status

Source	Description	Identification
	security documents, ISO documents, production records etc.	on the footer
Electronic Form	Information may be transferred/ received in this form having attachments.	Official emails will be identified from the domains from which they are sent. Restricted information should be sent with in a password-protected manner, with the password sent independently and there should be a disclaimer in emails.
Others	Any other industry standard media types shall be used only on System administrators / management approval.	Based on the media type the appropriate identification mark will be assigned.

LEVEL NO.	LEVEL	INFORMATION TYPES	ACCESS TO	APPROVING AUTHORITY	ACCESS RESTRICTIONS
Level 1 (Category 0)	**PUBLIC**	Website information Ex.: Press release and publications	General public	Internal/ External NA	Public domain. No authentication required.
Level 2 (Category 1)	**COMPANY INTERNAL**	**Production Details** (Product Details, Stock Details, Quality Reports etc) **QA** Templates/Formats **Security Documents** Internal Audit Results, Minutes of MRM **General** ISO Systems Procedures, processes, card layouts etc	Access restricted to employees of the respective projects/units Non-employees (respective clients/prospects/ consultants) - used for business purposes only.	Internal NA External Distribution/approval is at management's discretion. Distribution to external parties should be authorized/ marked to the reporting authority.	Electronic distribution – official authenticated ids.
Level 3 (Category 2)	**SENSITIVE (Confidential)**	**Production Details** (Product Details, Stock Details, Quality Reports, Artwork, Speciments, Work order, Job card etc) **Customer Data** (Account Number, Card Numbers, Transaction MIS, MIS Reports)	Access granted only to authoirzed employees only and specifc employees on a need-to-know/handle basis.	Internal Approval required by the concerned business owner/management External Distribution/approval is at management's discretion. Distribution to external parties	Electronic distribution – official authenticated ids. Verbal communication to official/ authorized callers. Fax/photocopies

LEVEL NO.	LEVEL	INFORMATION TYPES	ACCESS TO	APPROVING AUTHORITY	ACCESS RESTRICTIONS
		Others - Issuer confidential data - Card personalization data - Transport code - Supplier documents - Software related data - Source code		should be authorized/ marked to the reporting authority.	will be submitted to office staff for distribution, the same is recorded
Level 4 (Category 3)	**RESTRICTED (Highly Confidential)**	**Customer Data** (Embossing/pin data files, Pin mailers, Security Keys, Processed files,OTP,Biometric & Demographic Details if any) **Operations Data** (I/P address / User Ids / Passwords to Production Systems, Cryptographic data and keys) **Customer provided items** (Dongles, CDs, Manuals) **Strategic Information** (Commercials, company info like strategic plans and contracts, personnel files)	Access granted only to authorized employees/personnel. Access granted to respective external parties (Customers) as a business need-to-know	Internal Approval required by the concerned business owner/management While submitting to trainees –commercial info to be masked or withheld. External Distribution/approval is at management's discretion. Distribution to external parties should be authorized/ marked to the reporting authority.	Electronic distribution – official authenticated ids. Verbal communication to official/ authorized callers. Fax/photocopies will be submitted to office staff for distribution, the same is recorded

	Public	Company Internal	Sensitive	Restricted
Labeling (Paper/fax, Diskette, or Tape)	Accessible to all.	Recommended that media containing this information should be official media. Official hard copies will be identified by the MSP title, copyright notice, and footer (either "Confidential – for internal / limited use, or the Client's title)		
Labeling (Electronic File or E-mail)	Accessible to all.	Appropriate markings (should indicate "Confidential;" where possible) within the attachment and the email should contain the "MSP disclaimers".		
Storage (Paper, Diskette, or Tape – media/backup media containing the information)	Accessible to all.	Secure office	Storage in a locked drawer, file cabinet, or office required. If stored in an open-file storage area, access to the area must be restricted to authorized personnel	Storage in a locked drawer, file cabinet, or office required. If stored in an open-file storage area, access to the area must be restricted to authorized personnel
Storage (Electronic File or E-mail)	Accessible to all.	System and email/email client should be password protected		
Retention Period*	-	The final versions of documents / records relating to projects are retained as long as the relationship is ongoing. Subsequently the documents are archived. The minimum period would be one year.	The final versions of documents / records relating to projects are retained as long as the relationship is ongoing. Subsequently the documents are archived. The minimum period would be one year.	The final versions of documents / records relating to projects are retained as long as the relationship is ongoing. Subsequently the documents are archived. The minimum period would be two years.
Transmission (Paper/fax, Diskette, or Tape)	Accessible to all.	Internal – No security requirements. External – Appropriately marked and sealed to prevent unauthorized access. It is recommended that contents on storage media be password protected for further security. Items will be transported by known persons (employees) or recognized agencies.	Appropriately marked and sealed to prevent unauthorized access. It is recommended that contents on storage media be password protected for further security, unless the recipient specifies otherwise. Items will be transported by authorized persons (asset owner, employees) or recognized agencies.	

	Public	Company Internal	Sensitive	Restricted
Transmission (E-mail or Electronic File)	Accessible to all.	Information may be sent via email containing the "MSP disclaimers".		Information may be sent in via email with "MSP disclaimers". Recommended that files should be password protected; password sent independently.
Disposal * (Paper, Soft copy)	Accessible to all.	Hard copies which are non-essential can be destroyed as per destruction WI Soft copies which are non-essential can be deleted, else should be separated or identifiable (version number / date) from the current documents.	Hard copies which are non-essential can be as per destruction WI Soft copies which are non-essential can be deleted, else should be separated or identifiable (version number / date) from the current documents.	Dispose of the Confidential Information (directly submitted by the client to the organization) will be as specified in the Agreement. Other non-essential restricted hard copies should be destroyed manually or through shredder (pin mailers) and a record of the same maintained. Disposal of client data will be informed to the client before disposal. Soft copies which are non-essential can be deleted, else should be separated or identifiable (version number / date) from the current documents.
Disposal (Diskette, Hard Disks/Drives, or Tape)	Accessible to all.	Broken Manually by MSP in front of IT Security manager		

Data Transfer Process for Level 3 (Category 2) and Level 4 (Category 3)

1. All data are always be encrupted and sent to the customers or users.
2. No data is transferred between more than one facilities
3. Once the confidential and highly confidential datas are received from customer it will be handeled as per the defined procedure.

Enforcement

Any employee found to have violated this policy would be subject to disciplinary action, up to and including termination of employment.