

Documentation & Maintenance of Records

Lesson 2

KEY CONCEPTS

■ Document ■ Record ■ Repository ■ Coding ■ Archive ■ Privacy Control ■ Record Room

Learning Objectives

To understand:

- Effective documentation provides easy access to the required information on time for the effective and timely utilization of the Information.
- What are the statutory provisions with respect to preservation of records.
- The importance of the documentation and record maintenance and the principles of the good documentations.
- The document management system.

Lesson Outline

- Introduction
- Purpose of Documentation
- Electronic Repository of Documents
- Maintenance and Inspection of documents in electronic form under Companies Act, 2013
- Virtual and Physical data room – A comparison
- Coding and Nomenclature
- Safety & Retrieval of Records
- Preservation of Records
- Setting up of a record room
- Privacy of Records and its control
- Lesson Round-Up
- Glossary
- Test Yourself
- List of Further Readings
- Other References (Including Websites / Video Links)

REGULATORY FRAMEWORK

- The Companies Act, 2013
- The Companies (Management and Administration) Rules, 2014
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015

INTRODUCTION

Document means:

A document is a part and parcel of written, printed, or electronic matter that provides certain information. The information may be in a structured or unstructured format. Documents may usually be changed and revised as per requirement. In our daily lives, we all create, receive and use documents. The emails we send and receive, reports, shopping lists, etc. are all examples of documents.

Record means:

A record is a matter of evidence about the past. Many records initially start out as documents and later become records when they are used as evidence. Records can be used as proof in legal obligations or in the transaction of business. It is also important to keep in mind that not every record is a document. For instance, a taped conversation between two persons may be used as a record to conclude that they were framing a conspiracy. Some examples of records may include final reports, emails confirming actions or decisions, photographs, spreadsheets, business contracts, etc.

The primary responsibility of a Company Secretary is to prepare and maintain the secretarial and other records, which are required to be kept by the company and in many cases the role is extended towards creating & execution of the critical corporate records. This requires a good understanding of what documents need to be created, what is the purpose of such documentation, how much details are required to be disclosed in any documents etc.

At the next level of the documentation, it is the duty of the Company Secretary to ensure the confidentiality of the documents and check whether or not the document requires any further action, also to check whether it is consistent with prior records (in both substance and form), or if it conflicts with corporate policies, may create concerns under existing agreements, may result in a violation of law, or may have tax implications etc.

CASE LAW

Consequences of non-maintenance of record (updated Register of Members)

In the matter of *M/s. SDU Holdings Private Limited*, the Registrar of Companies, Bangalore, has passed an adjudication order by imposing of penalty, for violation of provisions of section 88 of the Companies Act, 2013. As per the provisions of the Companies Act, 2013, every company limited by shares shall from the date of its registration, maintain a register of its members in form no. MGT-1.

During the course of enquiry pursuant to section 206 of the Companies Act 2013, the inspection officer persuaded the statutory registers maintained by the company and noticed that the register Form No. MGT-1 maintained by the company is incomplete. Taking on account of default, the adjudication officer gave reasonable opportunity to being heard to the company and every officer in default by way of giving personal hearing notice.

Consequently, the Adjudicating Officer, after having considered the facts and circumstances of the case and also the submissions made by the company and its director during the personal hearing, decided to impose the penalty on the company and its directors for non-compliance of section 88 of the Companies Act, 2013.

Source: <https://www.mca.gov.in/content/mca/global/en/data-and-reports/rd-roc-info/roc-adjudication-orders.html>

The Company Secretary is also responsible for storing, maintaining, retrieving, certifying, and explaining corporate documents. Many issues are implicated relating to document storage, including the span of time the records need to be retained, ensuring the documents are stored in a safe place, whether documents are backed up, either in hard copy or electronically, and their timely access. A Company Secretary is often responsible for documents relating to subsidiaries, joint ventures, consortiums, and other entities also, many of which may be at locations other than corporate headquarters, including locations around the world. In such cases, the Company Secretary must consider whether and to what extent, he should rely on local partners in maintaining and creating corporate records, as well as to what extent he or she must exercise oversight. The Company Secretary may also execute documents on behalf of the company and may be involved in maintaining or advising with respect to the corporate website and social media.

CASE LAW

In the matter of *Welspun Project Ltd. V. National Company Law Tribunal, Ahmedabad Bench (T.P. NO. 149/621A/NCLT/AHM/2016)*, it was observed that the Register of directors' shareholding of the petitioner company did not disclose the complete particulars as required under section 307 of the Companies Act, 1956 (now section 170 of the Companies Act, 2013). ROC's report observed that this violation was committed for about 8 years. Petitioners admitted such violation and filed petition under section 621A (now section 441) for compounding violation. The offence committed was compounded on payment of fine.

PURPOSE OF DOCUMENTATION

Client Service: Documentation is a tool for professionals to serve better to their clients in a timely and effective manner.

Communication: Documentation is the base for better communication between professionals. Clear, complete, accurate and factual documentation provides a reliable permanent record of client.

Accountability: Documentation demonstrates professional accountability and records the work of the professional. It may be used in relation to performance management, internal inquiries, regulatory proceedings and/or legal proceedings.

Professional Responsibility: Documentation is an integral part of professional practice and forms the basis for evidence of professional conduct.

Legal Requirement: Professionals are required to make and keep records of their professional work in accordance with practice standards followed and organisational policy. However, the laws mandate specific information to be recorded and maintained.



Quality: Documentation may be used to evaluate professional practice in terms of Peer reviews, Quality reviews, audits and accreditation processes, Regulatory inspections or critical incident reviews.

Research: Documentation is a valuable source of data for researchers. It provides information to professional, evaluates client outcomes and is a concise record, essential for accurate research data and evidence based practice.

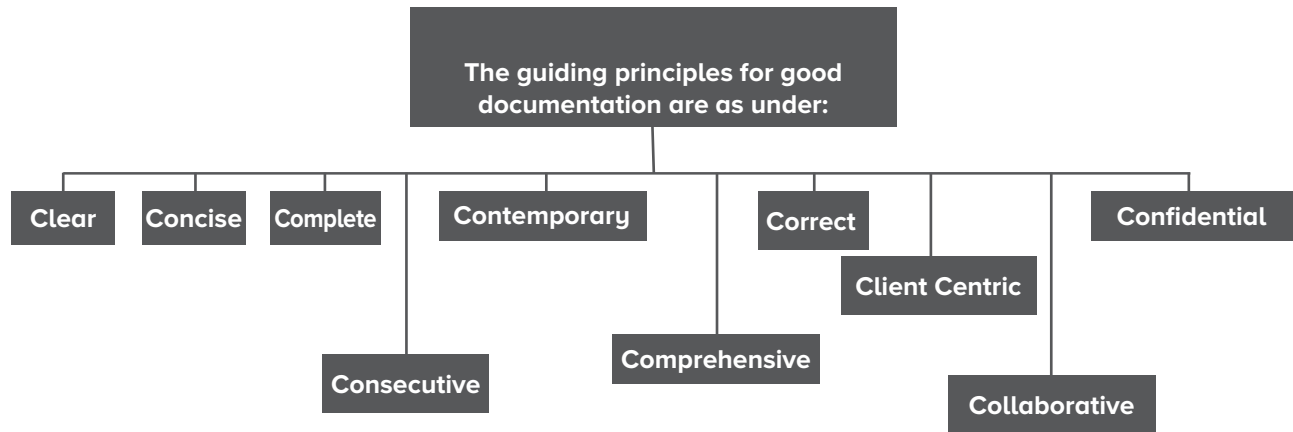
Resource Management: Accurate and comprehensive documentation is a valuable source of evidence and provide basis for resource management.

Illustration:

A multinational company conducts operations across the globe and employ millions of people and on every day basis millions of transactions are carried out. To maintain the company's interest, ensure the proper compliance of statutes, and retain the confidence of the stakeholders, proper documentation must be carried out.

Guiding Principles of Good Documentation

The term documentation includes any and all forms of documentation recorded by a person in professional capacity in relation to his professional duties and includes written and electronic records, audio and video tapes, emails, facsimiles, images (photographs and diagrams), charts, check lists, communication books, management reports, incident reports and working notes or any other type or form of documentation. The good documentation promotes good corporate governance practices and compliance level of the company and also improves communication and dissemination of information between and across various stakeholders. These guiding principles support professionals, employers, policy makers and managers in assessment, planning, execution and evaluation. Also, the good documentation practices and policies demonstrate the professional obligation, accountability and legal requirement to communicate and record client information and good secretarial practice.



What is Good Documentation Practice?

Good documentation practices is a set of best practices for documentation and recordkeeping. It aims to preserve the data integrity of important documents and records and can also serve as guidelines for how to record information and store data appropriately.

Examples of Poor Documentation Practices

The following are the some of the examples of poor documentations practices:

- Document with errors, correction, not signed/dated, and didn't include a reason for the correction;
- Write-overs, multiple line-through and use of "White-out" or other masking device;
- Recording of events is not in sequence & tabled;
- The delegation of work is not recorded/documentated;
- Standards operating procedures as adopted by the professional is not authorised;
- Out-of-specification procedure not detailed enough; flow chart and/or check list not available.

Examples of Good Documentation Practices

The following are the some of the examples of good documentations practices:

- Records should be completed at time of activity or when any action is taken;
- Superseded documents should be retained for a specific period of time;
- Concise, legible, accurate and traceable;
- Picture is worth a thousand words;
- Clear examples;
- Don't assume knowledge/information.

Illustration:

A regulatory authority has some follow-up questions for a business that has recently submitted evidence of its compliance.

Scenario 1- If Documentation Followed: Since the business immediately knows the person who recorded the compliance data, they are able to fetch more information and even able to answer the follow-up questions of the regulatory authority spontaneously. Consequently, the regulatory authority is able to confirm that the business is compliant.

Scenario 2- If Documentation Not Followed: Since the records submitted as evidence of compliance don't identify the person who is responsible for creating them, the business is having difficulty finding more information on their compliance data. They are unable to answer the regulatory authority's follow-up questions and consequently are in danger of being deemed as non-compliant by the regulatory authority.

CASE LAW

In the matter of *M/s Indiabulls Real Estate Limited, the Registrar of Companies, NCT of Delhi & Haryana*, has passed an Adjudication order for non-compliance of the provisions of sub-section (10) of section 118 (mandatory observance of Secretarial Standards with respect of general and board meetings) of the Companies Act 2013 read with Secretarial Standards – 1 & 2.

As per section 206(5) of the Companies Act 2013, the Central Government carried out the inspection of the books of accounts of the company and after going through the records / documents of the company, the inspector, upon completion of the inspection observed that the company has not complied with the provisions of section 118 (10) read with Secretarial Standards. The inspector while submitting the report pointed out that the company has not serially numbered their "Attendance Register" of board meetings and other meetings and also the "Attendance Register" maintained in loose-leaf form, not bound periodically, which is not in compliance with section 118 of the Companies Act 2013 read with Secretarial Standards issued by the Institute of Company Secretaries of India.

The Registrar of Companies, based on the report submitted by the inspector, issued a show cause notice to the company. The company in a reply to show cause notice stated that the company and its directors / officers accept that there has been an inadvertent mistakes and these have been rectified subsequent to the issue of the show cause notice. The company stated that there was no deliberate intention and no *mens-rea* with read to the offences and therefore the company, its directors / officers deserve to be excused.

The Registrar of Companies / Adjudicating Officer came to the conclusion after going through the application and also based on the oral and written submission made by the company at the time of the personal hearing and imposed penalty on the company and its officers.

Good Documentation Do's and Don'ts

Do's	Don'ts
Do record the data/document as soon as it is generated	Don't delay in data/document recording
Do add the reference notes (if possible) to provide the context	Don't make the data confusing, vague and unreadable
Do validate your computerised system or document software	Don't encourage handwritten documentation

Good Documentation Do's and Don'ts	
Do's	Don'ts
Do limit document access to authorised personnel	Don't intentionally falsify the record/document
Do specify when the data/document was recorded, reviewed and approved	Don't pre-date or back-date the data/document
Do keep data back-up, either automatically or by storing the true copy in separate location	Don't archive data/documents unless explicitly authorised to do so

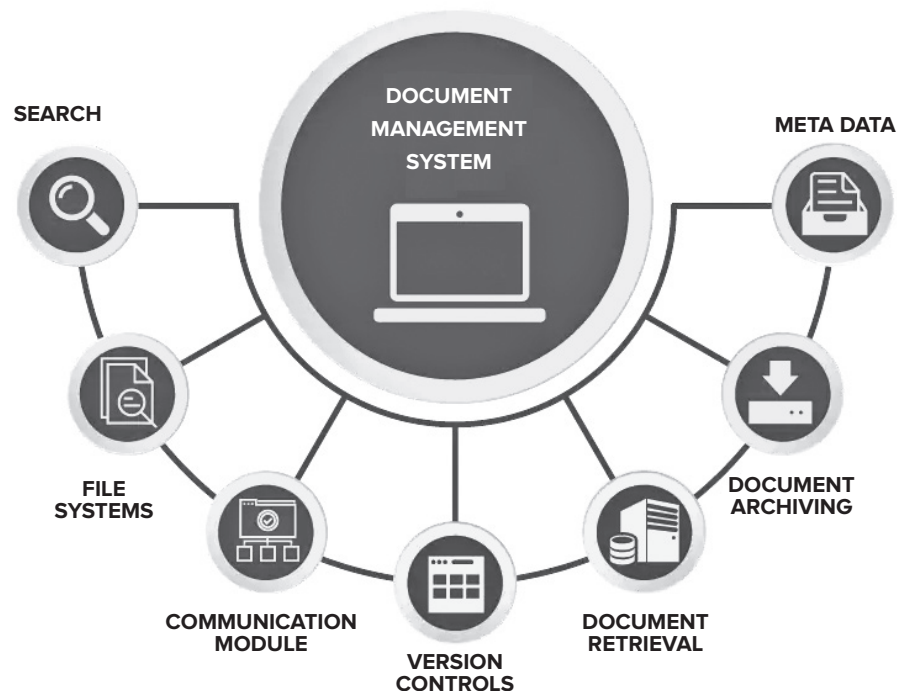
ELECTRONIC REPOSITORY OF DOCUMENTS

Document management refer the process of managing and tracking of the documents and records through an electronic or physical source of documents.

In an electronic repository, Document Management Systems (DMS) works by using a computer system and software to store, manage and track electronic documents and electronic images of paper based information captured through the use of a scanner.

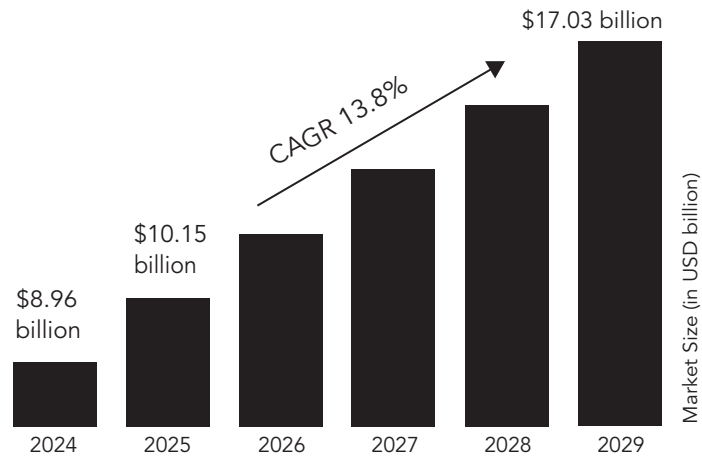
The term document management system can be defined as the software that controls and organizes documents of an organization. It incorporates document and content capture, workflow, document repositories and output systems, and information retrieval systems. Also, the processes used to track, store and control documents.

Now a days many business houses are adopting maintenance of records efficiently through document scanning, cloud document management and secure archive storage services. In Cloud Document Management – Digitised records can be uploaded, together with relevant data to secure cloud document management solution. This allows maintenance records to be accessed from any location using a web browser. The system provides a full electronic audit trail and restricts access to records by user, group or role, providing improved compliance. Documents can be tagged by any required data, which allows information to be found quickly and easily using a keyword search functionality.



The below statistics showcase volume of global document management system market size and its growth rate

Document Management System Global Market Report 2025



(Source: <https://www.thebusinessresearchcompany.com/report/document-management-system-global-market-report>)

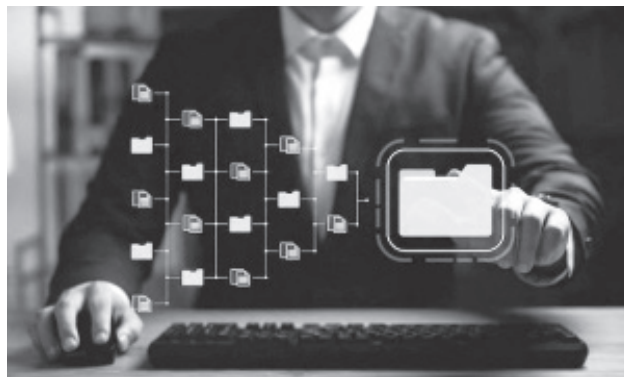
Document Management System Market Size 2025 and Growth Rate

The document management system market size has grown rapidly in recent years. It will grow from **\$8.96 billion in 2024 to \$10.15 billion in 2025 at a compound annual growth rate (CAGR) of 13.3%**. The growth in the historic period can be attributed to shift from paper-based to digital documentation, regulatory compliance and records management, corporate digitization initiatives, introduction of document imaging and scanning, emergence of enterprise content management (ECM) solutions.

Digitalization

Transitioning to a digital document management system is a fundamental step towards improving accessibility and operational efficiency. Key aspects of digitalization include:

- **Cloud-Based Solutions:** Leveraging cloud storage platforms provides secure, scalable, and easily accessible storage for documents. Cloud solutions enable remote access, facilitate collaboration, and offer robust backup and disaster recovery options. This shift reduces the need for physical storage and enhances document retrieval efficiency.



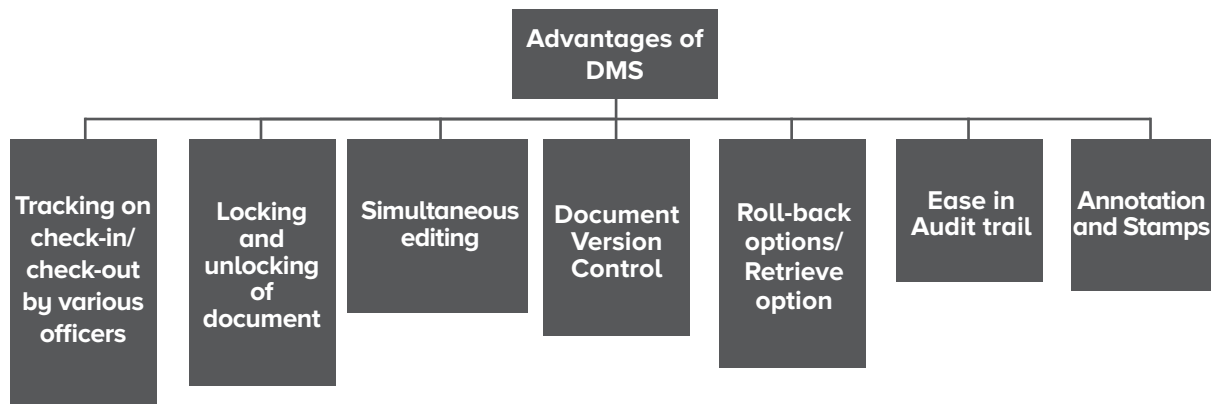
(Source: <https://www.icsi.edu/media/webmodules/CSJ/August-2024/ICSI-August-2024-CSJ.pdf>)

- **Electronic Document Management Systems (EDMS):** Implementing an EDMS can significantly streamline the creation, storage, and retrieval of documents. These systems often feature advanced document indexing, search capabilities, and integration with other business applications, which simplifies managing large volumes of documents.
- **Digitization of Existing Records:** Converting physical documents into digital formats is crucial for improving accessibility and reducing physical storage needs. Use high-quality scanners or imaging technologies and ensure thorough quality checks to maintain the accuracy and completeness of digitized records.

CASE STUDY

Health Care Provider Moves to Electronic Records

Top of minds for a North American Regional Health Care Provider (RHCP) had made the decision to move to electronic records. They wanted one organization (Electronic Record Keeping Service Provider) that could handle every aspect of implementing their electronic health record strategy, while simultaneously standardizing records management practices across the four major hospitals and numerous clinics they managed. Team of the Electronic Record Keeping Service Provider met with the senior management of RHCP and showcased the implementation plan for a new electronic health record strategy. The Electronic Record Keeping Service Provider recommended an automated, streamlined end tab labelling system that would standardize all files. The service provider completed the RHCP project in a tight timeline and with the integrity of every file intact, its ability to provide a “one stop” methodology for organizations moving to electronic records was proven successful. Approximately 500,000 records were converted during the project, an impressive feat.



Advantages of the Electronic Records

- **Cost Effective:** Storing and maintaining records in digital form is much cheaper than in any other format. With the increase in the technology advancement, the Digital media costs drop every day. Today, digital storage costs a 1000th of what it cost just a few decades ago, so the storage costs are continually dropping for electronic images.
- **Ease of use:** It's very easy to locate and share electronic documents through Computers aid searching now a days the process of filing doesn't exist anymore. The Document management system take care for finding and maintaining Records consistent locations.
- **Labor savings:** The labor required to locate, manage and dispose of electronic documents is almost nil and minimum. With electronic documents, all the steps like filing collating, stapling etc. can be automated and that labor completely disappears.

- **Search ability:** Electronic documents can be made searchable by doing OCR of a document and make the whole text keyword searchable. That is not possible with paper documents.
- **Portability:** It's very easy to transport electronic documents. No more boxes of records and trucks and semi-trucks to haul records archives. They can easily be stored on a removable hard drive or thumb drive and taken to the courthouse or to the field office.
- **Version tracking:** In case of the version tracking it is very easy with electronic documents, making it easy to see who has made changes to a document, when they made those and what the document looked like before the change. Version tracking and document management in the hard copy world is much more complex and much more costly.

Question: Which of the following is not an advantage of DMS?

Options: (A) Tracking on check-in/check-out by various officers

(B) Locking and unlocking of Document

(C) Simultaneous editing (D) Difficult Audit Trails

Answer: (D)

CASE LAW

A Case Regarding Admissibility of Electronic Evidence

In the matter of Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantayal and Ors. civil appl no. 20825-20826 of 2017, Civil Appeals were referred to a Bench of Judges of Supreme Court by a Division Bench, dealing with the interpretation of Section 65B of the Indian Evidence Act, 1872 by two judgments. It was found by the court that a Division Bench judgment in *Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801* may need reconsideration by a Supreme Court Bench of a larger strength. In the case of *Shafhi Mohammad (supra)*, it was observed by Supreme Court that it can be safely held that electronic evidence is admissible and provisions under Sections 65-A and 65-B of the Evidence Act are by way of a clarification and are procedural provisions. If the electronic evidence is authentic and relevant the same can certainly be admitted subject to the Court being satisfied about its authenticity and procedure for its admissibility may depend on fact situation such as whether the person producing such evidence is in a position to furnish certificate under Section 65-B(4).

The Supreme Court observed that the major premise of *Shafhi Mohammad (supra)* that the certificate under section 65-B(4) cannot be secured by persons who are not in possession of an electronic device is incorrect. An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B(4) in cases in which such person refuses to give it.

Disadvantage of Electronic records

- **Software risk:** Storing records in an electronic document management system, have a risk that the system being no longer supported by the software company; that the company will cease to exist; and that the documents will be locked in an unsupported system and have to pay conversion costs to recover them. So, the person is somewhat at risk to the software vendor that manages the records.
- **Format risk:** When storing the records in electronic format, a person run the risk of not being able to read them at some point. For example, some of the software are become the standard storage format now a days like PDF, JPEG, etc., but there is a risk that such software will cease to exist, be purchased or no longer support PDF format, and then it will be difficult in the future to read those PDF documents. Though such software provides to address this with their PDF or archive PDF format, which is supported by software code escrow and other measures that should make it forward and backwards compatible for years and years to come, but it is a risk.

- **Reliability:** Paper is an agnostic format. All person needs to have is a light source and some eyes to be able to read paper. It's a good idea to have most vital documents imaged, but keeping a paper copy assures that the person have access to them anytime. A person should keep a paper copy of vital documents - deeds, corporate documents-stored in a safe off-site location.
- **Portability:** The portability is an advantage for digital images. It's very easy to misplace or accidentally delete large amounts of data. It's very easy mode for data to duplicated and transported outside of any organization without permission or knowledge. It's very easy for it to be misplaced or corrupted as well. The very properties that make it easy to use, also make it easy to steal and easy to delete if the proper safeguards aren't in place but those safeguards are expensive.

MAINTENANCE AND INSPECTION OF DOCUMENTS IN ELECTRONIC FORM UNDER COMPANIES ACT, 2013

Section 120 of the Companies Act, 2013 (the Act) read with Rule 27 & 28 of the Companies (Management and Administration) Rule, 2014 provides for maintenance of documents in electronic form. The provisions also provide for inspection of documents maintained in electronic form. It states that any document, record, register, minutes, etc. that are required to be kept by a company or allowed to be inspected or copies to be given to any person by a company under the Act, may be kept or inspected or copies given, as the case may be, in electronic form. Rule 27 provides that every listed company or a company having not less than one thousand shareholders, debenture holders and other security holders, may maintain its records in electronic form.

Section 2(36) of the Companies Act, 2013, relates to the definition of "document" which includes summons, notice, requisition, order, declaration, form and register, whether issued, sent or kept in pursuance of Companies Act or under any other law for the time being in force or otherwise, maintained on paper or in electronic form.

Explanation to Rule 27 of the Companies (Management and Administration) Rules, 2014 states that the term "records" means any register, index, agreement, memorandum, minutes or any other document required by the Act or the Rules made thereunder to be kept by a company. Therefore, such documents and records can also be maintained in electronic form.

However, the records in electronic form shall be maintained in such manner as the Board of directors of the company may think fit, provided that -

- the records are maintained in the same formats and in accordance with all other requirements as provided in the Act or the rules made there under;
- the information as required under the provisions of the Act or the rules made there under should be adequately recorded for future reference;
- the records must be capable of being readable, retrievable and reproducible in printed form;
- the records are capable of being dated and signed digitally wherever it is required under the provisions of the Act or the rules made there under;
- the records, once dated and signed digitally, shall not be capable of being edited or altered;
- the records shall be capable of being updated, according to the provisions of the Act or the rules made there under, and the date of updating shall be capable of being recorded on every updating.

Security of Records Maintained in Electronic Form- Rule 28

- (1) The Managing Director, Company Secretary or any other director or officer of the company as the Board may decide shall be responsible for the maintenance and security of electronic records.

- (2) The person who is responsible for the maintenance and security of electronic records shall-
- (a) provide adequate protection against unauthorized access, alteration or tampering of records;
 - (b) ensure against loss of the records as a result of damage to, or failure of the media on which the records are maintained;
 - (c) ensure that the signatory of electronic records does not repudiate the signed record as not genuine;
 - (d) ensure that computer systems, software and hardware are adequately secured and validated to ensure their accuracy, reliability and consistent intended performance;
 - (e) ensure that the computer systems can discern invalid and altered records;
 - (f) ensure that records are accurate, accessible, and capable of being reproduced for reference later;
 - (g) ensure that the records are at all times capable of being retrieved to a readable and printable form;
 - (h) ensure that records are kept in a non-rewriteable and non-erasable format like pdf. version or some other version which cannot be altered or tampered;
 - (i) ensure that at least one backup, taken at a periodicity of not exceeding one day, are kept of the updated records kept in electronic form, every backup is authenticated and dated and such backups shall be securely kept at such places as may be decided by the Board;
 - (j) limit the access to the records to the managing director, company secretary or any other director or officer or persons performing work of the company as may be authorized by the Board in this behalf;
 - (k) ensure that any reproduction of non-electronic original records in electronic form is complete, authentic, true and legible when retrieved;
 - (l) arrange and index the records in a way that permits easy location, access and retrieval of any particular record; and
 - (m) take necessary steps to ensure security, integrity and confidentiality of records.

CASE LAW

In the matter of *M/s. Michelin India Pvt Ltd, the Registrar of Companies, Tamil Nadu on 18th October, 2022*, has passed an adjudication order by imposing of penalty for violation of provisions of section 134(3) (f) of the Companies Act, 2013. Pursuant to Section 134(3)(f) of the Companies Act, 2013, there shall be attached to statements laid before a company in general meeting, a report by its Board of Directors, Which shall include explanations or comments by the Board on every qualification, reservation or adverse remark or disclaimer made by the auditor in auditors report or by company secretary in his secretarial audit report.

The Regional Director, Southern Region Chennai has observed that while examining, that the statutory Auditor's in their audit report have reported deficiencies in the internal financial control and they were unable to obtain sufficient and appropriate audit evidence. It is clearly evident from the said statement that the company did not have proper internal financial control and also did not maintain appropriate records. Further, auditors report also mentioned non-maintenance of back up of books of accounts maintained in electronic mode in servers physically located in India. However, the Board of Director in their Boards report have not offered any explanation for the observations of auditors.

The Regional Director, Ministry of Corporate Affairs, had issued directions to take action against the company, every director and key managerial personnel of the company who is in default and to penalize the defaulter(s) *ibid* adjudication order.

CASE LAW

In *Re Anil Kumar Poddar V. Bonanza Industries Ltd. Co. application no. 20 of 2014 CLB Mumbai*, in this case the applicant filed application seeking to pass an order directing the respondent company to allow inspection of statutory register and record of the Respondent Company by stating that he had a statutory right to seek inspection of the documents in the capacity of he being a shareholder of the company and obtain copies thereof upon payment of the requisite charges.

The Respondent Company submitted that the applicant acquired had 10 shares only and started harassing the company and its management by frequently demanding the copies of statutory register required to be maintained under the Companies Act, minutes of the general meeting of the members of the company and the copies of the annual accounts and other documents.

The Court held that It appears that the applicant is in the habit of making such application. It is a matter of common knowledge that presently all the statutory records of any company are available on the MCA portal. It is open for inspection to all concerned. The certified copies can be obtained from the department of the ROC concerned. Yet, the Applicant keeps on filing such frivolous applications and it is, therefore, apparent that he is not a bona fide applicant. The application deserves to be dismissed.

PHYSICAL REPOSITORY

The term Physical repository refers to a central place where data is stored and maintained. A repository can be a place where multiple databases or files are located for distribution over a network, or a repository can be a location that is directly accessible to the user without having to travel across a network. The comparison between the virtual and Physical data room is illustrated as under:

VIRTUAL AND PHYSICAL DATA ROOM - A COMPARISON

Sl.No.	Particulars	Physical Data Room	Virtual Data Room
1	Form of documents	Papers, files, boxes or other tangible thing	Electronic/Digital/soft copies of documents including video/audio documents
2	Security of documents	Lies with the integrity of person who is in-charge of the data room	More secured through specific log-in id and pass word. In addition facilities like internet fire walls are there.
3	Time required for creation of data room	Longer time required	Can be created within 48 hours once demands of prospective bidders are identified
4	Cost	Cost is high because of reasons like- Requirement of one person to take care of data room. Requires bidders to travel from their place to the place of location of data room, etc.	Cost is Low as the documents can be viewed from any location with internet security
5	Convenience	Searching the documents is time consuming	More convenient as it enables multiple bidders to review documents at the same time with search facility also.

Sl.No.	Particulars	Physical Data Room	Virtual Data Room
6	Accessibility to data room	Timings to access data may be restricted	Data may be accessed nearly any time
7	Facility to restrict access of specific document	Difficult to implement any Restriction	Access can be restricted
8	Facility to check who has reviewed what documents and how many times	Available with high cost	Available with negotiable cost
9	Facility to highlight new information	To be conveyed manually to all bidders	A highlight can be made in the website created as data room
10	Ability to copy documents	Possible	Not possible always
11	One to one communication with the seller or his representatives	Available	Not available

CODING AND NOMENCLATURE

For naming of any documents adopting good file naming conventions can help ensure that files will work with different operating systems. Further, the file names can be either self-descriptive or non-descriptive.

The **Descriptive file** names are useful for small, well-defined projects with existing identification schemes that link the digital object to the source material. However, inconsistent application of terms or typos will increase to indexing and sorting errors.

Non-descriptive file names are usually system-generated sequential numerical string or the system based, such as a digital ID number, combination of Date and time, name of original file and are often linked to meta data stored elsewhere. Non-descriptive file names are often created for large scale digitization projects and may employ a digital ID number and numerical sequences to indicate batch or parent-child relationships. The advantage of non-descriptive names is that there is less chance of repeated or non-unique file names within a data structure.

Some applications and computer scripts could not recognize spaces or process files differently when using spaces. A best practice is to replace spaces in file names with an underline (_) or hyphen (-).

However, the punctuation, symbols, or special characters (periods, commas, parentheses, ampersands, asterisks, etc.) should be avoided. The following are best practices for file naming.

The File names should:

- Be unique and consistently structured;
- Be persistent and not tied to anything that changes over time or location;
- Limit the character length to no more than 25-35 characters;
- Use leading 0s to facilitate sorting in numerical order if following a numeric scheme “001, 002, 010, 011 ... 100, 101, etc.” instead of “1, 2, ...10, 11 ... 100, 101, etc.”;
- Contain a file format extension;
- Use a period followed by a file extension (for example, .tif, .jpg, .gif, .pdf, .wav, .mpg);
- Use lowercase letters. However, when a name has more than one word, start each word with an uppercase letter for example, “File_Name_Convention_001.doc”;

- Use numbers and/or letters but not characters such as symbols or spaces that could cause complications across operating platforms;
- Use hyphens or underscores instead of spaces;
- Use standard date notation (YYYY-MM-DD or YYYYMMDD);
- Avoid blank spaces anywhere within the character string; and
- Not use an overly complex or lengthy naming scheme that is susceptible to human error during manual input, such as “filenameconventionjoesfinalversioneditedfinal.doc”.

The strength of a folder and file naming convention is dependent on the proposed naming structure and the quality and quantity of the data elements chosen to build it. It should be of no surprise that for any business activity there is always an ideal naming structure. However, any structured naming convention that attempts to be all encompassing may result in overkill and unwieldiness.

The ten basic rules that could serve as a general guideline in structuring folder and file naming are:

S.No.	Particulars	Do's	Don'ts	Reason
1	Avoid extra-long folder names and complex hierarchical structures but use information-rich filenames instead.	D:\ABC\FY\16-17\ AR\ MGT-7.doc	D:/ Alfa Botanicals Private\Financial Year\2016-2017\ Annual Return\ Form MGT-7.doc	Complex hierarchical folder structures require extra browsing at time of storage and at the time of file retrieval. By having all the essential information concisely in the file name itself, both the search and identification of the file is streamlined and more precise.
2	Put sufficient elements in the structure for easy retrieval and identification but do not overdo it.	ABC_SearchReport_ Invoice 20.07.2018. pdf	ABC_Report_ Invoice. pdf	Precision targeted retrieval requires sufficient elements to avoid ambiguous search results but too much information adds undue effort at file naming time with little or no returns at retrieval time.
3	Use the underscore (_) as element delimiter. Do not use spaces or other characters such as: ! # \$ % & ' @ ^ ` ~ + , . ; =) (SMITH-J_AXA_7654-6_ POLICY_20120915. pdf FUJITSU_ S1500_ SPEC_ Scanner.pdf	SMITH-J AXA 7654-6 POLICY 20120915.pdf FUJITSU \$S1500\$ SPEC\$Scanner.pdf	The underscore (_) is a quasi standard for field delimiting and is the most visually ergonomic character. Some search tools do not work with spaces and should be especially avoided for internet files. Other characters may be interesting but visually confusing and awkward.
4	Use the hyphen (-) to delimit words within an element or capitalize the first letter of each word within an element.	Smith-John_AIG_7654-6_POLI- CY_2009-09-15. pdf WhitePaper_ Structured File Naming Strategy.doc	Smith John AIG 7654 6 POLICY 2009 09 15.pdf White Paper Structured file naming strategy.doc	Spaces are poor visual delimiters and some search tools do not work with spaces. The hyphen (-) is a common word delimiter. Alternatively, capitalizing the words within an element is an efficient method of differentiating words but is harder to read.

S.No.	Particulars	Do's	Don'ts	Reason
5	Elements should be ordered from general to specific detail of importance as much as possible.	FY2009_Acme-Corp_Q3_TrialBal_20091015_V02.xls Production_Paint-Shop_WorkOrder_775-2. xls	TrialBal_Q3_20091015_Acme-Corp_V02_FY2009.xls Paint-Shop_775-2_WorkOrder_Production.xls	In general the elements should be ordered logically, in the same sequence that you would normally search for a targeted file.
6	The order of importance rule holds true when elements include date and time stamps. Dates should be ordered: YEAR, MONTH, DAY. (e.g. YYYYMMDD, YYYYMMDD, YYYYMM). Time should be ordered: HOUR, MINUTES, SECONDS (HHMMSS).	RFQ375_Cables-Unlimited_BID_20091015-1655.pdf 2009-11-20_AMATProj_Phase1_Report.doc	RFQ375_Cables-Unlimited_BID_10152009-1655.pdf Nov-20-2009_AMATProj_Phase1_Report.doc	To ensure that files are sorted in proper chronological order the most significant date and time components should appear first followed with the least significant components.
7	Personal names within an element should have family name first followed by first names or initials.	Tate-Peter_SunLife_1-7566-2_POLICY_10YrTerm. pdf SmithJ_ID3567_ADMIN_WageReview.xls	Peter-Tate_SunLife_1-7566-2_POLI-CY_10 Year Term.pdf JSmith_ID3567_ADMIN_WageReview.xls	The family name is the standard reference for retrieving records. Having the family name first will ensure that files are sorted in proper alphabetical order.
8	Abbreviate the content of elements whenever possible.	RevQC_QST_2009-Q2.xls MCIM_27643_POD. doc	Minister of Revenue Quebec_Quebec-Sales-Tax_2009-2ndQuarter.xls MultiCIM-Technologies-Inc_27643_Proof-Of-Delivery.pdf	Abbreviating helps create concise file names that are easier to read and recognize.

S.No.	Particulars	Do's	Don'ts	Reason
9	An element for version control should start with V followed by at least 2 digits and should be placed as the last most element. To distinguish between working drafts (i.e. minor revisions) use Vx-01->Vx-99 range and for final draft (i.e. major version release) use V1-00-> V9-xx. (where x =0-9)	MCIM_Proposal_V09.doc eXadox_UserManual_V1-02.doc	MCIM_Proposal_9.doc eXadox_UserManual_V2FinalDraft.doc	The "V" helps denote that the element pertains to a version number. A minimum of 2 digits with a leading zero is required to ensure that search results are properly sorted. The intent is to avoid the situation where for example, a filename with a "V1-13" will wrongly appear before an identical filename with a "V1-2" version number when sorted in ascending alphabetical/numerical order. To distinguish between working, review and final draft a single digit prefix followed by hyphen "-" is preferred to facilitate proper sorting; using words in the file name such Final, Draft or Review in the filename affect the order and should be avoided.
10	Prefix the names of the pertinent sub-folders to the file name of files that are being shared via email or portable storage devices.	Prod_PS_AssL7_W O _ Suzuki _ J3688-20090725.xls FY2009_Acme-Corp _Q3_TrialBal_20091015_V02.xls	WO_Suzuki_J3688-20090725.xls Q3_TrialBal_20091015_V02.xls	Attached files and files shared through portable devices include only the file name and can be totally devoid of the context that is generally provided by the folder structure of origin. To compensate and avoid confusion it is sometimes essential to prefix the name of the subfolder(s) to such file names.

CIRCULATION OF DOCUMENTS

In a company efforts shall be established to control the issuance of documents, such as instructions, procedures, and drawings, including changes thereto, which prescribe all activities affecting quality of the document & record. These measures shall assure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel and are distributed to and used at the location where the prescribed activity is performed. Changes to documents shall be reviewed and approved by the same authority that performed the original review and approval unless the organization designates another responsible Authority.

SAFETY AND RETRIEVAL OF RECORDS

To assure the best quality of documents, it is to be assured that sufficient records are maintained to furnish evidence of the activities affecting quality. The records should incorporate the following:

- **Operating logs:** the names of the individuals who all have worked on the same documents;

- **Results of reviews:** the recording of the changes suggested by each reviewer and basis of the rejection on Non agreement;
- **Inspections:** list of individuals who have access of the records and have inspection rights of the same;
- **Monitoring of work performance:** will ease in the monitoring of work performed by the person to whom the file is shared;
- **Information analyses:** Provide ease in the Information system of the organization and tracking of files.

Records should be identifiable and retrievable and should consistent with applicable regulatory requirements. The company should comply with requirements concerning record retention, such as duration, location, and assigned responsibility. Every record must be well managed in order to ensure that they are protected for both administrative purposes and to serve as evidence of the organization's work. Records management provides a professional approach to caring for records. The care of records and archives is governed by three key concepts.

(i) Keeping together

The records must be kept together according to the department / Section responsible for their creation or accumulation, in the original order established at the time of their creation. This gives them their 'evidential' nature and distinguishes them from other kinds of information. It is the basis for retrieving information from records. Knowing who created or used a record, and where, when and why, is the key to retrieval rather than their format, subject matter or content. This is true for paper-based records as well as the electronic records.

(ii) Ensure life cycle

Every records follow a 'life-cycle', in that they are created, used for so long as they have continuing value and then disposed of by destruction or by transfer to an archival institution. Every record pass through three main phases, i.e. current phase, semi-current phase and non-current phase.

In the **current phase**, they are used regularly in the conduct of current business and maintained in their place of origin or in the file store of an associated records office or registry.

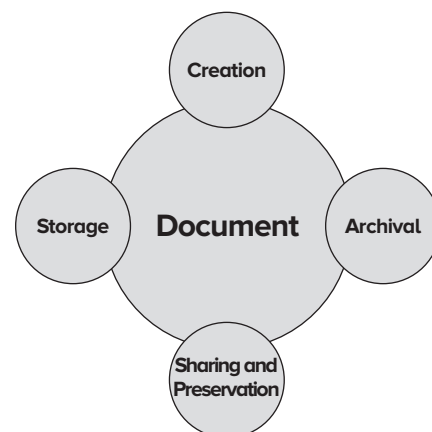
In the **semi-current phase**, they are used infrequently in the conduct of current business and are maintained in a records center.

In the **non-current phase** they are destroyed unless they have a continuing value which merits their preservation as archives in an archival institution. The effective management of records throughout this life-cycle is a key issue in civil service reform.

(iii) Record Preservation

The care of records and archives is that the care should be managed through a coherent and consistent range of actions from the development of record-keeping systems, through the creation and preservation of records to their use as archives.

The concept suggests that four actions continue or reappear throughout the life of a record: i.e., identification of records; intellectual control; provision of access; and physical control. The management of this continuum basis for a strategic approach to records management.



CASE STUDY

U.S. Food & Drug Administration (FDA) has issued series of warning letters to pharmaceutical companies for Good Manufacturing Practices (GMP) violations particularly for data integrity. The different companies who fail to ensure the data integrity are as under:

Ranbaxy Laboratories, a multinational pharmaceutical company has received a warning letter by US FDA for its two facilities that are Dewas and Poanta Sahib facility. In Dewas facility, the company failed to maintain batch production and control records. And in Poanta Sahib facility, incomplete batch and production records were followed for the review and approval of production and control records for drug products.

Canton Laboratories, a manufacturer of chemical and bulk drugs has received a warning letter by US FDA for its Vadodara plant for reporting results for the tests that were never performed. Significant Good Manufacturing Practices (GMP) violations related to record maintenance were observed in the industry. The company was accused for serious documentation practices and reported missing data.

Wockhardt Limited, a Mumbai based pharmaceutical company received a warning letter by US FDA for Aurangabad plants for data integrity issues. The company failed to exercise appropriate controls over computer or related systems to assure that only authorised personnel institute changes in master production and control records or other records.

Source: <https://www.igmpiindia.org/DocumentationandMaintenance.pdf>

PRESERVATION OF RECORDS

Preservation of records refers to the implementation of strategies that enhance and prolong the useable life of records and archives. Preservation encompasses storage and handling. Responsibility for the preservation of records is vested in the creating office during the active and semi-active phases of the records life-cycle. The other offices are charged with ensuring accessibility in the short and medium terms. However, where it is evident that records will be required as archives, and to assist the organization in long-term preservation, standards in the storage and handling of records should refer to the long term rather than short or medium terms. The provisions of Regulation 9 and 30(8) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 state the provisions of preservations of records as under:

Preservation of Documents

Regulation 9 provides that the listed entity shall have a policy for preservation of documents, approved by its board of directors, classifying them in at least two categories as follows-

- (a) documents whose preservation shall be permanent in nature ;
- (b) documents with preservation period of not less than eight years after completion of the relevant transactions:

Provided that the listed entity may keep documents specified in clauses (a) and (b) in electronic mode.

Regulation 30(8) provides that the listed entity shall disclose on its website all such events or information which has been disclosed to stock exchange(s) under-regulation 30(Disclosure of events or information by listed entities), and such disclosures shall be hosted on the website of the listed entity for a minimum period of five years and thereafter as per the archival policy of the listed entity, as disclosed on its website.

Accordingly, the companies are required to prepare a policy statement relating to the preservation of its documents and archival of documents in the website. The following factors need to be considered in the preparation of the preservation and archival policy of the company.

- Analysis and Restructuring Existing Systems
 - reviewing and revising legislation and policies
 - reviewing and revising organizational policies and structures
 - determining resource requirements, such as facilities and staffing
 - developing strategic and business plans.
- Organizing and Controlling Records
 - building sound record-keeping systems
 - managing the creation, maintenance, and use of files.
- Providing Physical Protection for Records
 - implementing and maintaining preservation measures
 - developing emergency plans to protect records
 - identifying and protecting vital records.
- Managing Records in Records Centers
 - developing and maintaining records center facilities
 - transferring, storing and retrieving records according to disposal schedules
 - disposing of records as indicated by the schedules.
- Managing Archives
 - acquiring and receiving archives
 - arranging and describing archives according to archival principles
 - providing public access to the archives.
- Supporting and Sustaining the Program
 - promoting records services to the government and the public
 - promoting education for records and archives personnel
 - developing and expanding the records and archives professions.

Question : Which of the following regulation of SEBI (LODR) Regulations, 2015 provides for disclosures to be hosted on the website of the listed entity for a minimum period of five years and thereafter as per the archival policy of the listed entity, as disclosed on its website.

Options: (A) Regulation 9(8) (B) Regulation 30(8)
(C) Regulation 19 (D) Regulation 91

Answer: (B)

Preservation of Litigation Documents

Documents arising out of various litigation wherein a company is a party in any manner, shall need to be preserved as per the directions/orders of the court(s)/tribunal(s)/judicial/other authority(ies) as may be applicable, in absence of which the documents shall be preserved for a period of not less than eight consecutive calendar years after conclusion of the litigation.

Deviation from the Policy

Any court(s)/tribunal(s)/judicial/other authority(ies) shall have the power to direct a company to produce / preserve and/or destroy any document(s), however, if any document(s) has/have been destroyed pursuant to the Policy followed as per the SEBI Regulations, herein, it may not be possible for the company to produce such document(s), therefore, necessary permission to that effect has to be taken by the company and/or a statement to that effect shall be given by the company from/to the relevant authorities. Any other action(s) shall need to be taken as may be advised by these authorities.

Model Policy

The model policy on preservation of Documents and archival of documents is as under:

POLICY ON PRESERVATION OF DOCUMENTS AND ARCHIVAL OF DOCUMENTS IN THE WEBSITE

[Under Regulation 9 and 30(8) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015]

1. Purpose and Scope

The purpose of this document is to present a policy statement for (Company) regarding preservation of its documents and archival of documents on the website in accordance with the provisions of the Companies Act, 2013 and Regulation 9 and 30(8) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("LODR").

The policy is framed for the purpose of systematic identification, categorization, maintenance, review, retention and destruction of documents received or created in the course of business. The policy gives guidelines on how to identify documents that need to be maintained, how long certain documents should be retained, how and when those documents should be disposed of, if no longer needed and how the documents should be accessed and retrieved when they are needed.

2. Classification of Documents to be Preserved / Retained

The Company's physical and electronic documents shall be classified for the purpose of preservation as follows:

- A. Documents whose preservation shall be permanent in nature;
- B. Documents whose preservation period shall not be less than eight years after completion of the relevant transactions;
- C. Documents whose preservation shall be for a minimum period of three years after completion of the event.

The details of documents for the above three categories are given in the Annexure.

3. Principle of Responsibility of Employees for Preservation of Documents

All the Employees in the permanent rolls of the Company are responsible for taking into account the potential impacts on preservation of the documents in their work area and their decision to retain/ preserve or destroy documents pertaining to their area.

4. Periodical Review of the Policy

The Chief Executive Officer/ Managing Director/ Whole-time Director of the Company is authorised to periodically review the policy and make such changes as considered necessary.

5. Suspension of Record Disposal in the Event of Litigation or Claims

In case the Company is served with any notice for request of documents or any employee becomes aware of a governmental investigation or audit concerning the Company or commencement of any litigation against the Company, any further disposal of documents connected with the matter shall be suspended until such time the investigation / litigation ends.

6. Statutory Requirements

If as per any other law of land including Information Technology Act, a physical or electronic record should be preserved for a longer period than what has been stipulated in this policy, then the document shall be preserved as per the applicable statutory stipulations.

7. Web Archival Policy

The Company shall disclose on its website all events or information which has been disclosed to stock exchange(s). <<Not required>> We should be specific.

Such disclosures shall be retained on the website of the Company for a minimum period of five years.

Place:.....

Date:.....

ANNEXURE**A. Documents whose preservation shall be permanent in nature:**

1. Property records including purchase and sale deeds, licences, copyrights, patents & trademarks;
2. Corporate Records including Certificate of Incorporation, Common Seal, Minutes of Board, Committee and Shareholders' Meetings, Register of Members and other Statutory Records;
3. Personal files of all live employees;
4. Any other record as may be decided by the Chief Executive Officer/ Managing Director/ Whole-time Director of the Company from time to time.

B. Documents whose preservation period shall not be less than eight years after completion of the relevant transactions:

1. Books of Account, Bank Statements and vouchers;
2. Filings with Stock Exchanges, Registrar of Companies and other statutory authorities;
3. Payroll Records, Employee deduction authorisations, attendance records, employee medical records, leave records, Pension and retiral related Records, etc.
4. Corporate Social Responsibility Records;
5. Sponsorship Projects Records;
6. Correspondence and Internal Memoranda;
7. Any other record as may be decided by the Chief Executive Officer of the Company from time to time.

C. Documents whose preservation shall be for a minimum period of three years after completion of the event:

1. Tender Documents;
2. Lease Deeds and Contracts
3. Legal files;
4. Insurance Records including policies and claims;
5. All e-mail correspondence, internal & external <<Where it is coming from>>
6. Documents under Secretarial Standards:

Proof of sending Notice of the meetings of the Board / Committee and General meetings and its delivery. Proof of sending Agenda and Notes on Agenda and their delivery.

Proof of sending and delivery of the draft of the Resolution.

Proof of sending draft Minutes of the Board / Committee and its delivery. Proof of sending signed Minutes of the Board / Committee and its delivery.

7. Any other record as may be decided by the Chief Executive Officer/ Managing Director/ Whole-time Director of the Company from time to time.

SETTING UP OF A RECORD ROOM

The Records room must be located at convenient location to the accesses of the record. The record room should be kept separate from other administrative units and should be large enough to house the relevant files. The accommodation must be secure and well maintained, and it must be of strong construction so that it can bear the weight of the records.

Sometimes the Due to the absence of the proper record room, the documents were stored for years in a basement or in an attic which are the worst places to preserve them. The best conditions for conservation of Physical Records are a neat environment, free of dust, with controlled light, humidity and temperature. The following factors should be considered while setting up the Data Room:

Humidity: It's a very important factor. An excess of humidity creates fungus and produces a proliferation of corrosive insects. The lack of humidity, on the other hand, produces brittle and fragile sheets of paper. A controlled humidity between 30% and 40% is the best standard for preservation. With the less possible variation, and the maximum of stability, because variations of humidity provoke more damages than a stable low or medium range.

Temperature: The lower is the temperature, the better is for preservation of Records. However, it is suggested to maintain normal temperature in the record room, which is required for comfortable standard for human beings in public places.

Light: Light has a considerable impact on document's preservation. Not only the visible light to the human eye, but the infrared or ultraviolet radiation, could cause damages. At the environments exposed to the daylight, should be installed curtains with UV filters. Documents exposed to more luminance, should be stored in dark places until its public exposition.

Fire extinguisher, particular paint to be used in the room, security checks etc. need to be mentioned here.

The Public Records Act, 1993: An Act to regulate the management, administration and preservation of public records of the Central Government, Union territory Administrations, public sector undertakings, statutory bodies and corporations, commissions and committees constituted by the Central Government or a Union territory Administration and matters connected therewith or incidental thereto.

PRIVACY OF RECORD AND ITS CONTROL

The most official communication now a days done electronically and most corporate documents are kept in digital form yet there are plenty of physical data which cannot be circulated electronically and are need to be circulated around various branches and other offices in the form of documents, thumb drives, hard disks or log books. Such physical data needs to be protected and handled responsibly; especially if the data contains personal or confidential information. Just like companies have protocols, firewalls, passwords and other security measures to protect their digital data, they need to put in place the right processes and procedures to ensure their data is secure.

For the managing the confidential and privacy, the first step in the process is to identify what constitutes confidential documents at the workplace, and what to share securely. For any business house the following documents are primarily considered as confidential and need complete privacy:

(i) Customer's & Employees' Information

Safe guarding of the personal data is information about an individual that can be used to identify him/her. Information like Aadhar number, Mobile numbers, Residential addresses, Name, credit card numbers, etc. can all be considered personal information.

In India, by the majority of the business, the strong mechanism for safe guarding the personal information is not yet adopted. Even when the documents or data cease to be useful to the organisation, this doesn't mean that the information is no longer confidential. In such cases the data needs to be disposed of securely and cannot be placed freely on the public platform or mixed with other kinds of data in the office. In such cases the business should work with a trusted information destruction agency to physically destroy both electronic and physical data.

The Customer's & Employees Confidential Information includes discussions about employee relations issues, disciplinary actions, impending layoffs/reductions-in-force, terminations, workplace investigations of employee misconduct, etc.

(ii) Office Plans, Office IDs and Internal Procedure Manuals

For every organisation internal planning & procedures is the key aspect for controlling business and the organisation should ensure the protection of the same. It is important to place the documents with detailed office layouts throughout offices to identify key exits in case of emergency but the other documents and forms related to internal processes and procedures should be kept electronically on secure network drives and encourage employees to limit print-outs.

(iii) Contracts and Commercial Documents and Trade Secretes

In case of the business contracts, every detail of the arrangement should be treated with the utmost confidentiality for both organization itself and the third party's benefit. If the contract has a confidentiality agreement, it could be rendered obsolete if an unauthorised person got their hands on the physical copy of the contract. The contracts are full of commercially sensitive information such as the nature of the arrangement, the value of the services offered/received in the agreement, the names of the main contracting parties, etc.

The business should avoid sharing contracts broadly unless strictly required, and limit physical copies; consider using tools to sign contracts electronically in order to reduce unnecessary print-outs. While these documents are some of the most important to securely store and shared, the easiest and safest way to reduce the risk of a data breach is to implement a secure document retention policy specific to organisation's needs.

The confidential business information as "proprietary information" or "trade secrets." Which is not generally known to the public and would not ordinarily be available to competitors except via illegal or improper means. Common examples of "trade secrets" include manufacturing processes and methods, business plans, financial data, budgets and forecasts, computer programs and data compilation, client/customer lists, ingredient formulas and recipes, membership or employee lists, supplier lists, etc. "Trade secrets" does not include information that a company voluntarily gives to potential customers, posts on its website, or otherwise freely provides to others outside of the company. If such Confidential information is available in the wrong hands, confidential information can be misused to commit illegal activity (e.g., fraud or discrimination), which can in turn result in costly lawsuits for the Company. The disclosure of sensitive employee and management information can lead to a loss of employee trust, confidence and loyalty. This will almost always result in a loss of productivity.

SUGGESTIVE STEPS FOR PROTECTING CONFIDENTIAL INFORMATION

For every business/organization it is important to have a written confidentiality describing both the type of information considered confidential and the procedures employees must follow for protecting confidential information and dealing with the confidential information's. However, the company may adopt the following procedures for protecting confidential information:

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who are authorized.
- All electronic confidential information should be protected via firewalls, encryption and passwords.

- Employees should clear their desks of any confidential information before going home at the end of the day.
- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their work stations.
- All confidential information, whether contained on written documents or electronically, should be marked as “confidential.”
- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)
- Employees should refrain from discussing confidential information in public places.
- Employees should avoid using e-mail to transmit certain sensitive or controversial information.
- Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver’s license numbers) unless it is integral to the business transaction and restrict access on a “need-to-know’ basis.
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

LESSON ROUND-UP

- The good documentation promotes good corporate governance practices and compliance level of the company and also improves communication and dissemination of information between and across various stakeholders.
- The General principles for documentation provide that the document should Clear, Concise, Complete, Contemporary, Consecutive, Correct, Comprehensive, Collaborative, Client Centric and should maintain Confidentiality.
- Section 120 of the Companies Act, 2013 read with Rule 27 & 28 of the Companies (Management and Administration) Rule, 2014 provides for maintenance of documents in electronic form.
- Document management refer the process of managing and tracking of the documents and records through an electronic or physical source of documents.
- Disadvantages of the electronic records are software risk, format risk, chances of misplacing or accidentally deletion of large amounts of data.
- Responsibility for the preservation of records is vested with the creator of the document during the active and semi-active phases of the records life-cycle.
- For any business house the following documents are primarily considered as confidential and need complete privacy i.e. Customer’s & Employees’ Information; Office Plans, Office IDs and Internal Procedure Manuals; Contracts and Commercial Documents and Trade Secretes.
- The confidential policy should describe the type of information considered confidential and the procedures employees must follow for protecting confidential information and dealing with the confidential information’s.

GLOSSARY

Document Management System : The process of managing and tracking of the documents and records through an electronic or physical source of documents.

Version tracking : It is a way of finding out who has made the changes.

Format risk : When storing the records in electronic format, a person has the risk of not being able to read them at some point due to the format.

Media compatibility : When a document saved in a hard drive is compatible with the available technologies.

Physical repository : Physical repository is a central place where data is stored and maintained.

Descriptive file names : Small, well-defined projects with existing identification schemes that link the digital object to the source material.

Non-descriptive file names : System-generated sequential numerical string or the system based, such as a digital ID number, combination of Date and time, name of original file and are often linked to meta data stored elsewhere.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. Before drafting any document, it is the most essential to familiar with the purpose of document. Comment?
2. Briefly explain the advantage and disadvantage of the electronic records.
3. In naming of a document, briefly explain the concept of Descriptive file and Non-Descriptive file.
4. To assure the best quality of documents, the records should maintained of the activities affecting quality of the records. Comment.
5. Media compatibility is one of the biggest challenge in saving the documents electronically. Comment.
6. Briefly explain the provisions relating to maintenance of documents in electronic form under Companies Act, 2013 and rules made thereunder.
7. Draft a policy on preservation of Documents and archival of Documents in the website under SEBI (LODR) Regulations, 2015
8. What does the term documentation connote ? Name the 10'Cs which form the guiding principles of good documentation.
9. Records Management provides a professional approach to caring for the records and archives which is governed by certain key concepts. Explain the concepts that govern the care of records and archives.
10. The Board of directors of ABC Ltd. was of the view that as the company was diversifying its operations, it should evaluate digitizing the books of accounts and other records. The Board sought views from the Company Secretary about the same and asked him to appraise them about the Document Management System including good documentation practices. Advise the Board as the Company Secretary.

LIST OF FURTHER READINGS

- The Companies Act, 2013 and Rules made thereunder;
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015
- The Public Records Act, 1993
- ICSI Chartered Secretary

