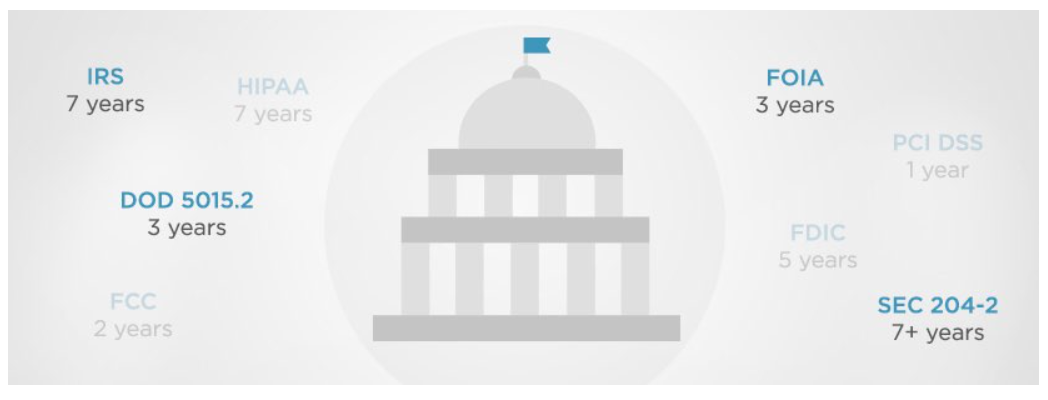
5/19/2022

Data Retention Timelines

Consolidation from various sources & standards

POLICY ON DOCUMENT RETENTION



|  |  |
| --- | --- |
| **Document Details** | |
| Document No | Doc\_Ref 01 |
|  |  |
| Revision number: | 1.0 |
|  |  |
| Release date: | 20-May-2022 |
|  |  |
| MS Word file name: | Data Retention Timelines |
|  |  |
| Document prepared by: | SriKrishna Panchadhara |

|  |  |  |
| --- | --- | --- |
| **Revision History** | | |
| **Revision number** | **Release date** | **Brief description or notes** |
|  |  |  |
| 1.0 | 20-May-2022 | Consolidate Data Retention Timelines from various standards or Industry Best Practices |
|  |  |  |

Contents

[1) https://www.esabindia.com/in/en/investors/policies/policy\_on\_document\_retention\_2015.cfm 4](#_Toc103898978)

[2) https://www.legalserviceindia.com/article/l428-Data-Retention-Policies.html 21](#_Toc103898979)

[3) https://www.intradyn.com/email-retention-laws/ 25](#_Toc103898980)

[4) Database Backup Retention Policy 28](#_Toc103898981)

[5) https://www.tetratecheurope.com/wp-content/uploads/2021/05/Tetra\_Tech\_Data\_Retention\_Policy.pdf 31](#_Toc103898982)

[*6)* *Disclaimer:* 39](#_Toc103898983)

# https://www.esabindia.com/in/en/investors/policies/policy\_on\_document\_retention\_2015.cfm

Policy on Preservation of Documents and archival of documents in its website

1.Purpose and Scope

The purpose of this documents to present a high level policy statement for ESAB India Limited (ESAB) regarding preservation of its documents in accordance with the provisions of the Companies Act, 2013 and in accordance with the provisions of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("LODR")

The policy is intended to define ESAB's preservation of documents responsibilities and to provide guidance to the executives and staff working in ESAB in making decisions and undertaking other activities that may have an impact on the operations of the Company. It also frame the guidelines for fundamental accountability of ESAB to retain and preserve its documents as the basis for communication with a range of external stakeholders

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 would contain 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

This policy has been adopted and approved by the Board of Directors at its meeting held on 5 November, 2015

2.Statutory Mandate

The policy on preservation of documents and archival is mandated by the provisions of regulation 9 of Chapter III of LODR, 2015. Under this regulation, the Company has a strategic objective of ensuring that significant documents are safeguarded and preserved to ensure its longevity of priority documents including its electronic resources

3.Classification of Documents to be preserved / retained

Based on the recommendation of the management of the Company, the Board of Directors have classified the following documents to be retained and preserved for posterity

Documents that need to be preserved / retained permanently - Doc 1

Documents that may be preserved / retained for a period of 8 years as specified under the Companies Act, 2013 or LODR - Doc 2

Documents to be preserved electronically and archived when necessary - Doc 3

Documents that may be required by judicial proceedings and which may be destroyed after closure of the legal case - Doc 4

Emails of all employees in the grade M3 (E6) and above for a period of 3 years - Doc 5

Documents like budget papers, bank guarantees etc., which may be retained for less than 8 years - Doc 6

4.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. Such policy bestowing responsibility on the Company's employees would immensely help company's litigation preparedness tool helping the Company's and Outside legal counsel to track down documents to handle the legal cases

5.Periodical Review of the Policy by Top Management

The Policy should be flexible and easy to understand and comply with by all levels of employees. The policy should be reviewed periodically by the Top Management and amendments effected to subject to approval of the Board if and when practical difficulties are encountered. The Top management may also review the policy on document retention to comply with any local, state, central legislations that may be promulgated from time to time

6.Administration

The Record Retention Schedule approved by the Board of Directors for initial maintenance, retention and disposal schedule for physical records is as given in the annexure

7.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 ESAB India or commencement of any litigation against the Company, such employee shall inform the Top Management and any further disposal of documents shall be suspended until such time as the Top Management with the due advice from the legal counsel determine otherwise. The Top Management in such case shall inform all the employee by mail under "Userlist" of the need to retain the documents and suspension of disposal of the same

8.Disaster Preparedness

ESAB India maintains a business continuity plan (BCP) designed to ensure safety of staff as well as members of the general public, safeguard the documents and records and to enable a return to normal operating with minimal disruption. Detailed procedures for responding to an incident are part of the BCP

In the event of major incident, the first priority is the safety of the people, followed by immediate action to rescue or prevent further damage to the records. Depending on the immediate threat, emergency response and recovery actions will take precedence over all other Company activities

The Company has made appropriate provision for the backup of its digital collections, including the provision of offsite security copies. The backup copies are actively maintained to ensure their continued viability. The Company's BCP ensures that the digital collections and technical infrastructure required to manage and access them can be restored in the event of an emergency

9.Board's Approval

This policy was approved by the Board of Directors at its meeting.

Type of Record

Accounting and Finance records including Annual Financial statement

Insurance Records

Tax records

Contracts entered into by the Company including Marketing Contracts

Corporate Records including Certificate of Incorporation, Listing Agreement and other approvals from other statutory authorities

Legal Files and Records

Property Records

Payroll Records

Pension and retiral related Records

Personnel and HR Records

Programs & Service Records

Sponsorship Projects Records

Corporate Social Responsibility Records

Correspondence and Internal Memoranda

Electronic Documents including email retention and back up

Miscellaneous Records

1. Accounting and Finance records including Annual Financial statement

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Accounts Payable ledgers and schedules | 8 Years | Doc -2 |
| Accounts Receivable ledgers and schedules | 8 Years | Doc - 2 |
| Annual Audit Reports and Financial Statements, Tax and Vat Audit | Permanent | Doc - 1 |
| Annual Audit Records, including work papers and other documents that related to the audit | 8 years after completion of audit | Doc - 2 |
| Annual Plans and Budgets | 3 years after the budget year is closed | Doc - 6 |
| Bank Statement and Cancelled Cheques | 8 years | Doc - 2 |
| Employee Expense Reports | 8 years | Doc - 2 |
| General Ledger | Permanent | Doc - 1 |
| Interim Financial Statements | 8 years | Doc - 2 |
| Notes Receivable ledgers and schedules | 8 years | Doc - 2 |
| Investment Records | Permanent | Doc - 1 |
| Security deposit receipt copies | 3 years after termination of the contract | Doc - 6 |
| Fixed Asset Register with supporting Purchase Orders and Bills for fixed assets addition | Permanent | Doc - 1 |
| Cost records | 8 years | Doc - 2 |
| Payroll extract, salary advice and payroll JVs | 8 years | Doc - 2 |
| Payroll TDS, PF, ESI return and challan applicable on payroll | Permanent | Doc - 1 |
| Treasury documents - Credit approvals from bank | Permanent | Doc - 1 |
| Bank Account passbook or statement, Bank Reconciliation Statement and LC Documents | 8 years | Doc - 2 |
| Bank Guarantees | Till the expiry of the claim period | Doc - 6 |
| Tax Litigation documents | Permanent | Doc - 1 |
| Bill of entries | Permanent | Doc - 1 |

2. Insurance Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Annual Loss Summaries | 8 Years | Doc -2 |
| Audits and Adjustments | 8 Years | Doc - 2 |
| Claim Files (Including correspondence, medical records, injury documentation, etc. | Permanent | Doc - 1 |
| Group Insurance Plans - Active Employees | 8 years | Doc - 2 |
| Group Insurance Plans - Retireees | Permanent | Doc - 1 |
| Insurance Policies for the Company | Permanent | Doc - 1 |
| Journal Entry Support Data | 8 years | Doc - 2 |
| Releases and Settlements | Permanent | Doc - 1 |

3. Tax records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Tax-Exemption Documents and related correspondence | Permanent | Doc -1 |
| Excise Tax records | Permanent | Doc - 1 |
| Payroll Tax records | 8 years | Doc - 2 |
| Tax Bills, Receipts, Statements | 8 years | Doc - 2 |
| Tax Returns - Income, Franchise, Property | Permanent | Doc - 1 |
| Tax workpaper packages - Originals | 8 years | Doc - 2 |
| Sales Tax Records | 8 years | Doc - 2 |
| Annual Information Returns - State and Central | Permanent | Doc - 1 |
| Service Tax Records | 8 years | Doc - 1 |

Responsibility : FINANCE AND ACCOUNTS DEPARTMENT

4. Contracts entered into by the Company including Marketing Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documents | 8 years | Doc - 2 |

Responsibility : LEGAL AND MARKETING DEPARTMENT

5. Corporate Records including Certificate of Incorporation, Listing Agreement and other approvals from other statutory authorities.

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Corporate Records (certificate of incorporation, commencement of business, listing agreement, common seal, minutes book of board and committees thereof, annual reports originals, etc.) | Permanent | Doc - 1 |
| Licence and Permits, Industrial entrepreneurial Memorandum, and other statutory approvals | Permanent | Doc - 1 |
| ROC Filings and Stock Exchange filings in physical and Electronic form | 5 years from the date of filing | Doc - 6 |

Responsibility : LEGAL AND SECRETARIAL DEPARTMENT

6. Legal Files and Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Legal Memoranda and Opinions | 3 years after the closure of the matter | Doc - 4 |
| Litigation files | 1 year after expiration of disposal of the case | Doc - 4 |
| Court Orders | Permanent | Doc - 1 |

Responsibility : LEGAL AND SECRETARIAL DEPARTMENT

7. Property Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Correspondence, Property Deeds, Assessments, Licenses, Rights of Way | Permanent | Doc - 1 |
| Original Purchase / Sale Deeds | Permanent | Doc - 1 |
| Original Lease Agreements | 3 years after expiration of the lease | Doc - 6 |

Responsibility : LEGAL AND SECRETARIAL DEPARTMENT

8. Payroll Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Employee Deduction Authorization | 3 years after termination of service of employment | Doc - 6 |
| Payroll Deductions | 3 years after termination of service of employment | Doc - 6 |
| Labour Distribution Cost Records including details regarding gratuity and retiral disbursements | 3 years after termination of service of employment | Doc - 6 |
| Payroll Registers (Gross and Net) | 3 years after termination of service of employment | Doc - 6 |
| Time Cards / Sheets | 2 years | Doc - 6 |
| Unclaimed Wage Records | 3 years | Doc - 6 |
| Leave Records | 2 years after the relevant period | Doc - 6 |

Responsibility : HUMAN RESOURCES DEPARTMENT

9. Pension and retiral related Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Retirement and Pension Records | Permanent | Doc - 1 |

Responsibility : HUMAN RESOURCES DEPARTMENT

10. Personnel and HR Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type of transaction |
| Personnel Files of individual employees | Permanent | Doc - 1 |
| Commission / Bonuses / Incentives / Awards | 8 years | Doc - 2 |
| Employee Earnings Records | 3 years after termination of service of employment | Doc - 6 |
| Employee Handbook & Induction Manual | Permanent | Doc - 1 |
| Employee Medical Records | 3 years after termination of service of employment | Doc - 6 |
| Attendance records, application forms, job or promotion records, performance evaluations, termination papers, test results, training and qualification records, enquiry related papers | 3 years after termination of service of employment | Doc - 6 |
| Employment Contracts - Individual | 3 years after termination of service of employment | Doc - 6 |
| Correspondence with Employment Agencies and Advertisements for job openings | 3 years | Doc - 6 |
| Job Description | 3 years after superseding the earlier document | Doc - 6 |

Responsibility: HUMAN RESOURCES DEPARTMENT

11. Programs & Service Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Attendance Records | 3 years | Doc - 6 |
| Program statistics, etc. | 3 years | Doc - 6 |
| Research & Publications | Permanent | Doc - 1 |

Responsibility: HUMAN RESOURCES DEPARTMENT

12. Sponsorship Projects Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Sponsorship agreements | Permanent | Doc - 1 |

Responsibility : HUMAN RESOURCES DEPARTMENT

13. Corporate Social Responsibility Records

|  |  |  |
| --- | --- | --- |
| Record Type | Retention Period | Document Type |
| Records on CSR Projects(including amount budgeted, spent and balance if any) projects undertaken and progress thereon | Permanent | Doc - 1 |

Responsibility : HUMAN RESOURCES DEPARTMENT

14. Correspondence and Internal Memoranda

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract

Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years

Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently

**Responsibility : RESPECTIVE DEPARTMENT**

15. Electronic Documents including email retention and back up

**1.Electronic Mail :** Not all email needs to be retained, depending on the subject matters

All e-mail - from internal and external sources to be deleted after 24 months

Staff will strive to keep all but an insignificant minority of their email related to business issues

Central I.T team would archive email for six months after the staff has deleted it after which time the email will be permanently deleted

Staff will not store or transfer the Company related emails on non-work related computers except as necessary or appropriate with due approvals from the Central IT team and the respective Managers

Staff will take care not to send confidential / proprietary information to outside sources

Any e-mail that the staff deemed vital to the performance of their job should be copied to the staff's specific folder and/or printed and stored in the employee's workplace

**Document Type : Doc 5**

**2.Electronic Documents including PDF files**

PDF documents - Can be a maximum period of 8 years. But the said document may be destroyed depending upon the completion of the job or its use coming to an end

Text/ Formatted files : All word / excel / Power point files may be deleted once every year depending on the importance or lack of it

**Document Type : Doc - 3**

**3.Web page files**

May be retained for a period of 5 years as specified in SEBI's LODR Regulations, 2015

May be archived by the I.T. department with the support of the service provider for a period of 3 years after the initial period of five years of live page

**Document Type : Doc - 3**

**Responsibility : INFORMATION TECHNOLOGY DEPARTMENT**

16. Miscellaneous Records

|  |  |  |
| --- | --- | --- |
| **Record Type** | **Retention Period** | **Document Type** |
| Consultant Reports | 3 years | Doc - 6 |
| Policy and procedures manuals - Original | Current version with revision history | Doc - 6 |
| Policies and procedures manuals - Copies | Retain current version only | Doc - 6 |
| Dealership agreements | Current version with revision history | Doc - 6 |
| Annual Reports | Permanent | Doc -1 |
| Export Documentation - FIRC details | Permanent | Doc - 1 |
| Import Documentation | Permanent | Doc -1 |

**Responsibility : RESPECTIVE DEPARTMENT**

<https://www.esabindia.com/in/en/investors/policies/policy_on_document_retention_2015.cfm>

# https://www.legalserviceindia.com/article/l428-Data-Retention-Policies.html

**Document retention, especially the retention of electronic data has become a hot topic in the legal industry. In the 21st century business world, companies are creating and storing the electronic document and information at light speed. Electronic documents are not only found on desktops and laptops but also stored on the phones like Blackberry's etc. But for modern business organizations storing all this business information can be expensive not only because of the cost of physical storage of tapes but also because of the potential liability of keeping sometimes seemingly useless information for too long.**

**What is Data Retention Policies?**

**A document retention policy provides for the systematic review, retention and destruction of documents received or created in the course of business. A document retention policy will identify documents that need to be maintained and contain guidelines for how long certain documents should be kept and how they should be destroyed.**

**What documents must be protected?**

**Temporary Records  
Temporary records include all business documents that have not been completed. Such include, but are not limited to written memoranda and dictation to be typed in the future, reminders, to-do lists, report, case study, and calculation drafts, interoffice correspondence regarding a client or business transaction, and running logs.  
  
Final Records  
Final records include all business documents that are not superseded by modification or addition. Such include, but are not limited to: documents given (or sent via electronic form) to any third party not employed by Organization, or government agency; final memoranda and reports; correspondence; handwritten telephone memoranda not further transcribed; minutes; design/plan specifications; journal entries; cost estimates; etc. All accounting records shall be deemed final.**

**Permanent Records  
Permanent records include all business documents that define Organization's scope of work, expressions of professional opinions, research and reference materials. Such include, but are not limited to contracts, proposals, materials referencing expert opinions, annual financial statements, federal tax returns, payroll registers, copyright registrations, patents, etc. Except as provided for in the Document Retention Schedule (Appendix A), all permanent documents are to be retained indefinitely.  
  
Accounting and Corporate Tax Records  
Accounting and corporate tax records include, but are not limited to: financial statements; ledgers; audit records; invoices and expense records; federal, state, and property tax returns; payroll; accounting procedures; gross receipts; customer records; purchases; etc.  
  
Workplace Records  
Workplace records include, but are not limited to Articles of Incorporation, bylaws, meeting minutes, deeds and titles, leases, policy statements, contracts and agreements, patents and trademark records, etc**

**Employment, Employee, and Payroll Records**

**Employment records include, but are not limited to job announcements and advertisements; employment applications, background investigations, resumes, and letters of recommendation of persons not hired; etc. Unless otherwise specified in the DRS, such records should be retained for the minimum of one (1) year. Employee records include, but are not limited to employment applications, background investigations, resumes, and letters of recommendation of current and past employees, records relating to current and past employee's performance reviews and complaints, etc. Unless otherwise specified in the DRS, such records should be retained for the minimum of three (3) years following unemployment with Organization. Payroll records include, but are not limited to wage rate tables; salary history; current rate of pay; payroll deductions; time cards; W-2 and W-4 forms; bonuses; etc.  
  
Bank Records  
Bank records include, but are not limited to bank deposits; check copies; stop payment orders; bank statements; check signature authorizations; bank reconciliations; etc.  
  
Legal Records  
Legal records include, but are not limited to all contracts, legal records, statements, and correspondence, trademark and copyright registrations, patents, personal injury records and statements, press releases, public findings, etc.  
  
Historical Records  
Historical records are those that are no longer of use to Organization, but by virtue of their age or research value may be of historical interest or significance to Organization.**

**How long to retain data?**

**Only for so long as the law requires or for as long as you actually have use for them, and not a moment longer. There is no bright line number. In typical lawyerly fashion, my real answer is that it depends. Any records management program must ensure that legally required documents are kept for at least the minimum prescribed time periods. But, are there circumstances under which they should be kept for a longer period of time? In my view there are two answers to that question. First, there may be records you think are critical to preserving historical continuity, for example, minutes of strategic planning meetings or of policy development sessions. Board members come and go, and these records may help their successors understand the intent behind certain policies and standards, hopefully preventing repetitive wheel inventing exercises. More importantly, they may help prevent inconsistent decision making. These calls are tough to make, but the executive director is the person most likely to have the long-term perspective or corporate memory needed to make that decision. The second reason may be litigation or governmental investigations and enforcement actions. As I will discuss next, these latter circumstances will almost always out trump your retention and disposition schedule.**

**Why to have Data Retention Policies? (Purpose)**

**In today's business world, information is created and stored electronically on the computer. Therefore, the importance of creating and implementing a Document Retention Policy becomes more complicated, but extremely important in order to protect against cases of future litigation. A document retention policy provides for the systematic review, retention and destruction of documents received or created in the course of business. A document retention policy will identify documents that need to be maintained and contain guidelines for how long certain documents should be kept and how they should be destroyed.  
  
The policy is also helpful to:  
• provide a system for complying with document retention laws;  
• ensure that valuable documents are available when needed;  
• save money, space and time;  
• protect against allegations of selective document destruction; and  
• provide for the routine destruction of non-business, superfluous and outdated documents.**

**The six most important reasons why an organization should implement a document retention policy are:  
1) To comply with legal duties and requirements, either statutory or regulatory;  
2) To avoid liability through spoliation, the improper destruction or alteration of documents in a litigation situation;  
3) To support or oppose a position in an investigation or litigation;  
4) To protect from unnecessary expense and time during discovery;  
5) To maintain control over discovery and e-discovery, and  
6) To keep documents confidential and avoid leakage to attackers or competitors.  
  
Document retention policy is important in various aspects; First, adhering to the policy may limit liability in long run. Many a case has been damaged due to suffering of unfavorable emails or documents kept too long and taken out of context. In many of those case if document retention policies been in place and enforced, that information would no longer be available.  
  
Second, if a document retention policy limits how long the information is kept, companies will have less information to search and review if served with a document request.  
  
Finally, under Federal Rules of Civil Procedure (FRCP) only electronic information that is reasonably accessible due to undue burden of cost is discoverable. Thus a good document retention policy will make company in control of what is available and discoverable under the Federal Rules.**

**Laws Related to Data Retention Policy:**

**In India:  
In India there is no Central Act which laid down the provisions related to Data Retention Laws. But there are different policies incorporated by various agencies and which maintain and follows their policies. Example: Government of India Central Vigilance Commission by their wide notification no. No.17/09/2006-Admn. Gives the provisions related to Retention period/destruction schedule of recorded files, available at http://cvc.nic.in/retention.pdf; similarly the Ministry of Finance- Financial intelligence Unit has its own policy. Notification No. 9/2005 - gives the rules for Record Keeping and Reporting.  
  
{Rule 6. Retention of records - The records referred to in rule 3 shall be maintained for a period of ten years from the date of cessation of the transactions between the client and the banking company, financial institution or intermediary, as the case may be."}.**

**Thus, it may be noted that organization has its own Data retention Policies and certain rules for retention of such records. However, there is no such established law wherein it is binding for the organizations to prepare such policies.**

<https://www.legalserviceindia.com/article/l428-Data-Retention-Policies.html>

# https://www.intradyn.com/email-retention-laws/

Everything to Know About Email Retention Laws:

|  |  |  |
| --- | --- | --- |
| Industry | Regulatory Organization | # of Years Required for Retention |
| Credit Card and Related Processing Companies | PCI DSS | One year |
| Telecommunication | FCC (Title 47, Part 2) | Two years |
| All Federal, State and Local Agencies | FOIA (Federal and State) | Three years |
| DOD Contractors | DOD 5015.2 | Three years |
| Banking | FDIC | Five years |
| Pharmaceuticals, Biological Products and Food Manufacturers |  | Seven years |
| All Companies | IRS | Seven years |
| All Public Companies | Sarbanes Oxley (SOX) | Seven years |
| Bank and Finance Firms | Gramm-Leach-Bliley Act | Seven years |
| Healthcare | HIPAA | Seven years |
| Investment Advisers | SEC 204-2 | Seven years to lifetime |
| Securities Firms, Investment Bankers, Brokers and Dealers and Insurance Agents | SEC 17a(3) and 17a(4) | Seven years to lifetime |

Email Retention Laws Internationally

General Data Protection Regulation ([GDPR](https://www.eugdpr.org/)), which was approved in April 2016, is a regulation in European Union (EU) law on data protection and privacy for all individuals within the EU and the European Economic Area (EEA).

The GDPR has created a new standard for consumer rights regarding their data, but companies will be challenged as they put systems and processes in place to comply. It also addresses the export of personal data outside the EU and EEA areas.

The GDPR aims to give EU citizens and residents control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Companies that collect data on citizens in EU countries now need to comply with strict new rules around protecting customer data, effective since May 25, 2018.

The GDPR replaces the [Data Protection Directive](https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML), which was enacted in 1995, before social media, instant messaging and other collaborative applications helped to create the day-to-day business hub into which the internet has morphed. The GDPR looks to close that gap to protect the privacy and security of data collected by organizations on individuals with today’s communications tools.

The provisions are consistent across all 28 EU member states, which means that companies have just one standard to meet within the EU. These standards are quite high and will require most companies to make a large investment to meet and to administer the new regulatory standards.

Another rule will make it mandatory for companies to notify their data protection authority about a data breach within 72 hours of first becoming aware of it. The data processor will need to notify customers “[without undue delay](https://gdpr-info.eu/art-33-gdpr/)” after learning of the breach.

The GDPR should also be seen against the wider context of [high profile data breaches](https://www.techadvisor.co.uk/feature/small-business/uks-most-infamous-data-breaches-3788338/) which businesses from banking and finance to healthcare and telecommunications have suffered in recent years. These data breaches have ranged from the deployment of ransomware, malicious insider activity or, most commonly, the loss of data through the lack of oversight of employee activities and inadequate procedures and training.

Now that GDPR has become law, businesses and organizations need to ensure that they pay attention to the stipulations of the new regulations, and to make sure that their email communications are compliant. Here are some of the things a business or organization needs to think about when sending or archiving emails, or otherwise face the imposition of significant fines:

Personal data can only be held and processed for as long as is necessary for a specific purpose.

This necessitates careful consideration of how long archived emails need to be kept, further emphasizing the need for a concrete, thorough email retention policy.

Email contact cannot be made with clients without prior consent.

Consent needs to be explicit and informed.

Once consent is received it can only be used for that specific reason.

https://www.intradyn.com/email-retention-laws/

# Database Backup Retention Policy

Organizations frequently develop their own data retention policies; however, they must also ensure those policies meet or exceed all applicable data retention laws – especially in tightly regulated verticals. For this reason, organizations often use a data retention policy template that is industry-specific.

For example, publicly-traded United States companies must establish a Sarbanes-Oxley Act (SOX) data retention policy. Organizations that accept credit card payments must establish Payment Card Industry Data Security Standard (PCI DSS) data retention policies. Health care organizations must develop data retention policies that adhere to the Health Insurance and Portability and Accountability Act (HIPAA). And any business that processes or stores personal information about EU citizens must comply with the General Data Protection Regulation (GDPR), whether or not they are member states.

Next, consider the location of the data subject. In some cases, data located in different places may require unique data retention policies. This is, in part, because different business and legal requirements may control various databases, servers, hardware, and other locations.

Any data retention policy guidelines should touch upon backup frequency. Relevant questions include:

Is there a risk of data loss? If so, how severe is that risk?

Should we backup the data more than once a day? If so, how often?

How long should we keep the data—and does it change depending on the type of data?

Scenario 1: This is an example of a retention schedule set forth in this kind of data backup and retention policy:

Retain every daily backup for 7 days

Retain every weekly backup for 4 weeks

Retain every monthly backup for 12 months

Retain every annual backup for 7 years

Scenario 2 Database backup retention policy refers to how long the database backups are kept within our possession. Some examples would be:

daily backups for big databases are kept for one week using local storage,

weekly backups for small databases are kept for eight weeks on disk storage (both local and remote),

monthly backups for all databases are kept for 3 months on cloud storage,

no backups are saved beyond 3 months.

To build a good backup retention policy, we need to consider the two most important aspects:

Backup storage size.

Database backup size.

To understand this easily, consider the following backup retention setting for a cluster:

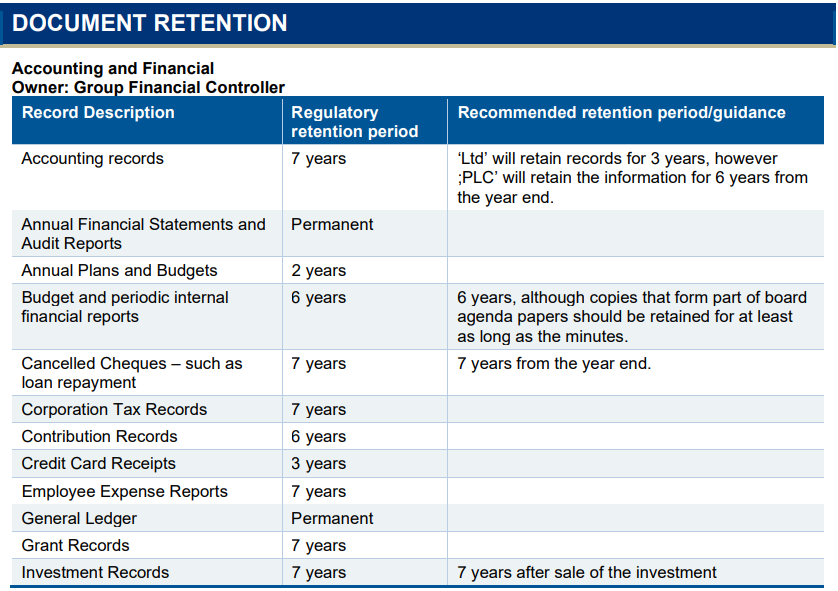
One creates a weekly backup, with a retention period of 14 days.

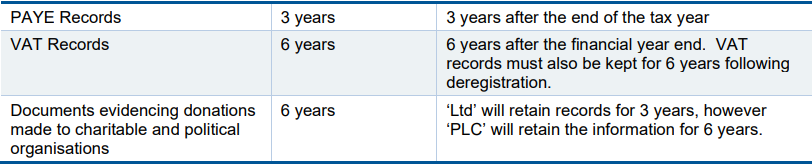
One creates an hourly backup, with a retention period of 7 days.

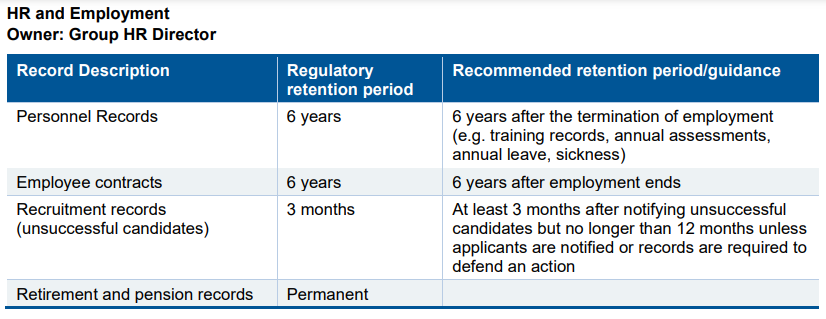
One creates a monthly backup, without a retention period (keep forever).

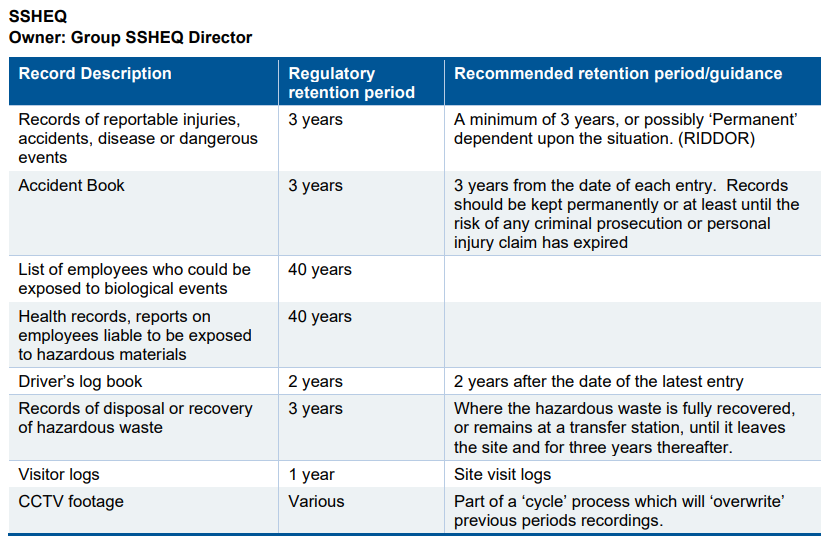
Finally, ensure you eliminate any data silos or islands of data outside the backup data retention policy, including desktops, laptops, and remote offices.

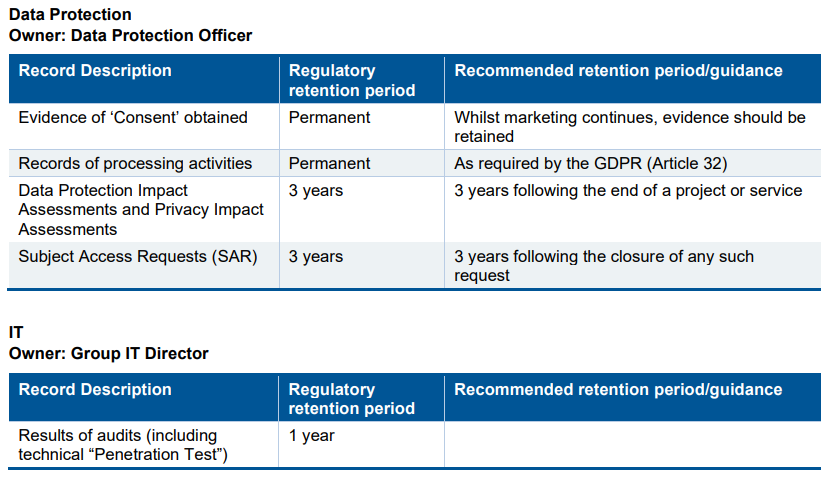
# https://www.tetratecheurope.com/wp-content/uploads/2021/05/Tetra\_Tech\_Data\_Retention\_Policy.pdf

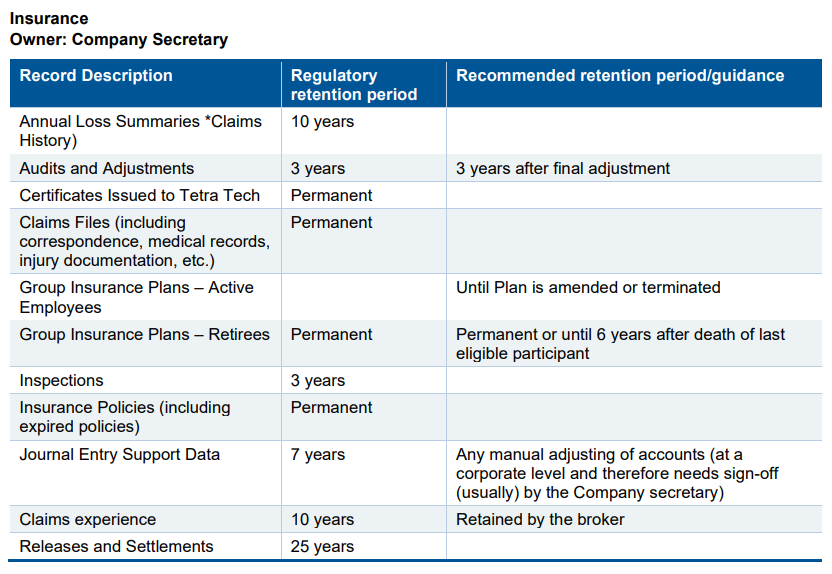


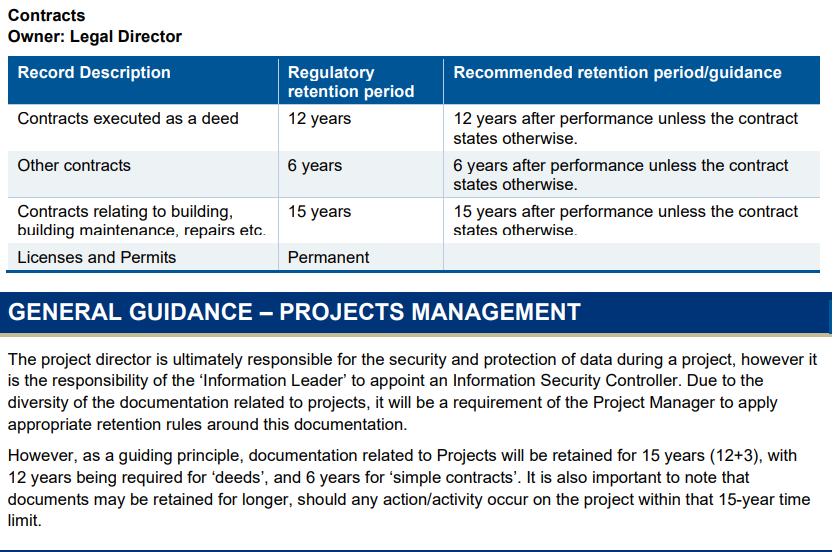


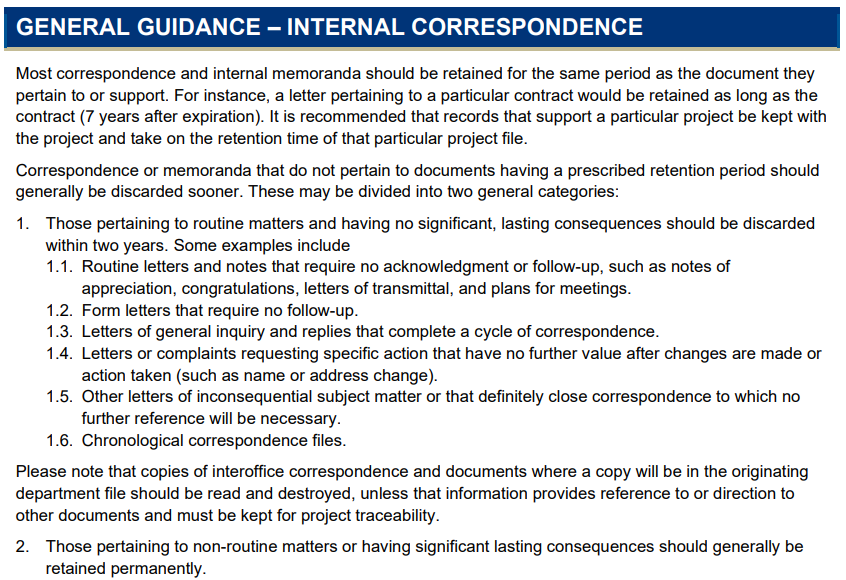


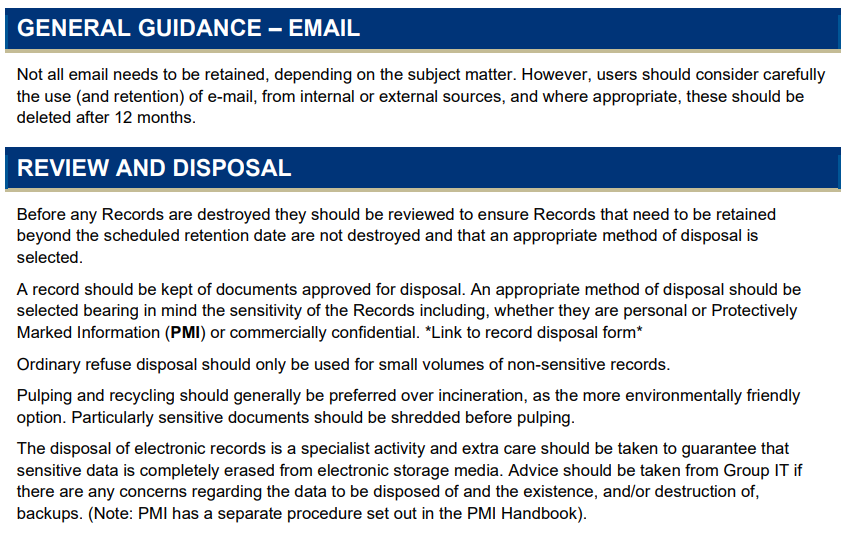












# Disclaimer:

(Please note: The information presented in this article is not legal advice. It is meant for educational and planning purposes only. Please consult with your legal counsel for any issues related to email retention laws.)