# Record retention policy

This **Record Retention policy** template is ready to be tailored for your company's needs and is a starting point for setting up your employment policies.

## Policy brief & purpose

Our Record Retention policy describes our guidelines to create, preserve and access our company's records. To ensure that our records are accurate and secure, we ask our employees to adhere to this policy.

## Scope

In this policy, a "record" is any type of electronic or paper file (document, spreadsheet, database entries) that we store in our systems. This includes files both employees and external sources create. All legal and business documents, as well as formal internal and external communications, fall under this policy's purview.

This policy applies to employees who may create, access and manage records. The HR and finance departments, which manage sensitive and critical information, are primarily responsible for keeping accurate and secure records. g. Every other employee who creates and stores important records should follow this policy too.

## Policy elements

### Creating records

We place high value on our company's records. By storing information, we are able to:

- Make better decisions
- Support our day-to-day operations
- Forecast and prepare for the future
- Learn from past mistakes
- Preserve and defend our company's legality
- Evaluate our operations and employee productivity over time
- Develop plans to improve and grow the company

### What records do employees need to create?

Creating and storing certain types of records are mandatory. Employees should keep records that:

- Are mandated by law (e.g. record keeping requirements of the Equal Employment Opportunity Commission (EEOC))
- Are necessary for them or other employees to perform their jobs
- Indicate internal or external changes that affect our operations, employees, partners or customers
- Include decisions, reports, data and activities that are important to our business
- Describe business ventures, deals and communication with regulatory bodies or the public

Employees, teams and departments may keep other records if they decide they're useful to their jobs.

We have a few general guidelines for creating records. Employees should:

- Ensure that information is accurate and complete
- Store records in appropriate mediums
- Name, categorize and share records properly
- Mark appropriate records as confidential
- Clarify who's authorized to access records

Employees should also check records electronic systems automatically generate to ensure their accuracy and proper storage.

## Authorization

Records may have different levels of authorization that limit their accessibility. The authorization level is usually determined by those who create the records, our company's official policy or the law (the law always take precedence.) The following records are strictly confidential and require a high-level authorization:

- [*Employment records*]
- [*Unpublished financial data*]
- [*Customer/ vendor/ partner/ job applicant information and contracts*]

Access to those records is restricted to employees who directly manage that information. Other types of records, like company performance metrics and internal policies, may be accessible by all permanent employees. Employees must not disclose records to people outside of our company, unless authorized.

Our confidentiality and data protection policies always apply to all relevant records.

## Retaining records

Our employees must protect our records, whether marked as confidential or not.

### Physical records

Printed records must be stored safely in filing cabinets or closed offices. Important, confidential files mustn't be left in open office areas.

When employees need to carry physical records out of our offices, they must prevent them from being damaged, lost or stolen. We advise our employees to avoid relocating records as much as possible.

### Electronic records

Electronic records will be protected by passwords, firewalls and other security settings (both locally and in the cloud.)

Employees are responsible for keeping these records intact. For example, if an employee shares a Google spreadsheet, they must decide whether to give colleagues permission to edit, view or comment. Employees should not grant editing privileges unless necessary.

Also, when employees access electronic, confidential records outside of our offices, they should ensure that both their devices and networks are secure. They should not leave their screens and devices unattended while logged in to our company's accounts.

### Data retention period

As a general rule, we will keep all records for a minimum of [two years.] The law may oblige us to retain certain records for a longer period. In this case, we'll abide by the law. Also, the following records must be preserved indefinitely:

- [*Tax returns*]
- [*Internal policies*]
- [*Employment contracts*]
- [*Partnership and vendor contracts*]
- [*Financial statements and annual reports*]
- [*Results of audits and legal investigations*]

## Discarding records

After the data retention period has passed, authorized employees may choose to discard records

for a specific reason. They will usually do this either by shredding physical documents or deleting data from a database or computer. Printed copies of electronic files should be shredded, too.

Records may also be discarded upon request from a stakeholder. For example, a customer or partner may ask us to delete their information from our databases. In this case, managers should authorize employees to discard relevant records.

We expect our employees to always respect our confidentiality policy. When files need to be discarded, employees must not create copies or store information on their devices. This may constitute a security breach and warrant disciplinary action.

*Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.*