

Employee Records & Files

Employers typically keep a number of different employee records, often called personnel files, as a way of documenting an employee's relationship with a company. Employers may also be required to keep certain records to comply with specific state and federal laws. General information and helpful links on how to keep compliant records are below.

<p>Which records should be kept in an employee's personnel file?</p>	<p>Among other things, personnel files generally contain the following categories of records:</p> <ul style="list-style-type: none"> • Basic Information Documents: The employee's full name, social security number, address, birth date, and emergency contact. • Hiring Documents: Job descriptions, employment applications, and resumes. • Job Performance Documents: Performance evaluations, notes regarding performance issues, corrective action or disciplinary letters, awards, nominations, commendation letters, promotion records, and records of training or education. • Employment-Related Agreements: Employment, non-compete, and nondisclosure agreements. • Compensation Documents: Salary letters, state and federal Form W-4s, and time cards. • Termination Documents: Termination letters, exit interview forms, benefits notices, and unemployment compensation forms.
<p>Which records should be kept in a confidential file separate from an employee's personnel file?</p>	<ul style="list-style-type: none"> • Medical records • Records relevant to workers' compensation claims • Employee leave documents • Form I-9s • Workplace investigation documents • Background check documents
<p>How long should records be kept?</p>	<p>Numerous federal laws impose specific requirements. States impose their own recordkeeping laws as well. To read about the requirements your state imposes, check out our State Laws section.</p>

<p>How should records be secured?</p>	<ul style="list-style-type: none"> • All paper records should generally be kept in a secure location, such as a locked cabinet or locked office. • Electronic records should generally be kept on password-protected systems. • Identify individuals authorized to access personnel and confidential files, and ensure that administrative, physical, and technical safeguards are in place that restrict access to those individuals only. • Define the specific circumstances in which employee files may be accessed or copied. <p>Click here for more information. However, please note that additional requirements apply to group health plans that create or receive employees' electronic protected health information.</p>
<p>How should records be disposed of?</p>	<ul style="list-style-type: none"> • Papers should be burned or shredded • Electronic files should be destroyed or erased
<p>Where can I download forms on which I can properly record employee information?</p>	<p>Click here to download helpful forms.</p>