Employee Records & Files

COMPLETE PAYROLL SOLUTIONS

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.

Question	Answer
Which records should be kept in an employee's personnel file?	Among other things, personnel files generally contain the following categories of records: • 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
Which records should be kept in a confidential file separate from an employee's personnel file?	• Medical records • Records relevant to workers' compensation claims • Employee leave documents • Form I-9s • Workplace investigation documents • Background check documents
How long should records be kept?	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.
How should records be secured?	• 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 • Only authorized individuals should be allowed to access personnel and confidential files, and administrative, physical, and technical safeguards should be in place to restrict access to those individuals • Specific circumstances should be defined for accessing or copying employee files 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.
How should records be disposed of?	• Papers should be burned or shredded • Electronic files should be destroyed or erased
Where can I download forms on which I can properly record employee information?	Click here to download helpful forms