

The Basics of Employee Files: What Every Small Business Needs to Know



Welcome!

Whether you're a business of one or one hundred, keeping accurate and well-organized employee files isn't just good practice—it's a legal and strategic necessity. If your HR “filing system” is currently a stack of papers in a drawer or a desktop folder labeled “HR Stuff,” it may be time to tighten things up.

What Goes Into an Employee File?

Employee files are more than just paperwork—they serve as a historical and legal record of an individual's employment with your company. According to both sources, a well-organized system typically includes three main categories:

1 Personnel File

This is the central file that contains the day-to-day employment documents such as:

- Job application and resume
- Offer letter
- Employment agreement or contract
- Job descriptions
- Performance reviews
- Promotions, demotions, or disciplinary actions
- Training and development records
- Termination documents (if applicable)

2 Confidential File (Medical & Protected Information)

To maintain compliance with laws like the Americans with Disabilities Act (ADA) and HIPAA, any document that includes sensitive or medical information must be stored separately.

This includes:

- Doctor's notes
- FMLA leave documents
- Disability accommodations
- Drug test results

3 Payroll/Tax File

Often stored separately for auditing and privacy reasons, this file includes:

- W-4 forms
- Direct deposit authorization
- Time sheets or time-tracking reports
- Salary history and pay changes
- Records of bonuses or commissions

Why Separation and Security Matter

It's tempting to keep everything in one folder (or worse, one PDF), but commingling sensitive information could put your business at risk. Both Factorial and Wolters Kluwer stress the importance of maintaining **separate files** to limit access to sensitive data and ensure compliance with employment and privacy laws.

For example, only those with a legitimate business reason—like payroll staff—should have access to tax and compensation information. Meanwhile, access to medical files should be highly restricted, often limited to HR personnel only.

Record Retention: How Long Should You Keep These Files?

A critical part of compliance is knowing how long to retain different types of documents. Here's a general guideline:

- **Job applications/resumes (not hired):** 1 year
- **Payroll records:** 3 years
- **I-9 forms:** 3 years after the date of hire or 1 year after termination, whichever is later
- **Personnel files:** 3–7 years after termination
- **Medical records (OSHA-related):** 30 years in some cases

These timelines can vary based on your state and industry, so it's wise to consult a professional or use reputable tools to stay current.

Pro Tips for Small Business Owners

- **Go Digital (Securely):** Cloud-based HR systems (like Factorial and others) make organization and compliance much easier.
- **Create an Employee File Checklist:** This ensures consistency across all personnel.
- **Limit Access & Use Password Protection:** Security isn't optional—it's your legal obligation.
- **Review Regularly:** Set a calendar reminder to review and purge outdated files at least annually.

Final Thoughts

Establishing and maintaining employee records isn't just red tape—it protects your business, supports your employees, and helps you make better decisions. By setting up the right structure from the start, you'll save yourself headaches down the road and stay in good standing with regulators.

Not sure where to begin? Start with a simple folder structure, use a checklist, and consider digital solutions that grow with your team. As the saying goes: "Don't get ready—stay ready."



TalentSENSE

Human Resources & Recruiting

Jennifer Osborn

President, TalentSENSE Consulting

www.talentsensehr.com

josborn@talentsensehr.com

Connect with me on LinkedIn:

www.linkedin.com/in/jenniferosbornhr

SPECIAL OFFER!

Schedule a free HR or Recruiting Consultation with me here,
or scan the QR code below

