Checklist: Employment Recordkeeping Audit

Note to Employers:
Each employer may have its own unique employment record maintenance practices. Personnel records can be maintained in paper form, scanned, or completed and maintained electronically. This checklist is meant to audit an overall employee recordkeeping system, and not individual file components.

Electronic storage system (if applicable)

☐ Does the recordkeeping system have reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form?

☐ Are the electronic records maintained in reasonable order, in a safe and accessible place and in a way which they may be readily inspected or examined?

☐ Can the electronic records be readily converted into legible and readable paper copy as needed?

☐ Are regular evaluations of the electronic recordkeeping system conducted to ensure the technology is sufficient and not obsolete?

☐ Are paper copies retained for records that cannot be clearly, accurately or completely transferred to an electronic recordkeeping system?

☐ Is there a written policy regarding the electronic recordkeeping system that includes clear parameters regarding access to electronic records?

☐ Are there security and password protections to ensure access is provided only to those with a need to know?

☐ Is there a backup system in place to ensure data are not lost?

☐ Is there a secondary backup system off-site in the event both the software and its backup are destroyed?

☐ Is training provided to authorized users on how to properly use and protect information in the electronic recordkeeping system?

Employee files

☐ Are files maintained in a locked and secure cabinet, or have proper electronic security features been developed?

☐ Have all documents that contain sensitive/confidential information such as social security numbers been removed from the personnel file?

☐ Are personnel files organized in a logical manner so that information is easy to find?

☐ Is there a policy regarding employee access to personnel files in compliance with state law?

☐ Are individual files audited internally for compliance on a regular schedule?

Medical files

☐ Are records containing employee medical information kept separate from employee personnel files?

☐ Is employee medical information securely stored with limited access?

I-9 forms

☐ Are I-9 forms and relevant documentation kept separate from employee personnel files?

☐ Are I-9 forms securely stored with limited access?

☐ Are I-9 forms audited internally on an established schedule?

EEO records

☐ Are equal employment opportunity (EEO) data records maintained separately from personnel files and used only for reporting purposes such as for an affirmative action program (AAP), EEO-1 reporting and internal diversity tracking?

☐ Are EEO records securely stored with limited access?

Terminated employee files

☐ Are terminated files securely stored with limited access?

☐ Is there a regular (monthly or quarterly) disposal plan for documents that have exceeded record retention requirements?

☐ Are records that have met or exceeded record retention requirements disposed of via shredding, burning or fully destroying these records prior to disposal?

☐ Are files related to a current or potential lawsuit maintained by legal counsel or otherwise marked to be exempted from any disposal process until after the suit is closed?

☐ Is there a written record retention and destruction policy and procedure?