FACT SHEET - HR PROFESSIONALS

The Secure Exit Kit

When an employee leaves:

Human Resources professionals have the responsibility to not only provide a smooth transition, but also ensure confidential data is protected in the process. Be sure to cover all your bases especially during a job transition or departure. This means establishing information security best practices that address all sources of fraud or identity theft, including physical and digital data.

The Six-Step Secure Employee Exit:

1. Collect all records

Collect all documents or records created during employment that contain personal or identifying information. This includes any notes or documents from the employee's supervisor regarding performance.

2. Stay organized

There are government and industry requirements for how long you need to keep certain records. Separate and store records based on required retention times or code them with colored folders. Ensure any documents that may be needed in the event of an audit are locked away but easily accessible.

3. Mark for destruction

Mark each record box with the employee's departure date and the destruction date for their documents, based on legal requirements. This way you can see clearly when it's time to destroy documents and avoid unnecessary stockpiling.

4. Protect customer data

Work with the departing employee to collect any contracts, accounting information or confidential customer data they have stored in paper files or on devices. Work with your IT team to remove any sensitive company or client information from personal devices used in a professional capacity, including smartphones, tablets and computers. Any information collected needs to be stored for the appropriate amount of time before destruction.

Did You Know?

25% of global data breaches are due to negligent employees. Globally, the average cost per lost or stolenrecord is $122 USD.

Source: 2017 Ponemon Cost of a Data Breach Study

5. Destroy digital data

Remove and destroy the hard drive from the employee's computer before sending it for recycling. Destroying the device's hard drive is the only way to ensure the employee and company information is unrecoverable. Don't forget to also collect and destroy any company or corporate credit cards issued to the employee.

6. Understand legal requirements

In addition to your own organization's rules on the collection and handling of confidential information, you have to follow legal requirements. Schedule a yearly meeting with your legal team to ensure you understand the requirements and any recent changes that affect document retention or the collection and handling of confidential information.

Employee Exit Checklist

What to Collect

- Résumés and initial job applications
- Interview records and notes
- Letters of reference and employment verification
- Background checks and drug test results
- Driving records
- Termination forms and letters
- Employee contracts
- Tax forms
- Medical or WSIB records
- Performance appraisals and dispute records
- Compensation records and job history
- FMLA and USERRA records
- I-9 and W4 forms
- OSHA and COBRA logs

Where to Look

- Desktop and desk drawers
- Filing cabinets, both shared and in the employee's workspace
- Removable media (USB sticks, CDs, removable hard drives, etc.)
- The employee's hard drive
- Area(s) on server(s) designated for the employee's use or under the employee's control
- Email and calendar accounts
- The shared areas of servers
- Electronic devices, whether owned by the company or individual

Timelines for Destruction

Pre-employment records	3 years
Background checks, drug test results, driving records, letters of reference	5 years
Compensation, job history, timekeeping records	4 years after termination
FMLA and USERRA and related leave records	3 years after termination
EEO-1 reports	2 years after filing
Annual Affirmative Action plans	2 years after AAP year
OSHA 300/300A	5 years after posting
Form 5500	6 years after filing
Federal/state tax reports	4 years after filing

This is a general guideline. Consult legal advice for your company's specific requirements.

Know your Legislation

The Privacy Act
PIPEDA
Sarbanes-Oxley Act
HIPAA & HITECH
Payment Card Industry (PCI) Security Standards
FMLA
USERRA
OSHA
FERPA
Fair and Accurate Credit Transaction Act (FACTA)
The Identity Theft Penalty Enhancement Act
US Patriot Act
SOX
GLBA
General Data Protection Regulation