Published on *The National Law Review* https://natlawreview.com

When Employees Leave, Make Sure Your Information Security Doesn't Walk Out the Door With Them

Article By:

Data Privacy & Information Security

An employee's departure represents a significant threat to an organization's information security if sufficient procedures are not in place (and actually followed) in connection with the departure.

Here are some important steps to take to keep departing employees (whether resigning or terminated) from undermining your security, whether unwittingly or intentionally.

- Make sure the HR department notifies IT of an employee's resignation or termination and last date of employment, so the departing employee's login credentials and access rights to company computers, email, and other information systems are deactivated prior to or at the time of departure.
- Have and use an exit interview process to identify and retrieve from a departing employee all company equipment, files, and information (which may be proprietary company information or personal information about other employees or customers). If there is advance notice of the employee's resignation or termination, advance planning may be appropriate to assess any anticipated logistical difficulties, such as timely retrieval of equipment or files the employee used at home.
- Follow up on or before the date of departure to make sure the departing employee returned all company equipment and portable devices and retrieved, returned, or destroyed all company information on any personal equipment or portable device. Requesting that the employee sign a certification to that effect may be appropriate.
- Upon retrieving a departing employee's equipment and records, review the material to determine whether any information or records must be preserved pursuant to the organization's records management program or an active legal hold. After taking appropriate preservation steps, dispose of information securely (the methods of disposal may be dictated by law). Ensure that portable devices returned by the departing employee are wiped prior to reissuing the devices to other employees.
- Use the exit interview process to remind departing employees of their obligations to maintain confidentiality and to return company property and information (which should have been included in policies, personnel manuals, and employment agreements). You also may want to inquire about new employment a departing employee has obtained or is seeking, and assess whether there is any risk that company information may be taken by the employee upon departure. If so, it may be appropriate to terminate access or eliminate "write" capabilities. If

there are any indications of possible misappropriation after departure, consult legal counsel regarding an appropriate response and a possible IT forensic investigation.

- Employees' access rights to company information and systems should be limited and carefully delineated based on individual roles and responsibilities. In the context of departures, this delineation can help establish that departing employees who may access and copy company information are doing so without authorization.
- Actively review employees' access authorizations on a regular basis to make sure departed employees' access rights were effectively terminated. Periodic reviews also help ensure that access rights of employees whose roles may have changed are adjusted accordingly.

Having these procedures in place and following them, both before and after notice of an employee's resignation or termination, should be an essential component of any company's information security program. The attorneys in our Privacy and Information Security Practice can help you develop a comprehensive strategy to address these and other aspects of your information security program.

National Law Review, Volume , Number 272