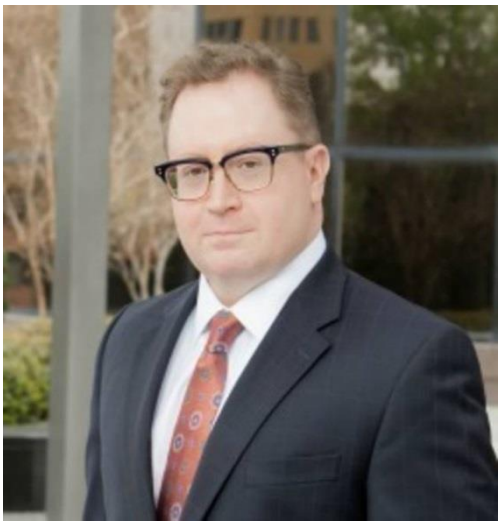
THE OKLAHOMAN

Data protection requires certain policy, procedural and equipment considerations

by **Paula Burkes** Published: November 30, 2017 5:00 AM CDT *Updated: November 30, 2017 5:00 AM CDT*



Data protection requires certain policy, procedural and equipment considerations

Q: When should companies start working with employees on security?

A: In today's environment, a data breach is less of a hypothetical and more of a likelihood. As almost every company handles valuable data of some sort, security is an important responsibility throughout an employee's entire tenure with the company — even before she's hired.

Q: What can an employer do to ensure employees don't become potential weaknesses in the company's data security profile?

A: In the pre-hire process, data security requirements and responsibilities of both the company and the employee should be established, documented and communicated. During the interview process, human resources and hiring managers should communicate the expected protocols and confirm the prospective employee's understanding and acceptance of them.

Q: What are some necessary security steps once a new employee comes on board?

A: When a new employee joins the team, managers should ensure he/she receives information security training that is appropriate to his/her particular job responsibilities. Company policies addressing internal information classifications and required security, acceptable use of company technology and devices belonging to the employee, and incident reporting procedures should be provided to and acknowledged by the prospective hire. This includes training on appropriate data storage and movement, such as where to save sensitive information, what to leave in and move from email, what can and can't be sent to and from personal email and how to properly send sensitive information. Employees should also be trained on how to report information security issues and provided a means to communicate any potential problems they encounter.

Q: What about information or equipment new employees might bring to the job?

A: During the recruiting and interview process, employers should communicate restrictions on bringing information from the prospect's prior employer. Such restrictions may be reinforced by requiring new hires to certify that they have taken no such information, particularly if the new employee is subject to an existing noncompetition or nonsolicitation agreement.

Q: What should be done when an employee leaves the company?

A: As an employee is leaving, it may be helpful to remind the employee of the company's data security rights and responsibilities. Given the transportability of data, the company may consider communicating the departing employee's responsibility to “bring everything back/leave everything here” and obtain some certification/acknowledgment that nothing has been taken. Limitations on systems access (appropriate to the timing and nature of the departure) should be applied, as well. The employer also should have a plan for dealing with personal information on company computers, with human resources and IT (and in some cases, legal) coordinating with the terminating manager. Finally, the employer should make sure the departing employee's technology is preserved in the event issues are identified later. This includes not “reassigning” a computer that may need to be reviewed because of potential difficulty in separating the new information from the old and the risk of the prior user's information being corrupted or deleted.

PAULA BURKES, BUSINESS WRITER

http://newsok.com/data-protection-requires-certain-policy-procedural-and-equipment-considerations/article/5574023