SMITH ANDERSON

PROTECTING COMPANY INFORMATION WHEN EMPLOYEES DEPART: CHECKLIST

Kimberly J. Korando
Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.
Raleigh, North Carolina
919.821.6671
kkorando@smithlaw.com

❑ Reasonable Efforts to Protect from the Beginning

The key to successfully pursuing rights or remedies for theft of company information is to be able to prove that the company took "reasonable steps" to protect the information. These efforts also likely will prevent theft from occurring in the first place. Common steps that should be considered include:

1. Limit Access

- Limit access to those who need to know the information to do their job. For example, customer information should be available only to those who need it, and not others.

- Limit the number of copies of confidential documents and, for especially sensitive information, use control numbers with records kept as to authorized recipients.

2. Educate Employees about Confidentiality

- Have signed confidentiality agreements with employees and third parties who have access to the information. These should be tendered to the employee at the time of employment and made a condition of the offer, and signed on or before the ***first day of employment and again at termination.***

- Distribute the confidential information policy in the employee handbook. The policy (and the confidentiality agreement) should have consistent terms and, among other things, include the following commonly omitted terms: address use of external storage devices, ban use of personal storage devices (e.g., thumb drives) and email of company documents to personal email accounts; prohibit installation of unapproved software; prohibit cleaning, defragmentation of employee computer; prohibit deletion of any emails or information before employee departs; and require return and deletion of all information that may reside on the employee's personal or home devices.

- Conduct ongoing employee awareness and training programs about confidentiality of company information. Protection of the company's information should be part of new employee orientation and, where appropriate department orientation.

3. Selected Security Measures

Management, IT and HR should collaborate on which documents and data require security measures and which measures are appropriate and feasible. Some commonly used measures include:

- Mark all proprietary and confidential documents, as such. Encrypt select documents to prevent them for being emailed, downloaded or copied.

- Establish firewalls for confidential and non-confidential information on the server.

- Use security software that prevents outgoing emails from attaching sensitive company information. (The software scans for key words and sequesters until reviewed internally.)

- Remote work should be done on company-owned computer or through a direct connection to the employer network. Allowing employees to work remotely from personal devices leads to retrieval problems.

□ Conduct an Exit Interview

- Review and audit the departing employee's paper and electronic documents; question the employee about information that may remain in his/her possession (e.g., at home, on PDA, etc.) At least one supervisor/management representative knowledgeable about the nature/scope of the employee's assignments should be present. Consider a pre-interview forensic examination of the computer; in voluntary terminations, check for large deletions or evidence of cleaning or defragmentation.

- Review the confidentiality agreement with the employee and provide him/her with a copy of the confidentiality agreement s/he signed.

- Question the employee about his/her next employment, including the specific job duties/nature of the projects), and document the exit interview, including the employee’s acknowledgement of duties to the company and return of company property and information provided about next employment (including specific job duties/nature of projects).

- Send a follow-up letter to individual detailing the exit interview acknowledgements and continuing obligations.

□ **Monitor System Activity**

- Ensure company information is not being downloaded or sent to personal email accounts.

- Consider forensic examination of hard drive. In involuntary terminations, the company may consider conducting a pre-notification examination so as to be able to determine whether suspicious activity occurred after the notification.

□ **Terminate Access Immediately**

HR should collaborate with IT to develop a checklist custom to the company. The following are some commonly included checklist items to help begin the process:

Premises

- Obtain security access cards

- Change access and security codes

Systems

- Remove network rights
- Disable remote access to network via web or dial-in
- Change passwords for all applications to which employee had access via the server
- Remove administrator rights, if any

Computer

- Obtain custody of desktop and/or lap top computer
- Disable Windows log-in account
- Change passwords for all applications on computer
- Remove employee’s personal files from system/computer, including any personal email folders

Hard Drives and Memory Devices

- Obtain custody of all company external hard drives and memory sticks
- If there is potential for litigation or other dispute, then remove and secure the hard drive and do not redeploy.

Email

- Disable email account
- Disable remote email access

Phones

- Obtain custody of cell phone, smart phone, PDA

  - Delete voicemail account or change the password
  - Update phone directory (hard and electronic)

  Credit Cards

  - Obtain custody

  Data

  - Take any additional steps to restrict access to confidential information

  Files

  - Take inventory of all files/projects on which individual was working; ensure that all materials are returned (very important if employee worked remotely).

□ **Warning Signs of Potential Theft**

- Refusing to disclose identity of new employer or new assignments
- Working unusual hours in final days (early, late, weekends)
- Giving little or no notice of resignation

□ **Preserving Evidence**

When you suspect theft or suspicious activity, you would be well-served to contact corporate legal counsel for direction as to how best to proceed to preserve evidence and potential legal rights before you take any other actions. In the meantime, the following steps can help preserve the company's rights:

- Lock down the computers, PDAs and other items where information may have been stored.

- Do not allow IT to look around for signs of inappropriate activity—this may contaminate evidence. A forensic examiner should be used for these activities. Lessons learned:

  - Electronic evidence is lost through computer use and activities as benign as booting up the computer.

  - A computer image conducted by IT is NOT a forensic image that will preserve evidence without altering the original. Forensic images can recover deleted files, search fragments of deleted files and perform other analyses without losing evidence.

  - Do not assume that a wiped computer no longer contains useful evidence; however, recovering that evidence may be expensive.

  - Complete forensic analysis requires input and follow-up questions from the company, particularly with regard to keyword searching, database/internet history review, file use history review, software use analysis, event log review and deletion reconstruction analysis.