Nichols College

Policy on Safeguarding Confidential Information

Background

The safeguarding of confidential information is not only good business practice, but failure to protect certain kinds of confidential information is a violation of federal and/or state law. Data breaches, as they are referred to in the law, can result in significant monetary damages to unsuspecting victims. As a result, businesses, including colleges, can be held legally liable for data breaches, whether they are the result of the inadvertent handling of files or equipment, or whether they result from intentional acts.

In order to prevent harmful data breaches, and in order to become compliant with government regulations, and in order to ensure that the College is safeguarding confidential information of all types, the College has developed the procedures set forth in this policy statement. This policy identifies three kinds of personal information which institutions are obligated to protect.

1) Social Security Numbers.
2) Driver's license numbers or state identification card numbers.
3) Financial, credit, and debit numbers, including passwords for access to such accounts.

On the federal side, the Federal Trade Commission has promulgated what they refer to as the "Red Flags Rule." The Rule focuses primarily on financial institutions. However, colleges need to become compliant with the federal rule because there are functions that colleges perform that resemble financial institutions, especially the loan work of college financial aid offices and credit card sales in the College Bookstore.

FERPA and HIPAA

These federal and state confidentiality/privacy regulations should not be confused with The Family Educational Rights and Privacy Act (FERPA) and The Health Insurance Portability and Accountability Act (HIPAA). While each of these federal acts has its own jurisdictional area (FERPA: student records; HIPPA: medical records), the new data security regulations, although different in what information they protect, overlap somewhat with both FERPA and HIPAA regulations. However, it is not so important to know the distinction among all these regulations as it is to be cognizant of the fact that all of the data and information that may fall within these areas should be treated confidentially and shredded when no longer needed.

Action to be Taken

Regarding data security, if it is not essential that your department collect and maintain any or all of the three kinds of personal information highlighted by the law, please eliminate collecting it. If your department needs to collect it but doesn't need to keep it, please have these records shredded.

If your department must collect and/or maintain personal information, you must develop effective and reliable methods for safeguarding the information from security breaches. Below is a list of simple procedures you should implement within your department to greatly lessen the chance that the College will be found liable for the damage caused by a data breach. Please note that these procedures are only a starting point for securing your department's data. Additional security measures should be implemented where necessary, and your department should audit its security measures on an annual basis to ensure the proper security of your department's information.

Workplace Security Measures

Confidential information should not be left in public areas where unauthorized individuals may view it.

When not in use, confidential information should be secured in locked cabinets, or in locked file-rooms which are not accessible to unauthorized individuals.

Confidential files should not be left out on desks at the end of the workday.

Keys to file cabinets and desks that contain confidential information should be properly secured.

You should confront anyone who you feel is unauthorized to be in certain areas of the College, or call Public Safety to investigate the situation.

Confidential information should only be discussed or shared with individuals on a need-to-know basis.

Telephone Security

You should not reveal confidential information about the College, its students or its employees unless the person you are speaking with is authorized to receive such information and has a legitimate need-to-know. You also must verify the person you are speaking to on the phone is who they say they are.

Do not leave any confidential information on a voice mail system unless the recipient is expecting this information to be left on the system.

Cellular and cordless telephones should not be used to transmit confidential information due to the fact that these devises are radio transmitters and can easily be monitored by radio hobbyists and interlopers who might sell the information they capture.

Employees who have their Nichols email forwarded to their cell phones, should not have confidential information sent or received in the emails.

Fax Security

Transmitting confidential information by fax can be dangerous. Make sure the fax number you are transmitting to is correct, and after you type the number on your fax machine, double-check the number for accuracy prior to hitting the “send” button. Also, when faxing confidential information it is prudent to first alert your intended recipient, as many fax machines are located in common areas where unauthorized individuals will have the opportunity to view, steal, or copy the faxed information.

Distribution of Confidential Information

When sending confidential materials by interoffice mail, use a sealed envelope and write or stamp “CONFIDENTIAL” in bold or in red ink across the envelope.

Discarding of Confidential Information

As soon as confidential information is no longer needed, it should be shredded.

At internal meetings where confidential information is distributed in the form of handouts, and where it is not necessary for the participants to leave with these handouts, they should be collected by the individual who handed them out and properly shredded.

If it is absolutely necessary for an employee to take home confidential materials, and if these materials are no longer needed, they should not be disposed of through residential trash unless there is a shredder available in the home. Otherwise, these

confidential materials should be taken back to the office where they can be properly shredded.

Traveling with Confidential Materials

There may be times when College employees need to travel with confidential materials. In these cases, employees should be extra vigilant in safeguarding these materials. Admissions recruiters and Institutional Advancement employees are examples of College employees who sometimes must travel with confidential information or confidential files. If traveling with a laptop, the hard drive must be password protected or encrypted if it contains any confidential information.

Do not place confidential reports or files on memory sticks or other media devices. Confidential information should only be on Nichols College servers or a password protected hard drive.

Each operational department is mandated to provide their employees with specific procedures that will likely reduce the chances of a data breach when they are traveling with confidential materials.

Confidential conversations should not occur in taxis or in public transit vehicles.

Precautions must be established to ensure that confidential materials are not left behind in taxis, on public transit vehicles, on airline seats, in hotel rooms, or in rented vehicles.

Electronic Security

Email

College Email accounts are not secure. Therefore, never “SEND” any confidential information via email or via email attachments unless they are properly encrypted.

If you receive emails or attachments containing confidential information, you are responsible for ensuring the security of this information. As soon as you no longer need the confidential information, please delete the email or attachment.

Files and Reports

Do not place confidential reports or files on your laptop computer (unless the hard drive is password protected or encrypted), on memory sticks or other media devices. Confidential information should only be on your server drives (e.g. H:\; T:\; other).

Working from home must be done securely. Nichols provides Citrix remote access to systems and server drives. All transmissions using Citrix are encrypted (secure). If you need to work from home with confidential information, contact the IT Department to learn how to have the Citrix software installed on your computer. When working from home or while on the road, leave secure files on the server. Do not try to copy them to your laptop or home computer.

The College Servers

The IT Department will endeavor to make the College network free from malware which attempts to steal confidential information for criminal use.

In order to accomplish this, the IT Department will endeavor to do the following:

- Establish user authenticity protocols that include control of user ID.
- Establish a secure method of assigning passwords.
- Ensure that password location does not compromise the security of the data.
- Restrict access to active users only.
- Block access after multiple unsuccessful attempts.
- Periodically monitor systems for signs of unauthorized use or access.
- Provide reasonably up-to-date malware protection and virus definitions.
- Restrict access to personal information on a need-to-know basis.
- Review security measures annually.

Awareness and Training

The Information Technology (IT) department will be responsible for developing a program for creating awareness of the critical importance of data security across the campus. IT will also be responsible for providing training to employees as well as to all newly hired employees about the importance of data security and common techniques to maintain the security of College information.

In the event of a data breach at the college, disciplinary measures for each situation will be handled on a case-by-case basis, taking into consideration the severity of the data breach and the extent to which the breach was a direct result of employee negligence. Disciplinary action may include, without limitation, suspension of system privileges, unpaid suspension of employment, termination of employment and/or legal action as may be appropriate. Intentional data breaches will be grounds for immediate termination of employment.

IT will also create protocols for limiting access to confidential information upon the separation or termination of employees. Employees who are terminated by the College should lose access to confidential information at the time they are notified of their termination.

Administration of the Data Security Policy

The regulations mandate that one person be designated by the College to act as the institutional Data Security Officer. This officer is to be responsible for the institution's data security, and is to be the institution's liaison official between the institution and state and federal officials such as the Attorney General. The Chief Information Officer will serve as the College's Data Security Officer. In this capacity he will be responsible for the following:

1) Promoting good business practices throughout the College community that directly lead to better data security practices.
2) Ensuring that employees are trained about the importance of data security and work habits that promote the security of confidential information.
3) Reviewing security measures annually.
4) Ensuring that vendors who need access to the College's confidential records will safeguard this information.
5) Limiting the amount of personal information collected.
6) Limiting the time College departments retain personal information that can be legally destroyed.
7) Properly identifying records that contain personal information.
8) Developing techniques and methods of destroying confidential information that is no longer necessary to keep.
9) Developing a records-retention policy for College records.
10) Developing a process to determine whether a data breach rises to the level of needing to contact the state Attorney General.
11) Documenting action taken in response to security breaches.

This policy was adapted with permission from Assumption College.

--- END ---